Administration Guide

Novell®
Dynamic File Services

1.6

February 17, 2011

www.novell.com

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

This product includes log4net open source software that is developed as part of the Apache Logging Services project. For information, see log4net (http://logging.apache.org/log4net/) on Apache.org.

This product includes Plossum open source software that is developed by the Plossum open source project. For information, see Plossum (http://sourceforge.net/projects/plossum) on SourceForge.net.

This product includes ZedGraph open source software that is developed by the ZedGraph open source project. For information, see ZedGraph.org (http://zedgraph.org).

Contents

D Keyboard Shortcuts   231

E Email Subject and Body Format for Event Notifications   235

About This Guide

This guide describes how to create and manage Novell Dynamic File Services (DynamicFS) 1.6 pairs and policies in a Microsoft Windows Workgroup or Active Directory Domain environment.

Audience

This guide is designed to help storage solutions administrators understand how to do the following:

- Make planning decisions for implementing pairs and policies as part of the overall storage solution strategy.
- Configure and manage the Service.
- Create and manage pairs and policies.
- Monitor the pair statistics, policy execution history, and disk history for each pair.

The Security Considerations section provides information of interest for security administrators or an administrator user that is responsible for the security of the system.

Some background knowledge of the host operating system, file system, and Active Directory is assumed.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to `www.novell.com/documentation/feedback.html` and enter your comments there.

Documentation Updates

For the most recent version of the *Novell Dynamic File Services Administration Guide*, visit the Novell Dynamic File Services 1.6 documentation Web site (http://www.novell.com/documentation/dynamic_file_services/).

Additional Documentation

See the following guides at the Novell Dynamic File Services 1.6 documentation Web site (http://www.novell.com/documentation/dynamic_file_services/):

- *Readme*
- *Installation Guide*
- *Client Commands and Utilities Reference*

Overview of Dynamic File Services

1

Novell Dynamic File Services (DynamicFS) is an information life-cycle management technology that uses a policy-based approach for relocating files between two paths located on different storage devices. These two logically related storage locations are referred to as a *pair*.

Dynamic File Services transparently provides users with a merged view of the two file trees via a network share on the primary path. Files on the primary and secondary paths are equally accessible to users. DynamicFS pulls data directly to the user from the primary path or the secondary path, depending on where the file is located.

Dynamic File Services makes your essential data readily available while storing it efficiently across a pair of paths. You decide how the files are distributed between them. By using policies, you can specify the files to be moved based on frequency of use, file name patterns, file content types, file size, and file owners. Policy enforcement is automated with scheduled and on-demand policy runs. You can also specify a list of files or folders to use for a one-time move between the two paths.

Dynamic File Services allows you to seamlessly tier files between high-performance and lower-performance storage devices. For example, you can establish policies that keep frequently used or mission-critical data on high-performance storage devices, and move seldom-used or less-essential data to lower-performance devices.

File backup can be performed separately on the two paths. This allows for different backup schedules. It can also help narrow the time window needed for backing up critical data.

- Section 1.1, "Benefits of Dynamic File Services," on page 13
- Section 1.2, "Deployment Scenarios," on page 15
- Section 1.3, "Key Components of Dynamic File Services," on page 18

1.1 Benefits of Dynamic File Services

File-based data is growing faster, consuming more space, and being retained longer than ever before. Novell Dynamic File Services enables you to manage your unstructured data with intelligent tiering in Microsoft Active Directory and Workgroup environments.

The following benefits of Dynamic File Services illustrate how it can help reduce storage infrastructure costs, save work hours, enhance existing investments in storage hardware and software, and improve retention compliance.

- Section 1.1.1, "Store Data Efficiently," on page 14
- Section 1.1.2, "Reduce Backup Windows," on page 14
- Section 1.1.3, "Access Data Securely and Transparently," on page 14
- Section 1.1.4, "Move Data Seamlessly between the Two Paths," on page 14
- Section 1.1.5, "Run Policies Whenever You Want," on page 15

1.1.1 Store Data Efficiently

- Frequently accessed data is stored on the primary path. Its high-performance storage system ensures that users remain productive. You can define policies to move data to the secondary path based on the date the file was last accessed.

- Important data is stored on the primary path, and less-important data is stored on the secondary path. For example, if users store personal music files on the system, you can define policies that transparently move files based on their file extension or file content type to the secondary location where the cost to store the data is lower.

- Current files can be stored on the primary path, and older files that need to be maintained can be stored on the secondary path. You can relocate files based on the date last accessed or last modified.

- Files can be moved between the primary and secondary paths based on their file size. This allows you to distribute files between two disks to make the most of the storage capacity that you have.

- The secondary path can be on a remote device such as a network filer. You can take advantage of lower-cost secondary storage solutions and seamlessly expand capacity for your system without affecting users.

1.1.2 Reduce Backup Windows

- Less data needs to be scanned for the daily backup of the primary path.

- You can back up the secondary path less frequently, without affecting user access to the data they use most often.

1.1.3 Access Data Securely and Transparently

- Dynamic File Services allows users to access data for both paths via a network share on the primary path.

- The native access control for the underlying file systems manages user access to the data.

- All access to the secondary path is made via DynamicFS as if the data were located on the primary path. DynamicFS does not need to relocate the data to give the user access to data on the secondary path.

- In order to set access control on data in the pair, you should access the merged view of the data via the network share on the primary path, then set the access control for files and directories as you normally would.

1.1.4 Move Data Seamlessly between the Two Paths

- You can define policies that control what unstructured files are moved between the two paths. A single policy can move data in one direction: from the primary path to the secondary path, or from the secondary path to the primary path.

- Policy rules are based on the file size, last accessed or modified times, filename patterns, and file content type.

- You can apply a policy to multiple pairs.

- You can apply multiple policies to a pair.

- You can define one-time moves of files or folders between the two paths.
- You can use policies and one-time moves to help migrate data to new storage with minimal end-user impact.

1.1.5 Run Policies Whenever You Want

- Every policy runs independently and has its own schedule. A policy's schedule applies to all pairs associated with it.
- You can run a single policy at a time on a pair to enforce its rules for moving data. A file is moved if it meets all of the filter options specified in the rule.
- You can configure multiple policies to run at the same time on a pair to enforce alternative rules for moving data. A file is moved if it satisfies the rules in any one of the concurrently scheduled policies.
- You can schedule the window of time when you want a policy to run by specifying the start time and duration of the run.
- You can schedule a policy to run hourly, daily, weekly, or monthly.
- You can start and stop policies manually. Scheduled and unscheduled policies can be run manually for one or more of their associated pairs.

1.2 Deployment Scenarios

Novell Dynamic File Services can help solve key storage problems. The scenarios in this section are intended as examples. They represent only a small sample of ways that DynamicFS can be applied in your environment.

1.2.1 Students: Essential versus Non-Essential Files

Abraham works for a large university system with thousands of students each semester. Students have home directories to use as a central storage location for their personal files and homework. The storage device is nearing capacity. Abraham needs to expand capacity for students without disrupting access to their essential academic files.

Understanding the Data

The student home directories contain numerous media files for music and photos that consume large portions of the available storage. The files have a variety of file extensions. For some files, the file extensions might not match their true content type.

The Dynamic File Services Solution

Abraham creates a Dynamic File Services pair on the server where the primary path is a folder that contains all user home directories. As the secondary path in the pair, he uses a UNC path on a remote filer storage device. He creates a policy that moves files based on their file types from the primary path to the secondary path every night between 2:00 a.m. to 4:00 a.m. Abraham specifies the file types as audio, video, and images so that a broad range of music and photo file types are moved based on their content type rather than on the file extensions.

Relocating the media files helps free the needed space on the primary path while allowing users to access their media files via a merged view of the data. Users are not aware of the physical location of their files.

1.2.2 Healthcare: Active versus Historical Files

Joe works for a research hospital that recently completed a multiple-year effort to digitize its patient records from 1900 to the present. Joe wants to assure that there is sufficient storage capacity for the current and future patient records while still making the older records available to researchers in the hospital and its affiliated university.

- ◆ "Understanding the Data" on page 16
- ◆ "The Dynamic File Services Solution" on page 16

Understanding the Data

The patient records are generated in the regular course of health care delivery. The individual patient files contain a broad spectrum of documents, including patient histories, diagnostic test results, inpatient and outpatient notes, operative notes, discharge summaries, follow-up reports, patient photographs, medical drawings, graphs, and treatment-related correspondence.

Since 1975, all patient records from the hospital's specialty clinics and units are merged in a centralized record-keeping system. Prior to 1975, each specialty clinic separately maintained its own patient record system, and the hospital units maintained their own centralized patient record system.

Current and active patient records from all specialty clinics and hospital units must be available on demand. The historical records should be available to medical researchers in the hospital and its affiliated university, but these records do not require the same immediate availability as those for the hospital's current patients.

The Dynamic File Services Solution

Joe plans a solution that is responsive to the access needs of the healthcare users to active files and of the research users for the historical files.

- ◆ "Historical Files" on page 16
- ◆ "Active Files" on page 17

Historical Files

Joe creates a Dynamic File Services pair for each of the pre-1975 records for the specialty clinics and hospital. A policy for each pair is tailored to move the largest image files daily between 12:15 a.m and 5:30 a.m. After the large files are migrated, Joe modifies the policy to move other file types

and sizes. Over time, the entire file set is migrated to the secondary location. Users are able to access the files throughout the process and afterwards without being aware of the physical location of the data.

Relocating the historical files helps free needed space on the primary storage location to allow for the growth of current and active medical records, which have a higher frequency of use and higher performance requirements. Both old and current medical records are easily available to users via a merged view of the files.

Active Files

Joe studies the current centralized patient record system to understand the types of files and their usage. Working with the medical staff, he determines that the image files that are more than a year old can be moved to a secondary storage location. He creates a Dynamic File Services pair where the secondary location is used to store the less frequently accessed images.

Joe creates a policy that moves images to the secondary location if they have not been accessed in more than one year. Initially, the policy runs daily in non-peak hours between 1:00 a.m. and 4:00 a.m. After the desired files have been relocated, Joe modifies the policy to run monthly.

Relocating the images helps free more space for the primary storage area. The reduced size of the data on the primary location helps shorten the needed backup window for weekly and incremental backups. The secondary storage area can use less expensive storage and be backed up monthly after the policy run. The users are able to access files throughout the migration process and are not aware of the physical location of the files.

1.2.3 Collaboration Applications

Hiroko works for an international marketing firm that provides employees a dynamic collaboration environment. She needs to manage the growing storage needs without disrupting the collaborative environment.

- ◆ "Understanding the Data" on page 17
- ◆ "The Dynamic File Services Solution" on page 17
- ◆ "Additional Information" on page 18

Understanding the Data

The company uses a collaboration application that allows team workspaces to be created dynamically as teams are formed to work on a variety of marketing projects. Users upload documents and images to their team sites for projects. The files are stored as unstructured data in the application's file repository.

The Dynamic File Services Solution

Hiroko studies the collaboration application's unstructured file repositories to understand the types of files and where the application stores them. She creates a Dynamic File Services pair where the primary path is the folder for the application's image file repository. She modifies the application to access the files via a network share so that the application accesses the files via a merged view of the files in the pair.

Hiroko creates a policy that moves image files to the secondary location. Thumbnail images for the files remain on the primary location. Initially, the policy runs daily in non-peak hours between 1:00 a.m. and 4:00 a.m. After most of the images have been moved, Hiroko modifies the policy to run weekly during non-peak hours.

The application accesses the files via the merged view and presents the view to users. When a user clicks a thumbnail image to open the file, the file is transparently retrieved from the secondary location and displayed in the collaboration environment. The application and the users are not aware of the physical location of the data.

This Dynamic File Services solution allows Hiroko to better control the storage environment and backup requirements for the collaboration application.

Additional Information

An example of how to set up a merged view for applications is available in Appendix B, "Setting Up a Merged View for Collaboration Applications: Novell Teaming," on page 213.

1.3 Key Components of Dynamic File Services

Novell Dynamic File Services has two major components as illustrated in Figure 1-1:

- **Management:** The Management component provides the graphical user interface and client command line tools for managing pairs and policies on DynamicFS servers.
- **Service:** The Service component provides the main engine for DynamicFS. It provides several features that enforce policies, provide users with a merged view of files, and provide utilities for configuring and controlling the Service.

Figure 1-1 *Dynamic File Services Software Components*
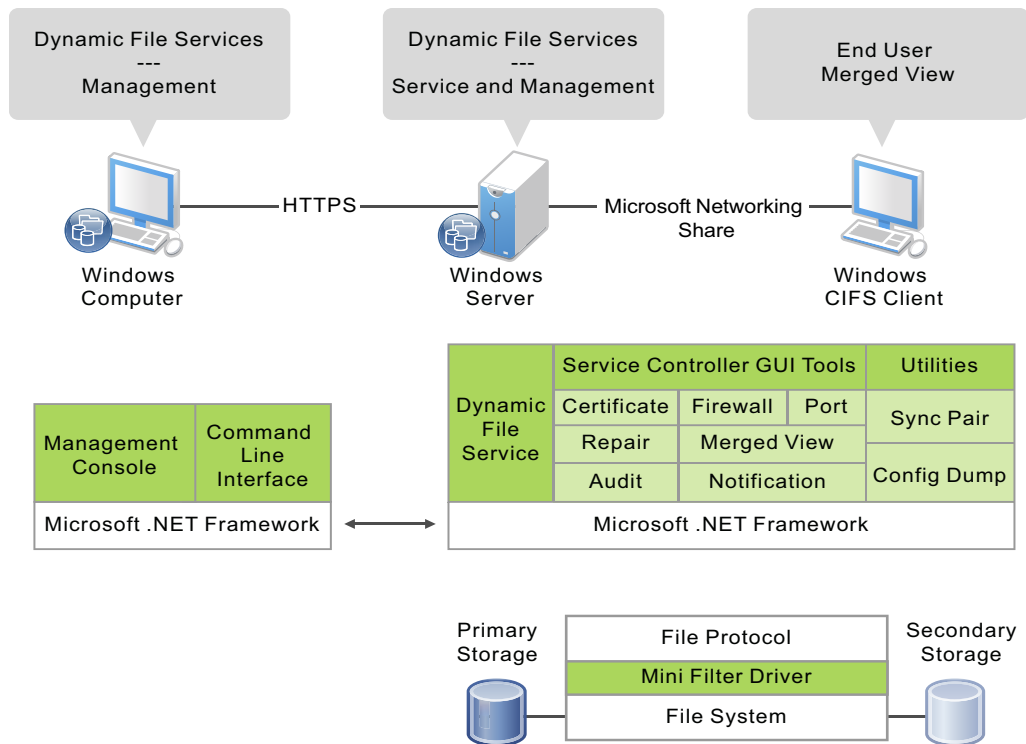
Table 1-1 describes the subcomponents that run automatically after the install.

Table 1-1   *Dynamic File Services Components That Run Automatically*

Component	Description
Dynamic File Services software	The software is installed in the `C:\Program Files\Dynamic File Services` folder by default. If the machine is a server, the path also contains the `Pairs` and `Policies` subfolders to contain configuration information about pairs and policies that you create for this server.
Service	The Dynamic File Service is the engine for all of the Dynamic File Services components. On a server, the Service automatically starts and runs in the background. You can verify that the Service is running by viewing the Service status in the Dynamic File Service Controller. You can also look for the `DswService.exe` process in the Windows Task Manager.
Service Controller	The Service Controller allows the Administrator user or users with Administrator privileges to enable, disable, or configure the Dynamic File Service or use the Repair tool. You can also launch the Management Console. The Service Controller icon (🌐) is displayed in the Windows notification area of the server desktop. It starts automatically when a user logs in to the server desktop. The application is `DswServiceController.exe`.
Filter Driver	The Filter Driver is a Windows File System filter driver that is managed by the Dynamic File Service and runs whenever the Service is running. It works with the network share on the primary path to provide a merged view to users of the files in both paths of a pair. The Filter Driver is installed in the `C:\Windows\System32\Drivers` folder and is named `dswflt.sys`.
Management Console	The Management Console is a GUI management tool that allows the Administrator user and members of the `Dynamic File Services` group to create, manage, and monitor pairs and policies. You can open the Management Console from the Install tool to immediately begin setting up pairs and policies. A shortcut to the Management Console is placed on the desktop, in the *Control Panel*, and in the *Start* menu in *Dynamic File Services > Dynamic File Services Management Console*. It launches the `DswMgmtConsole.exe` application.

Table 1-2 describes other Dynamic File Services components that run when they are called by the Service or Service Controller. Commands and utilities can be run as needed.

Table 1-2   *Dynamic File Services Components that Run As Needed*

Component	Description
Certificate Configuration	The Dynamic File Services Certificate Configuration utility automatically creates a self-signed SSL (Secure Sockets Layer) certificate during the install. The *Certificate Configuration* option in the *Service Controller* menu provides a way to create and manage the certificate after the install.
	You can also use a signed certificate that you have obtained from a certification authority. For information, see Section 6.8.5, "Configuring a Signed Certificate for Dynamic File Services," on page 88.
	Access this utility only through the *Service Controller* menu. The application is `DswCert.exe`.
CLI	The Dynamic File Services Command Line Interface (CLI) application allows you to create and manage pairs and policies on the server by issuing commands in the Windows command prompt console. The application runs only when you issue the command.
	For information, see "Dynamic File Services Client Commands for Pair and Policy Management" in the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.
	The application is `DswCLI.exe`.
Configuration Dump	The Dynamic File Services Configuration Dump utility aggregates information about the current server settings for pairs, policies, and logs, and outputs the information to a file. This tool is available to help with record keeping and troubleshooting when working with Novell Support.
	For information, see "Dynamic File Services Configuration Dump Utility" in the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.
	The application is `DswDump.exe`.
Standard Policy engine	The Standard Policy engine runs selected policies for a pair when you select *Execute Now* or when the policy is scheduled to run. It also provides an option to preview policy run results without actually moving the files.
	The Dynamic File Service controls when the Standard Policy engine runs. The application is `DswStandardPolicy.exe`.

Component	Description
File System Inventory	The Dynamic File Services File System Inventory utility automatically runs a Pair History Scan on a pair each day at 4:00 a.m. by default. It scans the pairs to gather statistics about the data stored on the primary and secondary locations, such as the file sizes, number of files, and file types.
	The time and frequency of pair history scanning is configurable. For information, see Section 8.10, "Scheduling the Pair History Scan," on page 119.
	For information on the utility, see "Dynamic File Services File System Inventory Utility" in the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.
	The Dynamic File Service controls when the File System Inventory runs. The application is `DswInventory.exe`.
Repair tool	The Dynamic File Services Repair utility can be run as needed to repair corrupted pair or policy databases by rolling back to a prior day's pair and policy definitions. DynamicFS takes a daily snapshot of the pair and policy databases. Snapshots are saved in a subfolder in the `Dynamic File Services\SnapShot` folder based on the day of the week the snapshot was taken. Each snapshot is saved for seven days until the day of the week next occurs and a new snapshot is taken.
	You can start the Repair tool from the *Service Controller* menu. The application is `DswRepair.exe`.
Synchronize Pair tool	The Dynamic File Services Synchronize Pair utility is used to detect duplicate files in the pair structure or to detect folders with attribute or ACL permission differences. It can generate reports in CSV and XML format.
	The primary and secondary locations are rarely out of synchronization. Such conditions might occur, for example, after recovering files in the two locations from backup media. For information, see Section 4.17, "Duplicate Files," on page 48.
	For information about running the utility, see "Dynamic File Services Synchronize Pair Utility" in the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.
	The application is `DswSyncPair.exe`.

What's New for Dynamic File Services

<div align="right">

2

</div>

This section describes the new features and changes for managing the service, pairs, and policies in Novell Dynamic File Services (DynamicFS) since version 1.0.

2.1 What's New for Dynamic File Services 1.6

In addition to bug fixes, Novell Dynamic File Services 1.6 provides the following new features and changes for the service, pair, and policy management:

2.1.1 Remote Shares as Secondary Paths in a Workgroup

Remote secondary paths can also be used in Workgroup environments. Dynamic File Services 1.6 supports using a remote share for the secondary path in a pair in the same Workgroup. The remote share must be defined in same Workgroup as the server that hosts the primary path. For requirements and guidelines, see Section 4.11, "Remote Shares as Secondary Paths in a Workgroup," on page 44.

2.1.2 Service Configuration Options

Dynamic File Services 1.6 includes the following new Service configuration options:

Audit Configuration

The Audit Configuration tool allows you to specify which pair and policy events should be included in the audit log. For information, see Section 6.4, "Configuring the Auditing Service," on page 74.

Notification Configuration

The Notification Configuration tool allows you to specify which pair and policy events should trigger a notification. The Email add-on to the tool allows you to configure a list of e-mail addresses to receive notifications. For information, see Section 6.5, "Configuring the Notification Service," on page 76.

Running the Repair Tool

The Repair tool must be run by a user with file system rights for all of the paths in the pair. For information, see Section 11.1.6, "Manually Repairing the Pair and Policy Database Files," on page 178.

Running the SyncPair Utility

The SyncPair utility must be run by a user with file system rights for all of the paths in the pair. The Dynamic File Service can be running or not running when you run the SyncPair utility, but policies must not be running against the pair. For information, see Section 8.11, "Reporting Conflicts for Attributes and ACL Permissions on Folders," on page 120 and Section 8.12, "Reporting Conflicts for Duplicate Files," on page 121.

For information about all options for the SyncPair utility, see see "Dynamic File Services Synchronize Pair Utility" in the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.

2.1.3 Pair Option

Dynamic File Services 1.6 includes the following new pair configuration option:

  - "Remote Share as the Secondary Path in a Pair in a Workgroup" on page 24

Remote Share as the Secondary Path in a Pair in a Workgroup

In an Workgroup environment, the Pair Wizard and Setup Wizard allow you to type the UNC (Universal Naming Convention) path of a remote share to use as the secondary path in a pair. The share must already exist and be in the same Workgroup as the server that hosts the primary path. For requirements and guidelines, see Section 4.11, "Remote Shares as Secondary Paths in a Workgroup," on page 44.

2.1.4 Policy Option

Dynamic File Services 1.6 includes the following new policy configuration option:

  - "Filter by File Owners" on page 24

Filter by File Owners

You can select the usernames of one or more file owners whose files you want to move. For information, see "File Owners" on page 127.

2.2 What's New for Dynamic File Services 1.5

In addition to bug fixes, the initial release of Novell Dynamic File Services 1.5 provides the following new features and changes for the service, pair, and policy management:

- Section 2.2.1, "Remote Shares as Secondary Paths," on page 25
- Section 2.2.2, "Security Features for Remote Shares," on page 25
- Section 2.2.3, "Service Configuration Options," on page 25
- Section 2.2.4, "Pair Options," on page 26
- Section 2.2.5, "Policy Options," on page 26
- Section 2.2.6, "Audit Log," on page 27
- Section 2.2.7, "Event IDs," on page 27
- Section 2.2.8, "Cloud-Based iSCSI Targets," on page 27
- Section 2.2.9, "Collaboration Applications," on page 27
- Section 2.2.10, "Commands and Utilities," on page 27
- Section 2.2.11, "Installation," on page 27

2.2.1 Remote Shares as Secondary Paths

In Active Directory environments, Dynamic File Services 1.5 supports using remote shares for the secondary path in a pair. The share must be published in Active Directory. For requirements and guidelines, see Section 4.10, "Remote Shares as Secondary Paths in an Active Directory Domain," on page 43.

2.2.2 Security Features for Remote Shares

In an Active Directory environment, Dynamic File Services creates a domain group called Dynamic File Services Storage Rights and a domain user called NDFS-*servername*. These new security features were added to support the use of remote shares as secondary paths in a pair. For information, see Section 4.2.1, "Default Domain Configuration," on page 38.

2.2.3 Service Configuration Options

Dynamic File Services 1.5 includes the following new Service configuration options:

- "Merged View Access Control" on page 25
- "Log Level Settings for Service and Enforcer Logs" on page 26

Merged View Access Control

In the Service Controller menu, the *Merged View Access* option allows you to enable (the default) or disable the merged view of data in pairs on a server basis. When the merged view is disabled, users see only the data that resides on the primary path in a pair. Previously, the merged view could not be disabled. For information, see Section 6.9, "Configuring the Merged View Access," on page 91.

Log Level Settings for Service and Enforcer Logs

In the Server Properties dialog box, the *Logging options* page allows you to set the logging levels for the Service and Enforcer logs. Previously, logging levels could be modified only by editing the settings in the log configuration files. For information, see Section 6.10, "Configuring the Logging Level for the Service and Standard Policy Log Files," on page 92.

2.2.4 Pair Options

Dynamic File Services 1.5 includes the following new pair configuration options:

- ◆ "Remote Share as a Secondary Path in a Pair in a Domain" on page 26
- ◆ "Move Files and Folders" on page 26

Remote Share as a Secondary Path in a Pair in a Domain

In an Active Directory environment, the Pair Wizard and Setup Wizard allow you to specify the UNC (Universal Naming Convention) path of a remote share as the secondary path in a pair, or you can browse to select the remote share. The shares must already exist and be published in Active Directory. For requirements and guidelines for using remote shares, see Section 4.10, "Remote Shares as Secondary Paths in an Active Directory Domain," on page 43.

Move Files and Folders

Dynamic File Services 1.5 allows you to browse to select folders and files to be moved between paths in a pair as a one-time move event. For information, see Section 8.9, "Moving Selected Files or Folders," on page 118.

2.2.5 Policy Options

Dynamic File Services 1.5 includes the following new policy configuration options:

- ◆ "Yearly Schedule Option" on page 26
- ◆ "Filter by File Patterns" on page 26
- ◆ "Filter by File Types" on page 26

Yearly Schedule Option

You can specify a policy run frequency of *Yearly* in a policy schedule. For information, see Yearly in Table 9-4, "Policy Schedule Options," on page 128.

Filter by File Patterns

You can specify file patterns for filenames as a filter option in policies. File patterns include file extensions and regular expressions. Previously, you could specify only file extensions. For information, see "File Patterns" on page 125.

Filter by File Types

You can select one or more file types as a filter option. The file types are based on the content types (standard MIME types) of applications that are installed on the server. For information, see "File Types" on page 126.

2.2.6 Audit Log

Dynamic File Services 1.5 automatically ensures that the Audit log contains well-formed XML. For information, see Section 10.9.2, "Detecting and Resolving a Corrupted Audit Log," on page 170.

2.2.7 Event IDs

Dynamic File Services 1.5 provides Event IDs for events reported in the Microsoft Event Viewer. For information, see Section 12.10, "How do I find event ID information?," on page 187.

2.2.8 Cloud-Based iSCSI Targets

Dynamic File Services 1.5 supports the use of cloud-based iSCSI targets as the secondary location in a pair. For information about using secondary storage in a cloud environment, see Appendix A, "Using iSCSI Targets in a Cloud Storage Environment," on page 199.

2.2.9 Collaboration Applications

Dynamic File Services 1.5 supports using pairs and policies to manage unstructured file repositories for collaboration applications. For general guidelines and an example for using pairs and policies for Novell Teaming, see Appendix B, "Setting Up a Merged View for Collaboration Applications: Novell Teaming," on page 213.

2.2.10 Commands and Utilities

For information about new features and changes for the client commands and utilities, see "What's New for the Dynamic File Services Client CLI and Utilities" in the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.

2.2.11 Installation

For information about new features and changes in the installation tool, see "What's New for the Dynamic File Services Installation" in the *Dynamic File Services 1.6 Installation Guide*.

Getting Started

3

Novell Dynamic File Services (DynamicFS) is a powerful and dependable tool to help you effectively manage your storage. Getting started is easy! This section describes common tasks to help you quickly set up and use DynamicFS.

3.1 Installing and Setting Up Dynamic File Services

The Dynamic File Service and the Management Console are installed on the servers where you want to create pairs and policies. You can also install the Management Console on workstations. You can manage the pairs and policies on multiple servers from any computer where the Management Console is installed.

Dynamic File Services
Software

Service
and
Management Console

Management
Console
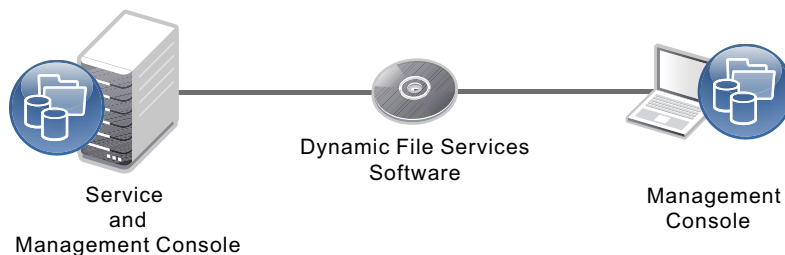
The Dynamic File Service controls the pairs and policies that you create on a server. After the install or after a server reboots, the Service automatically starts and runs in the background. Each server's pairs and policies are unique on the server, and their related configuration files are stored locally.

The `Dynamic File Services` group is created when the Service is installed, but no members are automatically assigned to it. Before you can manage DynamicFS, you must log in to the DynamicFS server as a user with Administrator privileges (server Administrator, Domain Admin, or a user with equivalent privileges) to add members to the `Dynamic File Services` group. Only the Administrator user and members of the `Dynamic File Services` group can manage the Service.

On DynamicFS servers, the Service Controller starts automatically when the Administrator user or a member of the `Dynamic File Services` group logs in. The Service Controller allows you to manually start and stop the Dynamic File Service and manage its settings, such as the Service Port Access, the Windows Firewall Access, the Certificate Configuration, and the Merged View Access. You can also use it to launch the Management Console or launch the Repair tool.

3.2 Connecting to the Dynamic File Services Server

Open the Dynamic File Services Management Console, then set up the server you want to manage. You can set up multiple servers to be managed in the same console. To connect to a server, provide the login credentials of the Administrator user or a member of the `Dynamic File Services` group on the target server.

You can run the Management Console on the server, or from another computer where the Management Console is installed. For remote connections, the Dynamic File Services *Windows Firewall Access* option must be enabled on the target server so that an exception in the Windows Firewall is allowed for the configured Dynamic File Service port. Remote management communications are secured with SSL.
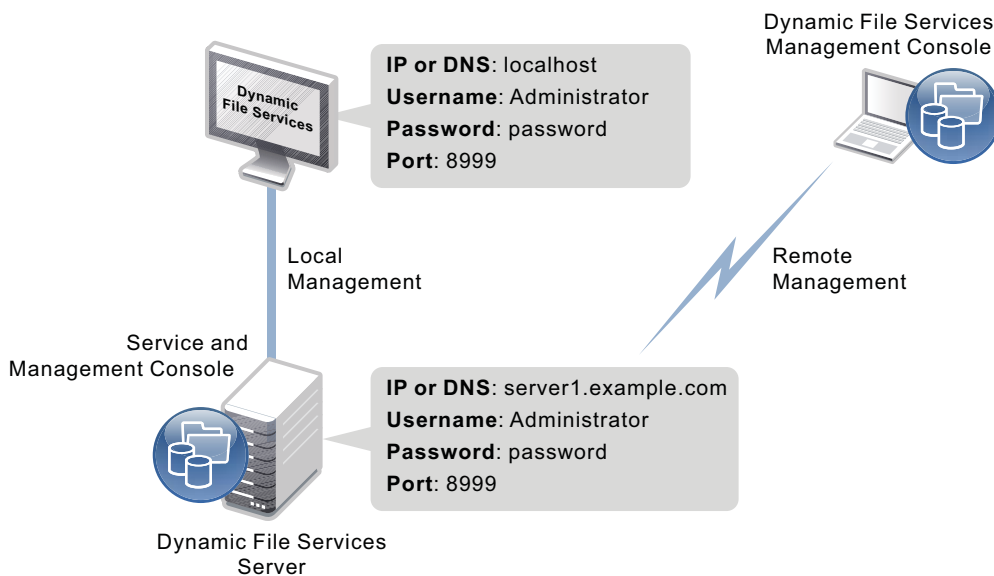
3.3 Creating a Dynamic File Services Pair

A Dynamic File Services pair consists of two independent paths on the same or different disks, referred to as the primary path and secondary path. You can use a remote share as the secondary path. Paths can contain files or be empty. Pair names must be unique on the server.

Create a pair on the server by specifying the primary path and the secondary path to use for the pair. If no pairs exist on the target server, the Setup Wizard automatically opens and guides you through the process of creating a pair and creating a policy. The wizard automatically associates the pair and the policy. Other pairs can be created with the Pair Wizard.

After you create a pair, you can specify folders in the primary location that can be included or excluded from policy runs. You can include folders or exclude folders, but not both.

A Windows network share must be set up on the primary path so that users can access data on the pair in a merged view. Use the Windows Network Sharing feature to set up the network share before or after you create the pair. The merged view is also shown if you nest other network shares above and below the share on the primary path. Do not create a network share on the secondary path.
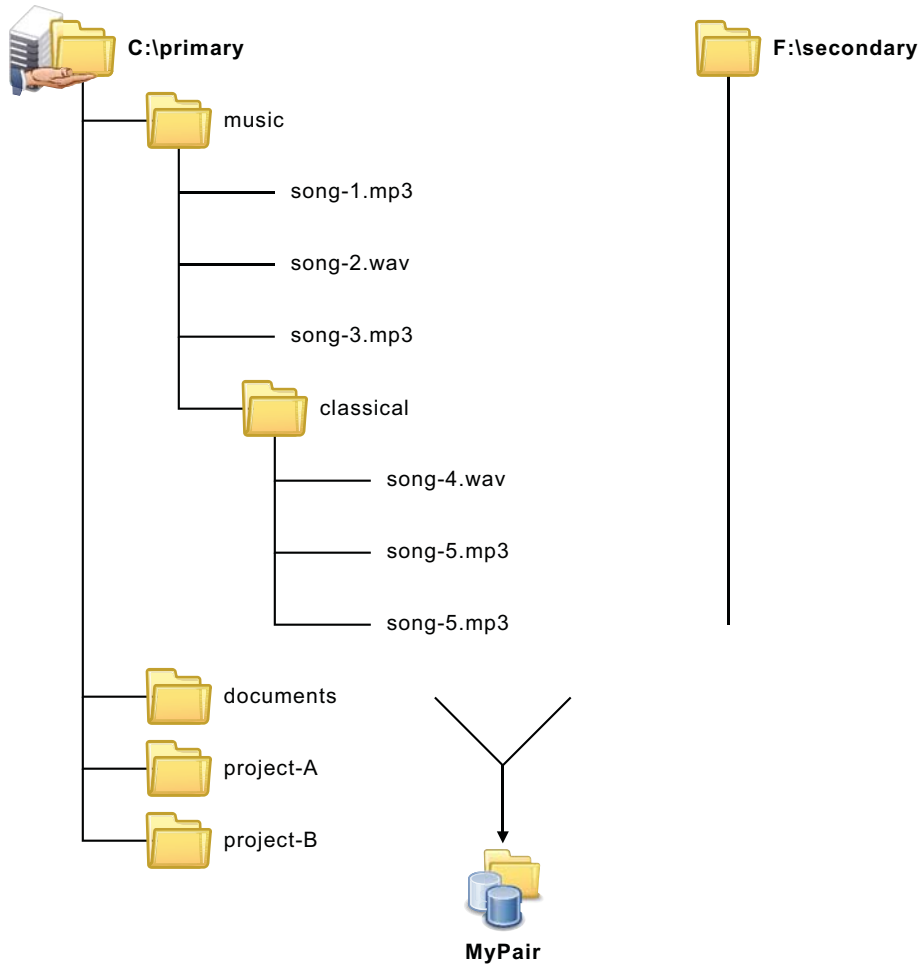
Primary Path: Path on a local drive.

Secondary Path: Path on a different local drive or a remote share.
Typically, this is an empty directory.

 IMPORTANT: Do not nest paths used in the same or different pairs.

Pair Name: Give the pair a unique name.

3.4 Creating a Policy

A policy specifies the rules that determine what files are moved between the primary path and the secondary path, the direction files are moved, and when the policy is enforced.

Create a policy that determines what data to move and when to move it. A rule defines the direction to move files and at least one of the following filter options:

- File size
- Last accessed time
- Last modified time
- File patterns
- File types
- File owners

A policy can have no schedule, or it can be scheduled to run hourly, daily, weekly, monthly, or yearly. Scheduled and unscheduled policies can be run manually.

If no pairs exist on the target server, the Setup Wizard automatically opens and guides you through the process of creating a pair and creating a policy. The wizard automatically associates the pair and the policy. Other policies can be created with the Policy Wizard. Policy names must be unique on the server.

MyPolicy

Direction: Move files that meet the filter criteria from Primary to Secondary, or move them from Secondary to Primary.

Filter: Set one or more filter options to specify which files to move.

Filters set in the same policy are "AND" operations. A file is moved only if it meets all of the criteria in the policy.

Filters set in separate policies that run at the same time are "OR" operations. A file is moved if it meets the criteria in any one of the policies.

Schedule: Set when to run the policy. Policy runs can also be started manually.

Policy Name: Give the policy a unique name.

Description: If desired, summarize the policy characteristics and its purpose.

3.5 Associating the Pair and Policy

An association links a Dynamic File Services pair and policy so that the policy is enforced for the pair. No files are moved between the primary path and secondary path in a pair until a policy is associated with the pair. Policy runs are enforced against all pairs that are associated with the policy.

An association between a policy and a pair occurs automatically when you use the Setup Wizard to create a pair and a policy at the same time. The Policy Wizard allows you to select the pairs you want to associate with a new policy. The Pair Wizard allows you to select the policies you want to associate with a new pair. You can also associate (or disassociate) pairs and policies at any time by selecting the Properties dialog box of the pair or policy, and modifying its associations.

MyPair   **MyPolicy**

3.6 Creating More Policies and Pairs

You can create additional Dynamic File Services pairs and policies and associate them. A pair can be associated with multiple policies. A policy can be associated with multiple pairs.

Associate one or more policies
with a given pair.

Associate one or more pairs
with a given policy.
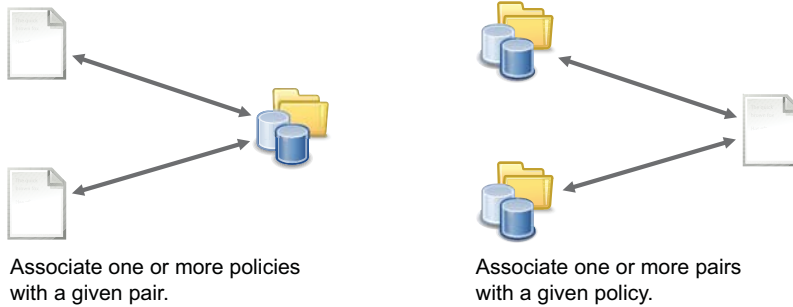
Use any of the following methods to create additional pairs and policies and associate them:

 ◆ **Pair:** Right-click *Pairs* under the server in the left panel, then select *Pair Wizard*.
 ◆ **Policy:** Right-click *Policies* under the server in the left panel, then select *Policy Wizard*.
 ◆ **Pair and Policy:** Right-click the server in the left panel, then select *Setup Wizard*.

Use either of the following methods to associate existing pairs and policies:

 ◆ Select a policy and associate it to one or more pairs.
 ◆ Select a pair and associate it to one or more policies.

3.7 Enforcing Policies

In a policy run, a policy is enforced separately for each of the pairs associated with the policy. A policy can run on demand or when it is scheduled. Each policy has its own schedule, but multiple policies can be scheduled to run at the same time. Scheduled and unscheduled policies can be run manually.

Run a single policy at a time on a pair to enforce the policy's rules for moving data. A file is moved if it meets all of the filter options specified in the rule.

Configure multiple policies to run at the same time on a pair to enforce alternative rules for moving data. When the group of policies moves files in both directions, the primary-to-secondary policies are grouped and enforced, then the secondary-to-primary policies are grouped and enforced. A file is moved if it meets the rules for any one of the policies that are run together.

For example, a policy might move all files with extensions of `.mp3` from the primary location to the secondary location.

Example: Move *.mp3 files from Primary → Secondary.
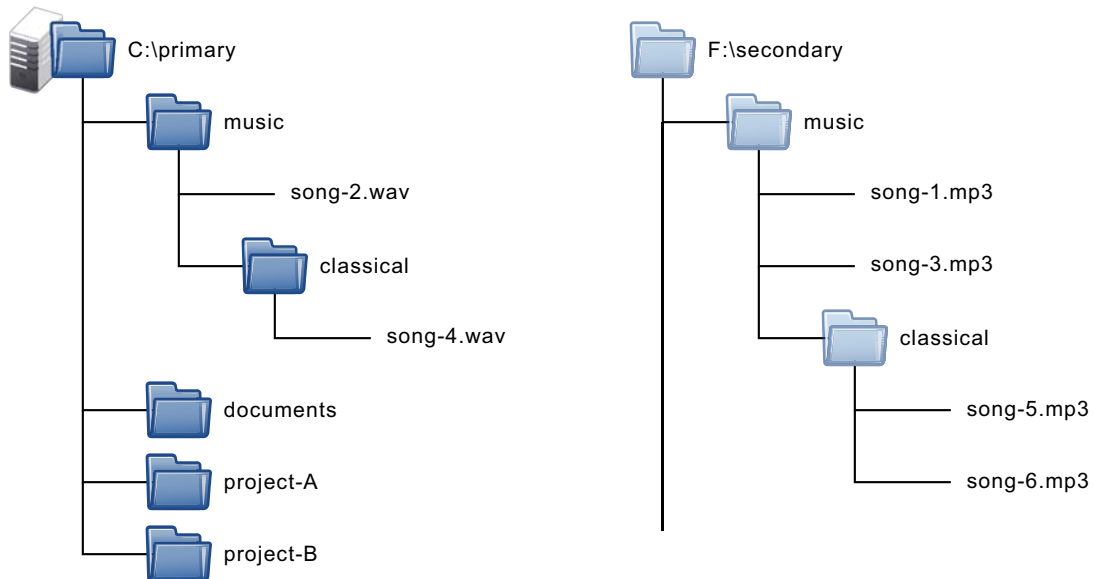
3.8 Viewing the Merged File Tree for a Pair

Users access the primary path on the Dynamic File Services pair via a network share (*servername**sharename*) to get a merged view of the data on the pair. Users see files on the primary and secondary locations as if the files are all stored on a single device.

The native access control of the underlying file systems controls user access to the data. All access to the secondary path is made via DynamicFS as if the data were located on the primary path. DynamicFS does not need to relocate the data to give the user access to data on the secondary path.

To set ACLs and attributes on files and folders, you should access the merged view of the data via the network share on the primary path, then set the access control for files and folders as you normally would. If direct access to the path is necessary to set ACLs, make the changes to the folder instance that resides on the primary path.

In a merged view, the users are not aware that the .mp3 files are now located on a different disk than their other files. There is no performance impact for the user.
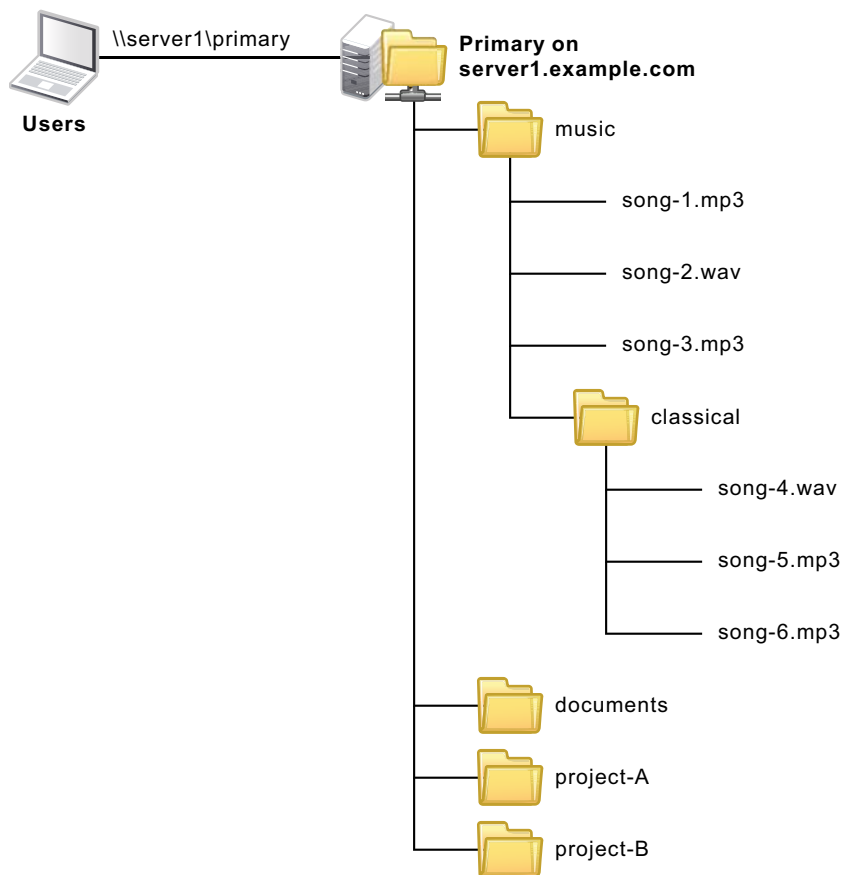
3.9 Backing Up Files in the Pair

The administrator can perform backup and restore operations independently on the two locations in the Dynamic File Services pair. Backups can be scheduled to run at different frequencies on each path. Having less data to back up can help shorten the backup window.

For example, if data changes more frequently on the primary path, it can be backed up more frequently than the secondary path.

The primary location contains frequently used and volatile files, so it is backed up incrementally and weekly.

The secondary location contains static or less important files, so it is backed up less often.

C:\primary
  music
    song-2.wav
    classical
      song-4.wav
  documents
  project-A
  project-B

F:\secondary
  music
    song-1.mp3
    song-3.mp3
    classical
      song-5.mp3
      song-6.mp3
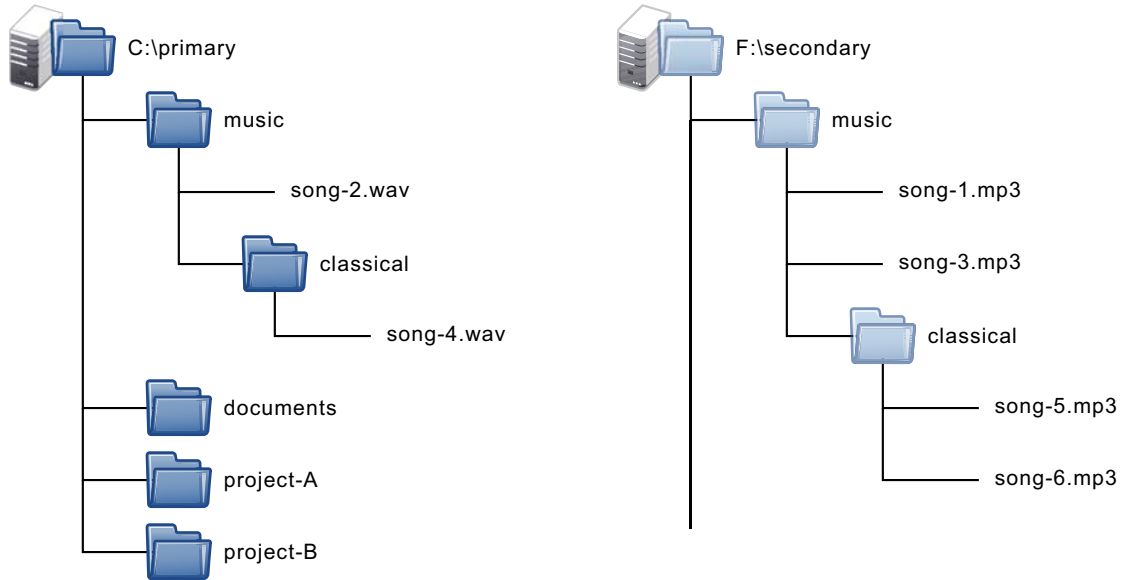
Planning for Pairs and Policies

4

Novell Dynamic File Services (DynamicFS) pairs and policies are easy to set up and manage. Before you begin, it is important to take time to plan and design your overall storage solution. This section provides information to help you plan an effective implementation in your Windows environment.

IMPORTANT: For information about supported configurations and installation requirements, see "Planning the Installation" in the *Dynamic File Services 1.6 Installation Guide*.

4.1 Dynamic File Services Group

The `Dynamic File Services` group controls which users are allowed to create and manage pairs and policies on the Dynamic File Services server. The group is created automatically during the installation of the Service component. The `Dynamic File Services` group has no default members. Only local users with Administrator privileges on the server, a domain user with Domain Admin privileges in an Active Directory Domain, and members of the `Dynamic File Services` group can create and manage pairs and policies on the server.

In a workgroup environment, the Administrator user or any user with Administrator privileges can add or remove usernames as members of the `Dynamic File Services` group. It is not necessary to explicitly add the Administrator user to the group, but you can add it. Administrator privileges are not required to be a member.

In an Active Directory domain environment, any user with Domain Admin privileges can add or remove usernames as members of the `Dynamic File Services` group. It is not necessary to explicitly add a Domain Admin user to the group, but you can add it. Domain Admin privileges are not required to be a member.

For information about how to add members to the `Dynamic File Services` group, see Section 6.2, "Configuring Administrators for Pair and Policy Management," on page 69.

4.2 Active Directory Domain Configuration for Dynamic File Services

In an Active Directory environment, Dynamic File Services configures a special domain group and user in order to support the use of remote shares as the secondary location in a pair.

- Section 4.2.1, "Default Domain Configuration," on page 38
- Section 4.2.2, "Dynamic File Services Storage Rights Domain Group," on page 39
- Section 4.2.3, "NDFS-servername Domain Proxy User," on page 40
- Section 4.2.4, "Security Implications of the Default Domain Configuration," on page 40

4.2.1 Default Domain Configuration

When you install the Service component on a domain controller or member server in an Active Directory environment, the installation sets up the following security features:

- Creates a domain user called `NDFS-servername`.
- Creates a domain group called Dynamic File Services Storage Rights (`DFSStorageRights`).
- Adds the `NDFS-servername` user to the `DFSStorageRights` group.
- Gives the `NDFS-servername` user the *Log on as a service* right.
- Sets up the Dynamic File Service to log on as the `NDFS-<servername>` user.
- Makes the `DFSStorageRights` group a Member of the `Domain Admins` group.

This setup requires that the installation to be done by a domain user that has local Administrator privileges and domain Administrator rights.

4.2.2 Dynamic File Services Storage Rights Domain Group

The Dynamic File Services Storage Rights (`DFSStorageRights`) group is an Active Directory domain group that is used for remote shares to allow Dynamic File Services to manage traffic between the Service running on the server and the remote share. Before you use a remote share in a pair, you must add the `DFSStorageRights` group to the remote share in Active Directory, and grant it all permissions to the share.

The `DFSStorageRights` group is created automatically during the installation of the Service component if the computer is a domain controller or a member server in an Active Directory environment. The group scope is *Global* and the group type is *Security*.
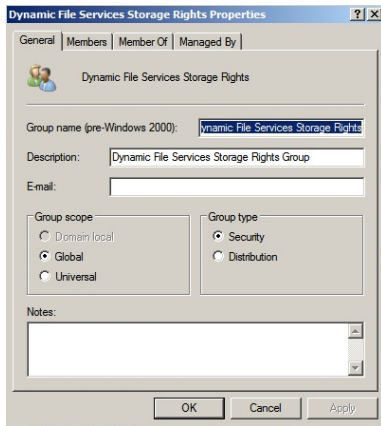
Members of the `DFSStorageRights` group include the `NDFS-servername` proxy users for the Dynamic File Services servers in the same Active Directory domain/forest. The members are automatically added to the group when the Service component is installed on a server in the domain.
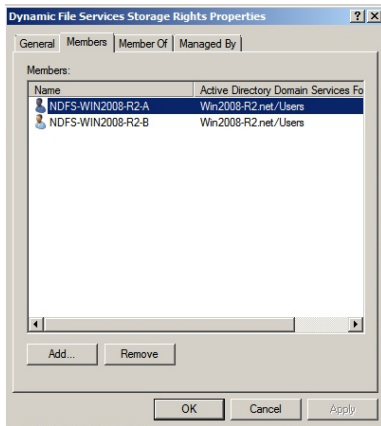
A server's `NDFS-servername` proxy user is automatically removed as a member of the `DFSStorageRights` group if Dynamic File Services is uninstalled from the server. The group is not deleted by the uninstall unless the server's proxy user is the only member of the group.

The `DFSStorageRights` group is a member of the `Domain Admins` group. This gives the `DFSStorageRights` group equivalent rights to the `Domain Admins` group. Alternatives to the default domain configuration are described in "Security Implications of the Default Domain Configuration" on page 40.
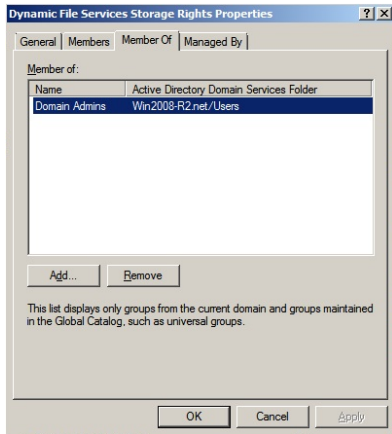
4.2.3 NDFS-*servername* Domain Proxy User

The `NDFS-servername` user is an Active Directory domain user that serves as a proxy user in communications between the Service on a server that is running Dynamic File Services and a remote share that is being used as the secondary path in a pair on that server. The user is created automatically during the installation of the Service component if the computer is a domain controller or a member server in an Active Directory environment.

The `NDFS-servername` proxy user is automatically added as a member of the Dynamic File Services Storage Rights (`DFSStorageRights`) group in the same domain as the server. The user is given the *Log on as a service* right.

The password for the `NDFS-servername` user is created automatically, and can be modified by using the Active Directory tool for modifying user passwords.

4.2.4 Security Implications of the Default Domain Configuration

The default configuration gives the Dynamic File Services Storage Rights (`DFSStorageRights`) group equivalent rights to the `Domain Admins` group. In some situations, this can be undesirable. The following describes two options to tighten security:

- Remove the Dynamic File Services Storage Rights group from the `Domain Admins` group, and give only the specific rights needed to the Dynamic File Services Storage Rights group.
- Delete the Dynamic File Services Storage Rights group, and add only the specific rights needed directly to the `NDFS-servername` proxy user. Then give the `NDFS-servername` user share-level rights or the NTFS security rights to the remote share used as the secondary path.

You can manage domain groups and users by using the Active Directory Users and Computers snap-in the Microsoft Management Console.

The specific rights needed are as follows:

- Allow log on locally
- Restore file and directories
- Backup files and directories
- Load and unload device drivers
- Log on as a service
- Manage auditing and security log
- Take ownership of files or other objects

4.3 Server-Centric Pair and Policy Configuration

The management of Dynamic File Services servers, pairs, and policies is server-centric rather than being managed through a centralized LDAP directory repository. The pair and policy configuration files are stored in subfolders in the `Dynamic File Services` folder on the server where the Service is installed and running. Import and export features of DynamicFS make it possible to copy a policy to multiple servers.

The Service login can validate administrator user identity in Workgroup environments and in Active Directory domain environments.

4.4 Dynamic File Services Pairs

A Dynamic File Services pair consist of a primary location and a secondary location that DynamicFS manages as a unit. It supports up to 16 pairs per server.

Before forming a pair, make sure you have prepared the storage areas that you want to use as the primary and secondary locations by verifying that your storage setup meets the following requirements. Then gather the information you need about the paths that you want to use as the primary path and secondary path.

- Local drives must be mounted and appear as native local drives. Local drives must have a static drive letter assigned to them so that the letters remain the same on server reboots. If you plan to change the drive letters (or modify paths), you must unlink the paths by removing the pair definition, and create a new pair that uses the new locations.
- The devices must be online and available to the server where you want to create the pair.

  For information, see Section 4.5, "Supported Devices," on page 42.
- UNC paths on remote storage can be used as a secondary location. Users should not have direct access to the shared folder on a secondary location. For requirements and guidelines, see Section 4.10, "Remote Shares as Secondary Paths in an Active Directory Domain," on page 43.

  Remote shares must be published in Active Directory in order to be used as the secondary path. For information, see Section 8.3, "Preparing Remote Shares for Use in a Pair," on page 112.
- You must have the access permissions and credentials necessary on the paths you specify for the pair.
- Pairs cannot be nested. The paths you use as the primary location and secondary location must not be nested above or below any other paths that are used in the same or different pair.

- Usually, the secondary path is empty when you create a pair. Both paths can contain data, but if there are duplicate files, only the instance of the file in the primary path is available to the user. As an Administrator user (or as a user with Administrator privileges) on the server, you can access the secondary path to rename the duplicate file, which makes it available to users in the merged view.

- All user access to the pair must be made through a network share on the primary path that you create.

  - You can add network shares on the primary device above or below the network share on the primary path. The merged view works from the primary path and downward in the file tree structure.

  - Do not give users direct access to the secondary path and to any shares on, above, or below the secondary path.

4.5 Supported Devices

Devices that the system considers to be native storage devices can be used for the primary path and secondary path. This includes Fibre Channel, iSCSI, and direct-attached storage devices (internal or external).

For iSCSI devices that are hosted in a cloud, we recommend that the device be used only for secondary paths.

The native storage devices used in a pair must have a static drive letter assigned so that the drive letter remains the same through server reboots. If you plan to change the drive letters (or modify paths), you must unlink the paths by removing the pair definition, and create a new pair that uses the new locations.

DynamicFS does not support using CDs, DVDs, floppy drives, or flash drives in a pair. It also does not support using mapped drives.

In an Active Directory environment, a remote share can be used as a secondary path. For requirements, see Section 4.10, "Remote Shares as Secondary Paths in an Active Directory Domain," on page 43.

4.6 Supported File Systems

Dynamic File Services supports the NTFS file system for the primary and secondary locations.

4.7 SMB

Dynamic File Services supports SMB2 and SMB1.

4.8 UTF-8

The servers and filers used with Dynamic File Services must be Unicode capable and set up for UTF-8 (8-bit Unicode Transformation Format) encoding and character sets.

4.9 Primary and Secondary Paths

The paths you use as the primary location and secondary location in a Dynamic File Services pair must not be nested above or below any other paths used in the same or different pair.

4.10 Remote Shares as Secondary Paths in an Active Directory Domain

You can specify UNC (Universal Naming Convention) paths as the secondary location in a pair in an Active Directory domain. This allows a secondary storage target to be a remote share on third-party network filers (such as EMC and NetApp) or Windows Server 2003/2003 R2/2008/2008 R2 servers. The remote share must be published in the same Active Directory domain as the server that hosts the primary pair.

A UNC path describes the location of a volume or folder. The format for a UNC path is `\\server\volume\folder` and is case-sensitive. For example:

`\\my_iscsi_svr1\Engineering\ProjectA`

Make sure your setup meets the requirements in the following sections:

- Section 4.10.1, "Installation Requirements for Using Remote Shares in a Domain," on page 43
- Section 4.10.2, "Configuration Requirements for Using Remote Shares in a Domain," on page 43

4.10.1 Installation Requirements for Using Remote Shares in a Domain

Install Dynamic File Services on a supported Windows server in an Active Directory domain. The server can be a domain controller or a member server.

The installation must be done by an Active Directory domain user that has Administrator rights. This allows the Installation Wizard to create the `Dynamic File Services` group, the `NDFS-servername` proxy user, and the `Dynamic File Services Storage Rights` group in Active Directory. To add members to this group, see Section 6.2.2, "Setting Up Administrators in a Domain," on page 71.

4.10.2 Configuration Requirements for Using Remote Shares in a Domain

Before you can use a remote share as a secondary location, your system must meet the following requirements:

- "Primary Path Requirements" on page 43
- "Remote Secondary Path Requirements" on page 44

Primary Path Requirements

- The server hosting the primary path and running Dynamic File Services must be a supported Windows server in an Active Directory environment. The server can be a domain controller or a member server.

For information, see "Supported Platforms" in the *Dynamic File Services 1.6 Installation Guide*.

 * The primary path must be on a local device (direct-attached, Fibre Channel, or iSCSI).

 * Users access data on the pair via a network share on the primary path.

 * Users must be given share permissions or NTFS security rights to access the primary path.

Remote Secondary Path Requirements

 * The Secondary path must be a remote share that resides in one of the following locations in the same domain as the primary server. It is not required that the secondary Windows server be running Dynamic File Services.

   * Windows Server 2008 R2 server

   * Windows Server 2008 Service Pack 2 server

   * Windows Server 2003 R2 server

   * Windows Server 2003 Service Pack 2 server

   * Network attached storage or a network filer (such as NetApp and EMC)

 * The secondary storage must be hosted in the same Active Directory domain/forest as the Dynamic File Services server.

 * To avoid potential data loss and conflicts, use only dedicated volumes when using UNC paths.

 * You must publish the remote share in Active Directory.

   The remote share can be published in any container where the `NDFS-<servername>` proxy user or `Dynamic File Services Storage Rights` group has browse rights.

   Use Microsoft Networking to create a share on the remote secondary location, and then publish the remote share in Active Directory. For information, see Section 8.3, "Preparing Remote Shares for Use in a Pair," on page 112.

 * Add the `Dynamic File Services Storage Rights` group as a user of the remote share and grant the group all permissions. Set up permissions on the share and the NTFS file system.

 * Users must not have direct access to the remote share or to the path used for the share.

4.11 Remote Shares as Secondary Paths in a Workgroup

You can specify UNC (Universal Naming Convention) paths as the secondary location in a pair in a Workgroup. This allows a secondary storage target to be a remote share on third-party network filers (such as EMC and NetApp) or Windows Server 2003/2003 R2/2008/2008 R2 servers. The remote share must be created in the same Workgroup as the server that hosts the primary pair.

A UNC path describes the location of a volume or folder. The format for a UNC path is `\\server\volume\folder` and is case-sensitive. For example:

`\\my_iscsi_svr1\Engineering\ProjectA`

Make sure your setup meets the requirements in the following sections:

- Section 4.11.1, "Installation Requirements for Using Remote Shares in a Workgroup," on page 45
- Section 4.11.2, "Configuration Requirements for Using Remote Shares in a Workgroup," on page 45

4.11.1 Installation Requirements for Using Remote Shares in a Workgroup

Install Dynamic File Services on a supported Windows server in a Workgroup.

The installation must be done by a user that has Administrator rights on the server. This allows the Installation Wizard to create the `Dynamic File Services` group. To add members to this group, see Section 6.2.3, "Setting Up Administrators in a Workgroup," on page 72.

4.11.2 Configuration Requirements for Using Remote Shares in a Workgroup

Before you can use a remote share as a secondary location in a Workgroup, your system must meet the following requirements:

- "Workgroup Requirements" on page 45
- "Primary Path Requirements" on page 46
- "Remote Secondary Path Requirements" on page 46

Workgroup Requirements

- The computer that runs Dynamic File Services and hosts the primary path must be in the same Workgroup as the computer or filer that hosts the secondary path.
- The hostname of each computer in the Workgroup must be unique.
- The Service must be run as the Administrator user. The Administrator user password must be set the same on each participating computer or filer. This user must have all file system rights to the primary share and the secondary share.

  On a Windows XP computer, all computers in the workgroup must have the same user account with the same password. The user account must have all share access rights to all of the shares that you plan to use. The Service must run as this user account. The user must be granted the Logon as a Service Right. If you set the service to run as a user, then the Windows service controller set this right for you.

- On Windows 2008 and 2008 R2, the following services must be running and be configured to start for every boot in order for Dynamic File Services to work with remote secondary paths:

    - Function Discovery Resource Publication
    - Simple Service Discovery Protocol (SSDP)
    - Universal Plug and Play (UPnP)
    - Computer Browser

  After these services are started, go to the *Control Panel > Network and Internet > Network and Sharing Center > Sharing and Discovery* option, then turn on *Network Discovery*.

Primary Path Requirements

- The server hosting the primary path and running Dynamic File Services must be a supported Windows server in the Workgroup.

  For information, see "Supported Platforms" in the *Dynamic File Services 1.6 Installation Guide*.

- The primary path must be on a local device (direct-attached, Fibre Channel, or iSCSI).

- Users access data on the pair via a network share on the primary path.

- Users must be given share permissions or NTFS security rights to access the primary path.

Remote Secondary Path Requirements

- The Secondary path must be a remote share that resides in one of the following locations in the same Workgroup as the primary server. It is not required that the secondary Windows server be running Dynamic File Services.

  - Windows Server 2008 R2 server

  - Windows Server 2008 Service Pack 2 server

  - Windows Server 2003 R2 server

  - Windows Server 2003 Service Pack 2 server

  - Network attached storage or a network filer (such as NetApp and EMC)

- The secondary storage must be hosted in the same Workgroup as the Dynamic File Services server.

- To avoid potential data loss and conflicts, use only dedicated volumes when using UNC paths.

- Users must not have direct access to the remote share or to the path used for the share.

4.12 Merged View for Users

Dynamic File Services leverages Microsoft Network Sharing to provide the merged view to users. See the official Microsoft Windows documentation in the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/cc732793.aspx) for information about how to set up network sharing on the computers where the Service is running.

To see the merged view of the two storage locations, users access the Dynamic Storage pair through a Windows network share that you set up on the primary path in the pair. You can have additional network shares nested above and below the primary path. When you navigate the file tree through shares above the primary path, the merged view is shown when you open the primary folder to access the files and folders in the pair.

For secure access and authentication, users should access the data in the pair only via the network shares that are set up on the primary path. If users directly access files on the primary path or secondary path, potential issues can arise with duplicate files or with access rights and attributes being out of synchronization between primary and secondary folders.

To avoid these potential conflicts:

- Restrict direct access to the primary path and secondary path to administrative activities such as backup and restore.

- Use the merged view when changing ACL permissions and attributes for files and folders whenever possible as described in Section 4.15, "File and Folder Attributes and ACL Permissions," on page 47.
- Remove (or strictly limit access to) network shares for the secondary path.
- Do not create nested shares above or below the secondary path.

In a Windows cluster, always use the Windows cluster management tool and not Windows Explorer to manage file shares to folders on shared drives. Otherwise, changes to share information made by using Windows Explorer are lost when these file shares fail over to other nodes in the cluster. Workstations should be in an Active Directory domain to access the cluster-managed file shares.

4.13 Naming Conventions for Pairs and Policies

Dynamic File Services pair names and policy names can be up to 32 characters long. The characters in the name must be compatible with the share naming scheme for the file system. Character restrictions for the pair or policy name exclude the following:

```
"*\/[]:|<>+=;,?
```

Control characters (less then 0x20) are also invalid. All other ASCII characters, including extended ASCII, are valid.

If a policy name or pair name contains a space, you must delimit multiple entries with a comma when working from the command line interface.

4.14 Filename Path Length

Dynamic File Services uses the .NET Framework, which has length restrictions for folder paths and filenames. It allows a maximum of 248 characters in a folder name. The fully qualified filename must be less than 260 characters. For information, see *Long Paths in .NET* (http://blogs.msdn.com/bclteam/archive/2007/02/13/long-paths-in-net-part-1-of-3-kim-hamilton.aspx) in Microsoft Developers Network Blogs.

If a file's folder path or fully qualified filename is too long, the Standard Policy engine is not able to move the file during a policy run, and a `PathTooLongException` error is logged.

4.15 File and Folder Attributes and ACL Permissions

Dynamic File Services automatically synchronizes the attributes and ACL (access control list) permissions on files and folders that it moves, whether the move is triggered by a policy or by a user that accesses the data via the merged view.

After creating a pair, make sure to use the merged view of the pair's file tree when modifying the attributes and ACL permissions on files and folders in the pair. To make changes, access the pair via the network share on the primary path, then modify the settings.

- **Files:** When a file's ACLs are modified via the merged view, DynamicFS sets the permissions for the file on the primary path or secondary path, depending on where the file is currently stored.

◆ **Folders:** When a folder's attributes or ACLs are modified via the merged view, DynamicFS sets the permissions for a folder on both the primary and secondary paths, because folders have an instance in both locations.

To add username entries to a folder's ACL list, you must make the changes directly for the instance of the folder on the primary path. Windows does not allow usernames to be added to the ACL list when you are working in the merged view. DynamicFS monitors for security changes on the primary path and automatically synchronizes the ACL settings on the instance of the folder on the secondary path.

WARNING: Modifying the attributes and ACLs on folders when you are working outside of a merged view can cause conflicts for these values between the two folder instances on the primary path and secondary path.

To identify conflicts caused by mismatched attributes or ACL settings on a folder, you can run the DynamicFS Synchronize Pair tool (`DswSyncPair.exe`) to manually detect and report the attribute and ACL differences between the two instances of the folder. For information, see Section 8.11, "Reporting Conflicts for Attributes and ACL Permissions on Folders," on page 120.

4.16 Duplicate Folders

In a Dynamic File Services pair, a second instance of a folder is created on a target path as files are moved between the primary and secondary locations. In a merged view, users are not aware that two instances of a folder exist. If a folder is empty in one of the locations, the empty folder is not removed. If a user deletes a folder, both instances of the folder are removed.

Dynamic File Services automatically synchronizes the metadata information (such as ACLs and attributes) from the primary location instance of the folder to its secondary instance when the folders are accessed via the merged view or during a policy run. Because some metadata cannot be modified through a network share, DynamicFS also monitors instances of folders on the primary path for changes to metadata. For information about setting ACLs and attributes for folders, see Section 4.15, "File and Folder Attributes and ACL Permissions," on page 47.

The attributes and ACL settings for the two folder instances can become out of synchronization if you modify a folder's metadata by accessing a folder directly instead of via the merged view. Accessing a folder instance directly on the secondary path creates a conflict because the attributes or permissions are changed only on that instance of the folder, but not on its matching instance on the primary path.

For information about detecting and reporting conflicts in metadata on folders, see Section 8.11, "Reporting Conflicts for Attributes and ACL Permissions on Folders," on page 120.

4.17 Duplicate Files

In a Dynamic File Services pair, each file is intended to have a single instance on either the primary path or the secondary path. When a file is created, modified, or deleted through the merged view, DynamicFS automatically manages the file so that a single instance of a file exists. When policies are enforced, DynamicFS moves the single instance of a file between the two paths, and deletes the original copy of the file after the move is successfully completed.

Duplicate files are those where two instances the file have the same name and relative path in both locations. The content of the files might differ. If two instances of a file occurs, only the file instance on the primary is visible and accessible to the user. Users are not aware if duplicate files are present. However, a message is logged for the administrator. If a policy run attempts to move a file that has a duplicate in the target location, the move fails, and the error is logged in the *Statistics > Policy execution history > Files not moved* report.

Duplicate files are not intended to occur, but the situation can arise when you restore files from backup media, if files are accessed outside the merged view, or if the media becomes unavailable during a policy run and a file move is incomplete. Each of these situations is described in more detail below. For information about detecting and reporting duplicate files, see Section 8.12, "Reporting Conflicts for Duplicate Files," on page 121.

- Section 4.17.1, "Restoring Files from Backup Media," on page 49
- Section 4.17.2, "Accessing Files Outside the Merged View," on page 49
- Section 4.17.3, "Losing a Media Connection when Moving Files," on page 49

4.17.1 Restoring Files from Backup Media

Typically, duplicate files can occur when you restore files from backup media if different instances of a file are copied to the primary storage location and the secondary storage location. Backups for the primary and secondary are typically made at different times. Whether a file is captured in both backups depends on which policies were run in between the two backups. If you back up the primary path more frequently than the secondary path, the instance of the file that is restored on the primary storage area should be the most current of the two instances of the file.

4.17.2 Accessing Files Outside the Merged View

Duplicate files can also occur if users are allowed to access files directly instead of via the merged view. For example, a duplicate file can be created if a user has direct access to the two paths and manually copies a file from one path to the other. Users should always use the merged view of files in the pair when performing actions on them.

4.17.3 Losing a Media Connection when Moving Files

Duplicate files might occur if the source location or the target location of a file move becomes unavailable during a policy run. For example, if a connection is lost between the server and the secondary storage media, the file move that is in progress at that time cannot be completed, and the policy run is stopped. An `Invalid File Handle` error for the file is reported in the policy move log in the *Statistics > Policy execution history > Files not moved > Comment* field.

For file moves, Windows creates a sparse file in the target location that has the same filename and size as the original, and then copies the bits to the file. The original instance of the file is not deleted until all bits have been successfully copied to the new file instance. If the file move is interrupted, the information in the target location might be incomplete, and two instances of the file remain, which creates a duplicate file situation.

When duplicate files are caused by an incomplete move, the valid file is the instance on the source location of the move, and the invalid file is on the instance on the target location. If the incomplete file resides on the primary location, users see only the corrupted file. However, the valid file instance remains on the secondary location, and no data is actually lost.

To resolve this duplicate file situation, you must identify the duplicate files and delete the invalid instance of the file. Your knowledge of the policy direction setting for the policy run where the duplicate file was created will help you know which instance of the file is valid. You can review the *Statistics > Policy execution history > Files not moved* report for the policy run to identify the duplicate file and the target location of the policy run. You can also run the Sync Pair (`dswsyncpair.exe`) utility to find the duplicate file. For information about using the SyncPair utility to identify duplicate files, see "Dynamic File Services Synchronize Pair Utility" in the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.

4.18 System Files

The Standard Policy engine ignores files in the Windows system folder and other system files in the root folder such as `System Volume Information` and `Recycling Bin` folders. The system files are not moved.

4.19 Policy Schedules

Policies can be scheduled, unscheduled, and executed on demand. A policy run scans the pair's path, then moves the files that satisfy the criteria for the move. While policy runs are in progress, performance is slower. It is best to schedule policy runs in off-peak hours so that the user experience is not adversely affected.

Multiple policies can be scheduled to run at the same time. The policies are grouped for the run according to the direction files are to be moved: Primary to Secondary, then Secondary to Primary. When policies are run in combination, a file is moved if its conditions meet the rules defined in any one of the policies. That is, the different policies are enforced with an OR condition. The rules within an individual policy are enforced as an AND condition.

Only one scanning action can be performed on a pair at any given time. Actions include the following:

- Running one or more policies on a pair.
- Previewing one or more policies on a pair by doing a test run that reports what files would be moved if the policy were enforced at that time.
- Scanning the pair to collect file statistics for the pair history. The history scan runs once daily by default. You can set it to run hourly or weekly. For information, see Section 8.10, "Scheduling the Pair History Scan," on page 119.

Dynamic File Services does not queue the requests for activities. If the pair is busy, the pending action might not run.

For interval-based policies, the policy can start whenever the pair is available during the specified interval. If the pair is busy at the beginning of the interval, the pending action retries to start itself until the end of the interval. After it starts, the policy runs until complete, or until the end of the interval, depending on which event first occurs.

For policies that begin at a given start time and run until complete, if the pair is busy at the scheduled start time, the pending action retries to start itself for up to 20 minutes beyond the scheduled start time. If you schedule the policies to start at the same time, they can run concurrently. If you schedule policies to begin at different times, there must be sufficient time available for one policy to complete before another is scheduled to begin.

For example, if PolicyA and PolicyB are scheduled to run on the same pair at 12:00 a.m. and 12:05 a.m. respectively, and each policy takes 30 minutes to complete, PolicyB probably never runs. However, if you schedule the two policies to start at the same time, both policies are run in combination.

To avoid scheduling conflicts, we recommend that you use one of the following approaches when scheduling policies for a pair:

- **Same Schedule:** Schedule the pair's assigned policies to start and stop at the same time. This allows the Standard Policy engine to run them concurrently, which is the most efficient way to enforce policies. Policies can be run manually at other times if needed.

- **Non-Overlapping Schedule:** Schedule the pair's policies so that each policy runs in its own window of time, making sure that the start times and stop times do not overlap. Policies can be run manually as needed at unscheduled times. This approach makes it more difficult to predict idle times to run policies manually on the pair.

For information about how scheduling works, see Section 9.7.1, "Understanding How Changes Affect the Scheduled Run Interval," on page 140.

4.20 Time Displays

All time stamps are stored and displayed in the server's time zone, regardless of where the client is located. That is, all time stamp viewing and configuration is relative to the Dynamic File Services server you are managing.

4.21 Event Logging

Dynamic File Services uses the Microsoft Event Viewer for logging the Dynamic File Service start/stop events and fatal errors such as application exceptions.

4.22 Using Antivirus Software with Pairs

Dynamic File Services can be used on servers running antivirus software. There are two common scenarios:

- Map a drive to the network share for the primary path, and run your antivirus software on the share. This scans both primary and secondary files through the merged view.

- Run your antivirus software separately on each drive, or run it separately on the primary path and secondary path.

4.23 Using Backup Software with Pairs

Dynamic File Services can be used with backup software. The administrator separately backs up the primary path and secondary path. Backup frequency typically differs between the two locations, with the frequency determined by data volatility and importance. The primary location is typically backed up more often than the secondary.

4.24 Using Compression with Pairs

Dynamic File Services supports using compression in a pair. DynamicFS behavior complies with the expected behavior for copying or moving compressed files:

- If the user copies or moves a compressed file to an uncompressed folder, the file is decompressed.
- If the user copies or moves an uncompressed file to a compressed folder, the file is compressed.

4.25 Using Disk Quotas with Pairs

Dynamic File Services supports using disk quotas on the primary path, secondary path, or both paths. If the primary and secondary locations are on the same disk, the disk quota applies across both areas.

In a typical configuration, different disks are used for the primary and secondary locations. If the disk quota is enforced on the primary disk and a user reaches the set quota, the user is no longer able to create new files. DynamicFS also cannot move the user's files from the secondary disk to the primary disk. However, if a policy moves some or all of the user's files to the secondary location, the freed space on the primary location is again available to the user.

If you also apply a disk quota on the secondary disk, you are dealing with two separate quotas: one for the primary path, and one for the secondary path. There are two conditions to consider:

- **User Reaches the Primary Quota:** If the user reaches the quota on the primary path but not on the secondary path, the effect is the same as if the second quota does not exist.
- **User Reaches the Secondary Quota:** If the user reaches the quota on the secondary path but not on the primary path, the user can create files and DynamicFS can move the user's files from secondary to primary when they are accessed. However, DynamicFS cannot enforce policies to move the user's files from the primary to the secondary.

Depending on where the user's files are located, the user's effective quota is somewhere between the minimum quota you set on the primary or secondary path up to the potential maximum, which is the sum of the two quotas.

4.26 Using Encryption with Pairs

Dynamic File Services treats all files and folders as if they are not encrypted.

WARNING: If an encrypted file or folder is moved by a policy, the encryption key changes and the data is no longer accessible to the user. The data is effectively lost.

- Section 4.26.1, "Windows File and Folder Encryption," on page 53
- Section 4.26.2, "Hardware-Level Disk Encryption," on page 53

4.26.1 Windows File and Folder Encryption

Dynamic File Services does not support using file or folder encryption for pairs.

To prevent possible data loss, make sure your pair does not use file and folder encryption by doing the following:

- Choose nonencrypted folders for the primary path and secondary path for the pair. The folders should not contain encrypted files or folders.
- Do not encrypt files or folders in the primary path and the secondary path of the pair.
- Do not encrypt parent folders above the pair's primary path and secondary path.

4.26.2 Hardware-Level Disk Encryption

Dynamic File Services supports using some third-party hardware-level disk encryption for drives that are used in pairs. The file moves are not affected by hardware-level disk encryption because the encryption operates at a level beneath the file system.

4.27 Using Windows Distributed File System with Pairs

Dynamic File Services supports using Windows Distributed File System (DFS) links to point to the network share on the primary folder in a pair. That is, the network share on the primary path of the pair can be the target of a DFS link. Pairs should not be created for the DFS namespace or links therein.

After you create a link to the network share on the primary path, users can map a drive on their workstations to the DFS Namespace share (or DFS Root share). The DFS link takes them to the network share on the pair's primary path. The users see the same merged view of the pair as if they connect directly to the network share on the pair's primary path. This does not prohibit other users from mapping directly to the network share on the pair's primary path. It is up to you which share path you give to your users.

It does not matter in which order you create pairs and Distributed File System links. You can create a pair where the primary path contains data that is the target of an existing DFS link. You can create a DFS link that points to the network share on the primary path of an existing pair.

A pair should not be created for the DFS Namespace folder (or DFS Root folder) and its contents. The DFS Root folder should not be nested above or below any path that contains a DynamicFS primary path or secondary path.

IMPORTANT: For all issues related to configuring and managing Windows Distributed File System, see the official Microsoft documentation for your Windows Server operating system in the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/cc753479(WS.10).aspx).

The following sections illustrate the general deployment guidelines for using Dynamic File Services and Windows Distributed File System in a Windows environment.

4.27.1 Example: Different Servers

Figure 4-1 illustrates a configuration where the Windows Distributed File System (DFS) Server is a different server than the targets of the Windows DFS links. DynamicFS is installed on the servers where you create the pairs, but it is not installed on the Windows DFS Server. The Windows DFS links point to the network shares on the primary paths of the pairs.

Figure 4-1   *Using Windows DFS and Dynamic File Services on Different Servers*
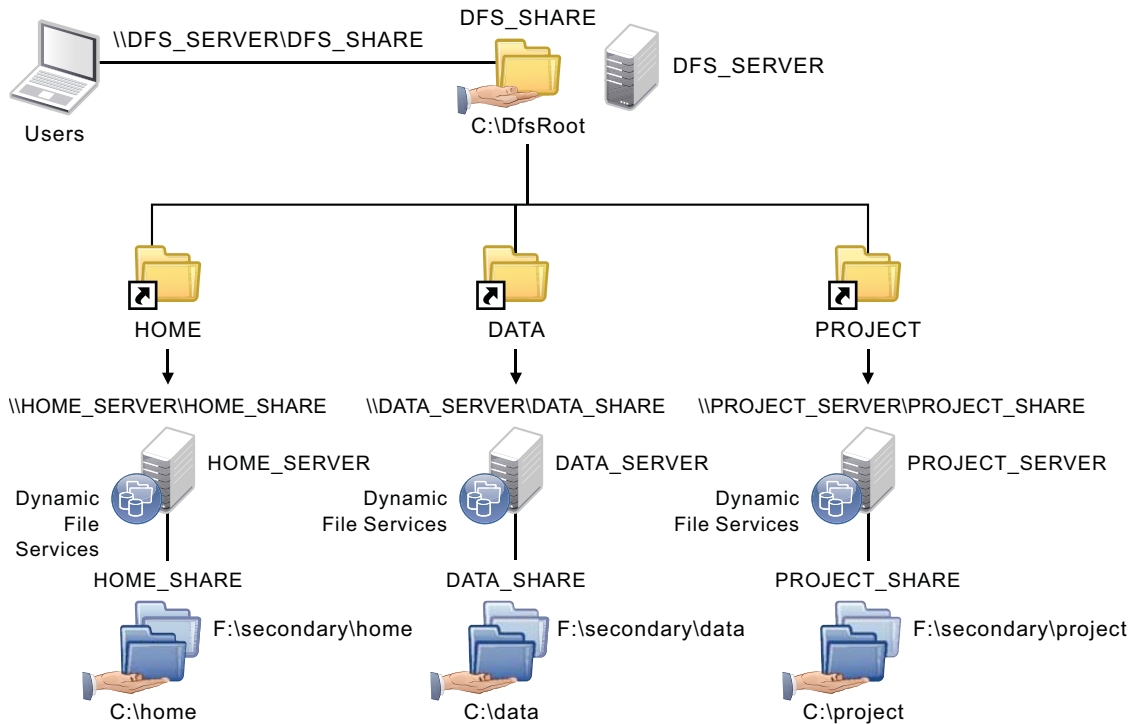
4.27.2 Example: Same Server

Figure 4-2 illustrates a configuration where the Windows Distributed File System Server is on the same server as the targets of the Windows DFS links. In this case, DynamicFS is installed on the DFS Server. The Windows DFS links point to the network shares on the primary paths of the pairs. The DFS Namespace folder (or DFS Root folder) is not configured as a pair, and it is not nested with any of the primary paths and secondary paths that are used in the pairs.

Figure 4-2 *Using Windows DFS and Dynamic File Services on the Same Server*
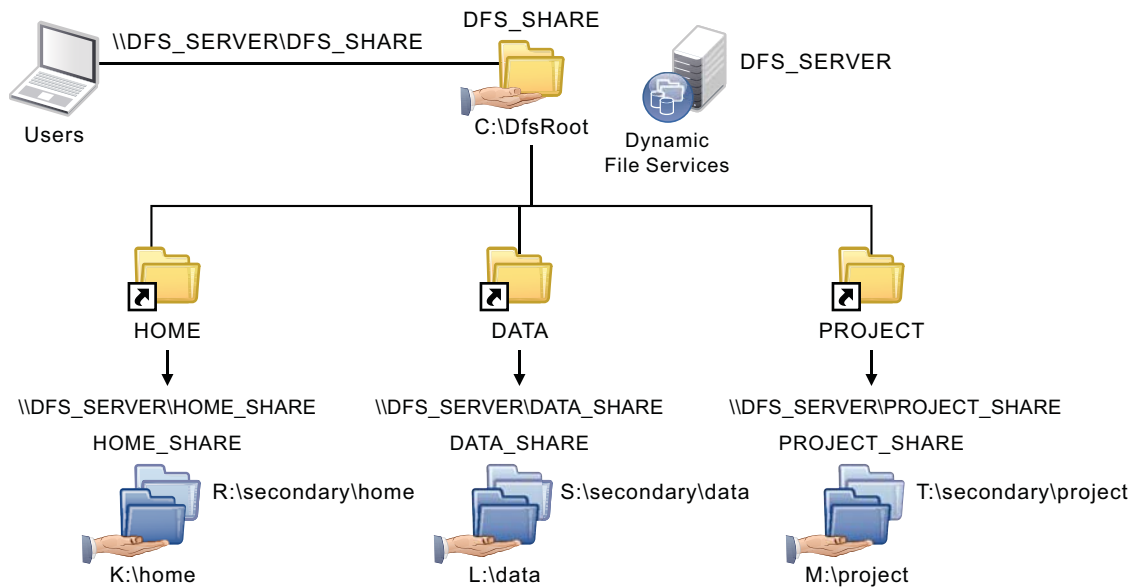
4.28 Using Dynamic File Services in a Windows Cluster

Dynamic File Services supports using pairs and policies in a Windows failover cluster. However, the software is not cluster aware.

This section describes known issues for using Dynamic File Services in an Windows cluster. For information about installing Dynamic File Services in a cluster, see the *Dynamic File Services 1.6 Installation Guide*.

- Section 4.28.1, "Management Console," on page 55
- Section 4.28.2, "Service Controller," on page 56
- Section 4.28.3, "Executable Files," on page 56
- Section 4.28.4, "Standard Policy Engine and Registry Information," on page 56
- Section 4.28.5, "Moving the Service Cluster Resource Between Nodes," on page 56

4.28.1 Management Console

When using the Management Console to manage the Dynamic File Service in a cluster, use the cluster resource IP address of the Service to connect to the cluster instead of the server node's IP address.

When creating pairs and policies, make sure that the primary path and secondary path of each pair reside on shared storage that can be failed over together between the cluster nodes.

4.28.2 Service Controller

The Service Controller starts automatically at the beginning of each session when you log in to the active node where the disk that contains the Novell Dynamic File Services software is currently mounted. The controller does not start if you log in to the failover node because the shared disk is not mounted there.

4.28.3 Executable Files

The Dynamic File Service is started automatically by the Windows cluster management tool when it brings the Dynamic File Service cluster resource online. The Service is stopped when the Windows cluster management tool brings the resource offline. Make sure to use the Windows cluster management tool to start and stop the Service, and not the Dynamic File Service Controller.

Other DynamicFS executable files are called from the Service, or can be started manually when you are logged in on the active nodes as user in the `Dynamic File Services` group (or as the Administrator user on that node). Conversely, you cannot start the executable files on the failover node because the cluster drive resource that contains the files is not attached to it.

4.28.4 Standard Policy Engine and Registry Information

Policy moves and previews should work correctly on the active node, regardless of which node is active, if the install location is correct in the registry. If policy runs and preview runs do not work after you set up your DynamicFS cluster resource group, check that the node's registry contains the right install location.

4.28.5 Moving the Service Cluster Resource Between Nodes

Before initiating a non-failover move of the Dynamic File Service cluster resource from the active node to a failover node, make sure that you have quiesced the Service as described in "Prerequisites for Stopping or Restarting the Service" on page 73.

If a policy is being run when the move is initiated, the resource enters an *Offline Pending* state until DynamicFS can gracefully complete the in-progress file copies, shut down the policy run, and go offline for the move. This process can take up to 10 minutes. During this time, the failover cluster File Server and IP address for the Service are unavailable, and users are unable to access the files.

If the active node crashes when a policy run is in progress, the Service also crashes. The Service cluster resource immediately goes offline and fails over to the failover node. The following issues must be addressed after the Service cluster resource is back online:

- The policy run does not automatically resume or start over after the failover.
- There is no ability to gracefully complete any file copies that are in progress for the policy run.

  There is no data loss, but duplicate files might exist, where the original file is good but the instance of the file in the target location is only a sparse file.

To resolve this problem:

1. Check for duplicate files in the pairs where the policy was running by running the Pair Synchronization utility on each pair. For information, see Section 8.12, "Reporting Conflicts for Duplicate Files," on page 121.

2. For each reported duplicate file conflict, delete the instance of the file in the target location of the policy move.

3. After all duplicate file conflicts have been resolved, the policy run can be started manually, or the policy runs at its next scheduled time.

4.29 Using Dynamic File Services in Windows Safe Mode

The Dynamic File Service does not load or run in Windows Safe Mode.

The Service Controller loads and runs under the same conditions as in Windows Normal Mode. However, you cannot start the Dynamic File Service in Safe Mode.

The `DswDump.exe` and `DswSyncPair.exe` utilities can be used in Safe Mode to gather and report information from the Dynamic File Services databases. For details about using these commands, see the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.

If networking is enabled in Safe Mode, the Dynamic File Services Management Console can be used to connect to and manage other Dynamic File Services servers.

Using the Management Tools

<div align="right">5</div>

Novell Dynamic File Services (DynamicFS) provides management tools to help you manage the service, create and manage pairs and policies, and repair the pair and policy databases. This section describes how to access the tools and where to find information about the tasks you can perform with them.

5.1 Service Controller

The Service Controller allows the Administrator user or users with Administrator privileges to view or configure the settings for the Dynamic File Service and to start or stop the Service. It displays the current Service status (enabled or disabled). You can launch the Management Console to create and manage pairs on the same server or different DynamicFS servers. You can also find information about the Dynamic File Services software.

The Service Controller can be used in Windows Safe Mode to modify the Service settings. However, you cannot start the Service while the computer is in Safe Mode.

5.1.1 Accessing the Service Controller

The Service Controller starts automatically when any user logs in to the desktop of a server where the Dynamic File Service component is installed. When the Service Controller is running, the Dynamic File Services icon (🌐) is displayed in the Windows notification area (the lower right corner of the computer screen).

1 Log in to the DynamicFS server.

> **IMPORTANT:** You must log in as a user with Administrator privileges to configure the Service settings, to start or stop the Service, and to use the Repair Tool.

The Service Controller starts automatically and displays the Dynamic File Services icon (🌐) in the notification area.

2 Right-click the Service Controller icon to access the menu.
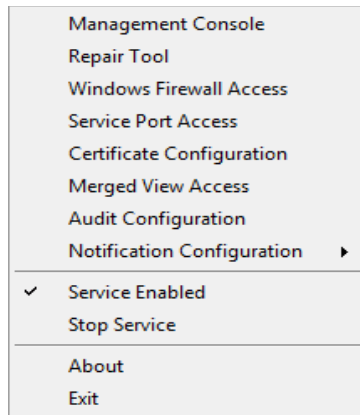
For information, see Section 5.1.2, "Service Controller Tasks Quick Reference," on page 60.

5.1.2 Service Controller Tasks Quick Reference

You can use the following quick reference to find information about the tasks you can perform from the Service Controller. Administrator privileges are required to start and stop the Service, to modify the configuration of the Service, or to use the Repair Tool. All users logged in to the desktop of the server can view the status of the service and use the *Management Console*, *About*, and *Exit* options.

Menu Option	For information, see
Management Console	Section 5.2, "Management Console," on page 61
Repair Tool	Chapter 11, "Repairing the Pair and Policy Databases," on page 173
Windows Firewall Access	Section 6.7, "Configuring Firewall Access for the Service Port," on page 82
Service Port Access	Section 6.6, "Configuring the Service Port," on page 81
Certificate Configuration	Section 6.8, "Configuring a Certificate for Secure Remote Management Sessions," on page 85
Merged View Access	Section 6.9, "Configuring the Merged View Access," on page 91
Audit Configuration	Section 6.4, "Configuring the Auditing Service," on page 74
Notification Configuration	Section 6.5, "Configuring the Notification Service," on page 76
Service Enabled or Service Disabled	Section 6.3.1, "Viewing the Service Status," on page 72
Start Service	Section 6.3.2, "Starting the Dynamic File Service," on page 73
Stop Service	Section 6.3.3, "Stopping the Dynamic File Service," on page 73
About	Section 6.11, "Finding Product Version and Build Information," on page 93
Exit	Section 5.1.4, "Stopping the Service Controller," on page 61

5.1.3 Starting the Service Controller

If the Dynamic File Service component is installed on the computer, Service Controller should start automatically when you log in to the computer. If the Service Controller is not running, the Service Controller icon is not displayed in the notification area. The most common reason that Service Controller might not be running is that you exited the tool.

To start the service automatically:

1 Log out of the DynamicFS server.

2 Log in to the DynamicFS server.

The Service Controller starts and its icon appears in the Windows notification area.

You can also manually start the Service Controller. Administrator privileges are required.

1 In a Windows Explorer browser, navigate to the folder where you installed the Dynamic File Services software.

The default location is the `C:\Program Files\Dynamic File Services` folder.

2 Double-click the `DswServiceController.exe` file.

If you are prompted for credentials by Windows User Account Control, provide the username and password of a user with Administrator privileges on the computer.

The Service Controller starts and its icon appears in the Windows notification area.

5.1.4 Stopping the Service Controller

The Dynamic File Service runs independently of the Service Controller. Although it is not necessary to do so, you can stop the Service Controller during a login session if you are not modifying the configuration or status of the Dynamic File Service at that time.

1 Right-click the Service Controller icon in the Windows notification area.

2 Select *Exit*.

5.2 Management Console

The Dynamic File Services Management Console is a GUI-based management tool that allows you to configure and manage pairs and policies on servers in the same local area network. In an Active Directory environment, the computer must also be in the same domain as the servers you want to manage.

The Management Console can be installed on a server or workstation. For information, see "Supported Platforms" in the *Dynamic File Services 1.6 Installation Guide*.

The Manage Console can be used to manage pairs and policies on one or more servers where the Dynamic File Service is installed and running. Each server's pairs and policies are unique to that server, and the related pair and policy configuration files are stored locally in the `C:\Program Files\Dynamic File Services` folder (or the folder where you installed Dynamic File Services) on the server that is being managed. This folder also contains the history and statistics information about policy runs on the server.

- Section 5.2.1, "Accessing the Management Console," on page 62

5.2.1 Accessing the Management Console

When you installed Dynamic File Services, a Management Console icon was placed in the following locations:

- ◆ The computer desktop
- ◆ The *Start* menu under *Dynamic File Services > Dynamic File Services Management Console*
- ◆ The Control Panel menu under *Additional Options*

An option to launch the tool is also included in the Service Controller menu.

To access the Management Console:

1 Log in to the DynamicFS server or client where the Management Console is installed.

2 Use any of the following methods to launch the Management Console:

- ◆ Double-click the Management Console icon on the desktop.
- ◆ In the *Start* menu, select *All Programs > Dynamic File Services > Dynamic File Services Management Console*.
- ◆ In the *Start* menu, select *Control Panel*, then select *Additional Options > Novell Dynamic File Services* in the Control Panel dialog box.
- ◆ Right-click the Service Controller icon in the desktop notification area, then select *Management Console*.

3 If you have not already done so, set up the Dynamic servers you want to manage as described in Section 7.1, "Setting Up a Server in the Management Console," on page 95.

If different administrator users log in to the same computer to use the Management Console, each user must configure a list of servers to manage.

5.2.2 Management Console Wizards

The Management Console provides the following configuration wizards to help you set up servers to manage and to create pairs and policies on them:

Wizard	Description	For information, see
Server Wizard	Helps you set up a DynamicFS server that you want to manage.	Section 7.1, "Setting Up a Server in the Management Console," on page 95
Setup Wizard	Helps you create a pair and a policy, and associates them automatically at create time.	Section 8.2, "Creating a Pair," on page 109 Section 9.2, "Creating a Policy," on page 130
Pair Wizard	Helps you create a pair and associate it with none, one, or multiple policies.	Section 8.2, "Creating a Pair," on page 109

Wizard	Description	For information, see
Policy Wizard	Helps you create a policy and associate it with none, one, or multiple pairs.	Section 9.2, "Creating a Policy," on page 130

5.2.3 Management Console Tasks Quick Reference

You can use the following quick reference to find information about the tasks you can perform from the Management Console. You must be able to provide the login credentials of the Administrator user or a member of the `Dynamic File Services` group on the DynamicFS server you want to manage.

* "Server Management Tasks" on page 63
* "Pair Management Tasks" on page 64
* "Policy Management Tasks" on page 65
* "Server, Pair, and Policy Monitoring Tasks" on page 67

Server Management Tasks

The following table helps you find the management tasks for DynamicFS servers:

Server Options	Description	For information, see
Server Wizard	Lets you provide the authentication credentials needed to connect to a DynamicFS server.	Section 7.1, "Setting Up a Server in the Management Console," on page 95
Connect to a server	Lets you log in to the DynamicFS server that you want to manage.	Section 7.3, "Connecting to a Server," on page 99
Disconnect from a server	Lets you disconnect from a DynamicFS server that you are managing.	Section 7.6, "Disconnecting from a Server," on page 103
Servers container	Lets you view a list of servers and their current status.	Section 7.4, "Viewing a List of Servers and Their Connection Status," on page 99
Export a server list	Lets you export a list of servers that are configured in the Management Console to an XML file in a local folder.	Section 7.8, "Exporting and Importing a Server List," on page 104
Import a server list	Lets you import a previously exported list of servers from a local folder to add the servers to the Management Console.	Section 7.8, "Exporting and Importing a Server List," on page 104
Remove a server	Lets you remove a server from the list	Section 7.9, "Removing a Server from the List," on page 105
Server Properties	Lets you view information about a DynamicFS server.	Section 7.5, "Viewing Server Properties," on page 100

Server Options	Description	For information, see
Server Properties > Disk details	Lets you view disk details and the disk capacity and used space history for server disks on a DynamicFS server	Section 10.6, "Viewing Capacity and Used Space History for Server Disks," on page 165
Server Properties > Log files	Lets you view the logged events for the Service, Standard Policy engine, and other components.	Section 10.7, "Viewing Logged Events," on page 168
Server Properties > Logging levels	Lets you set the logging levels for the Service and Standard Policy engine components.	Section 6.10, "Configuring the Logging Level for the Service and Standard Policy Log Files," on page 92

Pair Management Tasks

The following table summarizes the pair management tasks:

Pair Options	Description	For Information
Setup Wizard	Helps you create a pair and a policy, and associates them automatically at create time.	Section 8.2, "Creating a Pair," on page 109
		Section 9.2, "Creating a Policy," on page 130
Pair Wizard	Helps you configure a pair on a specified server, and associate it with none, one, or multiple policies.	Section 8.2, "Creating a Pair," on page 109
Pairs container	Lets you view a list of pairs and their current status (*Running* or *Idle*).	Section 8.6, "Viewing a List of Pairs," on page 115
		Section 8.7, "Viewing the Pair Status," on page 116
Pair Properties	Lets you view configuration information for a pair.	Section 8.8, "Viewing Properties for a Pair," on page 116
Pair Properties > Associations	Lets you view, add, or remove policy associations for a pair.	Section 9.5.4, "Associating or Disassociating Policies with a Selected Pair," on page 137
Policy Properties > Associations	Lets you view, add, or remove pair associations for a policy.	Section 9.5.3, "Associating or Disassociating Pairs with a Selected Policy," on page 136
Pair Properties > Include/Exclude	Lets you specify whether to include folders or exclude folders from policy runs on a pair, and add or remove folders from the list.	Section 8.5, "Including or Excluding Folders from a Pair's Policy Runs," on page 114
Pair Properties > Pair history	Lets you schedule the pair history scan on a pair.	Section 8.10, "Scheduling the Pair History Scan," on page 119

Pair Options	Description	For Information
Pair Statistics	Lets you view statistics about a pair's status and last policy run. You can also add or remove associated policies.	Section 10.1, "Viewing the Pair Statistics," on page 157 Section 9.5.4, "Associating or Disassociating Policies with a Selected Pair," on page 137
Pair Statistics > Pair history	Lets you view statistics about the disk space consumed over time for each path in a pair.	Section 10.5, "Viewing the Pair History," on page 163
Pair Statistics > Policy execution history	Lets you view statistics about policy runs on a pair, including the run history of files moved or not moved.	Section 10.2, "Viewing the Policy Execution History for a Pair," on page 158
Preview now	Lets you preview the results of a policy run on a selected pair without running the policy.	Section 9.9, "Previewing a Policy Run," on page 143
Execute now	Lets you run a policy on demand for a selected pair.	Section 9.8, "Starting a Policy Run," on page 142
Manual move	Lets you move selected files or folders for a one-time move event on a selected pair.	Section 8.9, "Moving Selected Files or Folders," on page 118
Stop running process	Lets you stop a currently running policy on a pair.	Section 9.10, "Stopping a Policy Run," on page 144
Server Properties > Disk details	Lets you view disk details and the disk capacity history for server disks that are used in a pair on a DynamicFS server that you are managing.	Section 10.6, "Viewing Capacity and Used Space History for Server Disks," on page 165
Unlink the paths in a pair	Lets you remove a pair relationship between two paths.	Section 8.13, "Unlinking the Paths in a Pair," on page 122

Policy Management Tasks

The following table summarizes the policy management tasks:

Policy Options	Description	For Information
Setup Wizard	Helps you create a pair and a policy, and associates them automatically at create time.	Section 8.2, "Creating a Pair," on page 109 Section 9.2, "Creating a Policy," on page 130
Policy Wizard	Helps you create a policy and associate it with none, one, or multiple pairs.	Section 9.2, "Creating a Policy," on page 130
Policies container	Lets you view a list of policies and their current status (*Running* or *Idle*).	Section 9.3, "Viewing a List of Policies," on page 134

Policy Options	Description	For Information
Edit or modify a policy	Lets you modify the policy direction, frequency, filter options, or description.	Section 9.6, "Modifying Policy Rules," on page 138

Section 9.7, "Modifying Policy Schedules," on page 139 |
Export a policy	Lets you export a policy's configuration information to an XML file in a local folder on the computer that is running the Management Console.	Section 9.11, "Exporting and Importing Policies on a Dynamic File Services Server," on page 144
Import a policy	Lets you import a previously exported policy from a local folder to add it to a DynamicFS server that you are managing in the Management Console.	Section 9.11, "Exporting and Importing Policies on a Dynamic File Services Server," on page 144
Preview now	Lets you preview the results of a policy run on a selected pair without running the policy.	Section 9.9, "Previewing a Policy Run," on page 143
Execute now	Lets you run a policy on demand for a selected pair.	Section 9.8, "Starting a Policy Run," on page 142
Manual move	Lets you move selected files or folders for a one-time move event on a selected pair.	Section 8.9, "Moving Selected Files or Folders," on page 118
Stop running process	Lets you stop a currently running policy on a pair.	Section 9.10, "Stopping a Policy Run," on page 144
Policy Properties	Lets you view configuration information for a policy. You can also modify the policy direction, frequency, filter options, or description.	Section 9.4, "Viewing Properties for a Policy," on page 134

Section 9.6, "Modifying Policy Rules," on page 138

Section 9.7, "Modifying Policy Schedules," on page 139 |
| Policy Properties > Associations | Lets you view, add, or remove pair associations for a policy. | Section 9.5.3, "Associating or Disassociating Pairs with a Selected Policy," on page 136 |
| Pair Properties > Associations | Lets you view, add, or remove policy associations for a pair. | Section 9.5.4, "Associating or Disassociating Policies with a Selected Pair," on page 137 |
| Pair Statistics | Lets you view statistics about a pair's status and last policy run, including the policy run history of files moved or not moved. You can also add or remove associated policies. | Section 10.1, "Viewing the Pair Statistics," on page 157

Section 9.5.4, "Associating or Disassociating Policies with a Selected Pair," on page 137 |
| Pair Statistics > Policy execution history | Lets you view statistics about policy runs on a pair, including the run history of files moved or not moved. | Section 10.2, "Viewing the Policy Execution History for a Pair," on page 158 |

Policy Options	Description	For Information
Server Properties > Log files > `DswStandardPolicy.log`	Lets you view the events for policy runs in the Standard Policy engine's log.	Section 10.7, "Viewing Logged Events," on page 168
Delete a policy	Lets you remove a policy.	Section 9.12, "Deleting a Policy," on page 145

Server, Pair, and Policy Monitoring Tasks

The following table summarizes the monitoring tasks for DynamicFS servers, pairs, and policies:

Monitoring Options	Description	For Information
Servers container	Lets you view a list of servers and their current status (*Connected* (green icon) or *Disconnected* (dimmed icon)).	Section 7.4, "Viewing a List of Servers and Their Connection Status," on page 99
Pairs container	Lets you view a list of pairs and their current status (*Running* or *Idle*).	Section 8.6, "Viewing a List of Pairs," on page 115 Section 8.7, "Viewing the Pair Status," on page 116
Policies container	Lets you view a list of policies and their current status (*Running* or *Idle*).	Section 9.3, "Viewing a List of Policies," on page 134
Server Properties	Lets you view information about a DynamicFS server that you are managing.	Section 7.5, "Viewing Server Properties," on page 100
Pair Properties	Lets you view configuration information for a pair.	Section 8.8, "Viewing Properties for a Pair," on page 116
Policy Properties	Lets you view configuration information for a policy. You can also modify the policy direction, frequency, filter options, or description.	Section 9.4, "Viewing Properties for a Policy," on page 134 Section 9.6, "Modifying Policy Rules," on page 138 Section 9.7, "Modifying Policy Schedules," on page 139
Pair Statistics	Lets you view statistics about a pair's status and last policy run, including the policy run history of files moved or not moved.	Section 10.1, "Viewing the Pair Statistics," on page 157
Pair Statistics > Pair history	Lets you view statistics about the disk space consumed over time for each path in a pair.	Section 10.5, "Viewing the Pair History," on page 163
Pair Statistics > Policy execution history	Lets you view statistics about policy runs on a pair, including the run history of files moved or not moved.	Section 10.2, "Viewing the Policy Execution History for a Pair," on page 158

Monitoring Options	Description	For Information
Server Properties > Disk details	Lets you view disk details and the disk capacity history for server disks on a DynamicFS server that you are managing.	Section 10.6, "Viewing Capacity and Used Space History for Server Disks," on page 165
Viewing Service events	Lets you view error events for the Dynamic File Service.	Section 10.8, "Viewing Service Events," on page 169
Viewing logged events	Lets you view the logged events for the Service, Standard Policy engine, and other components.	Section 10.7, "Viewing Logged Events," on page 168
Audit log	Lets you view the logged management events for the Service, pairs, policies, and repair.	Section 10.9, "Auditing Management Events," on page 169

5.3 Repair Tool

The Dynamic File Services Repair tool is used to repair problems in the pair and policy database files on a server. It provides a Report mode and Repair mode. The Report mode allows you to generate a report on the health of the pair and policy databases. The report identifies problems and indicates whether a problem is repairable or not. The Repair mode repairs problems if it can. For information, see Chapter 11, "Repairing the Pair and Policy Databases," on page 173

5.4 Command Line Interface

Dynamic File Services provides a command line interface (CLI) that can be used to create and manage pairs and policies. The CLI is a text interface that can be used in scripts. DynamicFS also provides utilities for troubleshooting, such as for synchronizing files and folders in a pair and for dumping the current configuration settings. For information, see the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.

Configuring and Managing the Service

<div style="text-align: right; font-size: xxx-large;">6</div>

An administrator can configure and manage the Dynamic File Service by logging in to the server where the Service is installed. This section describes the Service configuration options.

6.1 Requirements for Administering the Service

The Administrator user and users with Administrator privileges on the Dynamic File Services server have all the permissions necessary to administer the Dynamic File Service configuration.

The authorized user must log in to the server desktop where the Dynamic File Service is installed in order to administer the service.

6.2 Configuring Administrators for Pair and Policy Management

Pairs and policies can be managed by any user with sufficient rights to do so. Some administrators have rights automatically. You can allow other users to manage pairs and policies by adding them as members of the `Dynamic File Services` group. Table 6-1 identifies the rights needed when the DynamicFS server is in a Workgroup environment or in an Active Directory Domain environment:

Table 6-1 *Rights Needed to Manage Pairs and Policies*

Workgroup Environment	Active Directory Domain Environment
Not applicable	Domain Admin users and domain users with Domain Admin privileges

Workgroup Environment	Active Directory Domain Environment
Administrator user and local users with Administrator privileges on the server	Administrator user and local users with Administrator privileges on the server
Local users that you add as members of the server-based `Dynamic File Services` group	Domain users that you add as members of the domain-based `Dynamic File Services` group

You can use the procedures in this section to add or remove members in the `Dynamic File Services` group.

- Section 6.2.1, "Understanding the Dynamic File Services Group," on page 70
- Section 6.2.2, "Setting Up Administrators in a Domain," on page 71
- Section 6.2.3, "Setting Up Administrators in a Workgroup," on page 72

6.2.1 Understanding the Dynamic File Services Group

You can set up a group of users to manage pairs and policies on Dynamic File Services servers by adding them as a member of the `Dynamic File Services` group. The nature of the group and its setup are different, depending on whether the server is located in an Active Directory domain or in a Workgroup. This section describes the differences.

- "How is the group created?" on page 70
- "Who controls membership in the group?" on page 70
- "Who can be a member of the group?" on page 71

How is the group created?

The `Dynamic File Services` group is created automatically during the installation of Dynamic File Services. If the server is a member of a workgroup, the group is created locally in the Windows *Local Users and Groups* area. The group is created in the domain *Users* area if the server is a domain controller or member server in an Active Directory domain. The group is removed from the server if you uninstall Dynamic File Services.

In an Active Directory domain, the group is created when Dynamic File Services is first installed on a domain controller server or member server. The group is used by all DynamicFS servers that are subsequently installed in the same domain. The group is removed when you uninstall the last instance of Dynamic File Services in the domain.

The user that installs Dynamic File Services must have sufficient privileges to create groups. Otherwise, the group creation fails and a user Administrator privileges or Domain Admin privileges must set up the group manually in the appropriate location.

Who controls membership in the group?

Generally, administrators control which users are added or removed as members of the `Dynamic File Services` group.

In a workgroup, the Administrator user or a local user with Administrator privileges can add or remove members. In the Windows Computer Management tool, select *Local Users and Groups > Groups > Properties > Members* field. For information, see Section 6.2.3, "Setting Up Administrators in a Workgroup," on page 72.

In a domain, the Domain Admin user or a domain user with Domain Admin privileges can add or remove members. In the Active Directory Users and Computers tool, select the domain, then select *Users and Groups > Groups > Properties > Members tab*. For information, see Section 6.2.2, "Setting Up Administrators in a Domain," on page 71.

Who can be a member of the group?

The `Dynamic File Services` group has no default members.

For a local group, any local user can be added to the group. A local user does not need Administrator privileges in order to be a member. It is not necessary to explicitly add the Administrator user to the group, but you can add it. The members can manage pairs and policies on the DynamicFS server where the group was created.

For a domain group, any domain user can be added to the group. A domain user does not need Domain Admin privileges in order to be a member. It is not necessary to explicitly add a Domain Admin user to the group, but you can add it. The members can manage pairs and policies on any DynamicFS server in the same domain.

6.2.2 Setting Up Administrators in a Domain

In a domain environment, members of the `Dynamic File Services` group can manage pairs and policies on any of the DynamicFS servers in the domain.

To add or remove domain users as members of the domain-based `Dynamic File Services` group:

1 Log in to the DynamicFS server as a Domain Admin.

2 Open the Active Directory Users and Computers utility by selecting *Administrator Tools > Users and Computers*.

3 Select the domain, then select *Users > Groups*.

4 Open the group's *Properties* dialog box by double-clicking the `Dynamic File Services` group.

   You can also right-click the group and select *Properties*. Current domain users that are members of the group appear in the list.

5 In the *Properties* dialog box, click the *Members* tab.

6 Configure the members of the group by doing either or both of the following tasks:

   ◆ **Add a member:** Click *Add*, use the *Enter the object names to select* field to specify the users you want to manage DynamicFS in the domain, then click *OK* to save and apply your changes.

   ◆ **Remove a member:** Select one or more usernames from the member list, click *Remove*, then click *OK* to save and apply your changes.

7 Click *OK* to close the `Dynamic File Services` group *Properties* dialog box.

6.2.3 Setting Up Administrators in a Workgroup

In a workgroup environment, members of the server-based `Dynamic File Services` group can manage pairs and policies for the server.

To add or remove local users as members of the server-based `Dynamic File Services` group:

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 Open the Windows Computer Management tool.

3 Select *Local Users and Groups* > *Groups*, then double-click the `Dynamic File Services` group to open the group's Properties dialog box.

Current members appear in the list.

4 Configure the members of the group by doing either or both of the following tasks:

   ◆ **Add a member:** Click *Add*, use the *Enter the object names to select* field to specify the users you want to manage DynamicFS on that server, then click *OK* to save and apply your changes.

   ◆ **Remove a member:** Select one or more usernames from the member list, click *Remove*, then click *OK* to save and apply your changes.

5 Click *OK* to close the `Dynamic File Services` group Properties dialog box.

6.3 Starting and Stopping the Service

The Dynamic File Service is the engine that manages the various components. It starts automatically after the install and on system boot in Windows Normal Mode. (The Service does not run in Windows Safe Mode.) A user with Administrator privileges on the DynamicFS server can also start and stop the Dynamic File Service without rebooting by using the Service Controller.

The Service component must be installed and running on the server in order to connect to the server from the Management Console, or to use commands and some utilities. The `DswDump.exe` and `DswSyncPair.exe` utilities can be used when the service is running or not running in order to gather and report information from the Dynamic File Services databases. The Repair Tool can be used when the service is running or not running in order to repair the databases.

6.3.1 Viewing the Service Status

The Dynamic File Service has two possible states: *Enabled* (running) and *disabled* (not running). Its current status is displayed in the Service Controller menu. The Service status is also displayed in the Microsoft Management Console.

1 Log in to the DynamicFS server.

The Service Controller starts automatically and places an icon in the notification area.

2 In the notification area, right-click the Service Controller icon (🌐) to display the menu.

3 View the status of the Service.

The following combinations of options convey the current status and options to start or stop the Service accordingly:

- *Service Enabled* and *Stop Service*

✓	Service Enabled
	Stop Service

- *Service Disabled* and *Start Service*
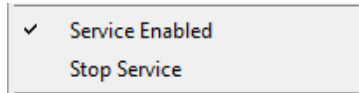
	Start Service
✓	Service Disabled
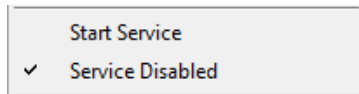
6.3.2 Starting the Dynamic File Service

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 Right-click the Service Controller icon ( ) in the notification area, then select *Start service* from the pop-up menu.

3 (Optional) Verify that the Service is running by right-clicking the Service Controller icon in the notification area.

In the pop-up menu, the options are now *Service enabled* and *Stop service.*

6.3.3 Stopping the Dynamic File Service

You must stop the Dynamic File Service before you attempt to modify, repair, or uninstall the Dynamic File Services software. You should also stop the Service gracefully before performing system maintenance. The Service is automatically restarted to apply changes that you make to the settings for the port, certificate, and merged view access.

- "Prerequisites for Stopping or Restarting the Service" on page 73
- "Stopping the Service" on page 74

Prerequisites for Stopping or Restarting the Service

Do not stop or restart the Dynamic File Service while the Service is scanning pairs, the Standard Policy engine is moving files in a policy run, users are accessing files via the merged view, or management tasks for pairs and policies are in progress.

- **Policy Runs:** You should wait until all pairs on the server are in the *Idle* state. If the pair state is *Running*, wait until the policy run is complete, or you can manually stop any policy runs that are in progress for a pair by using the *Actions > Stop running process* option from the pair's Statistics dialog box.

- **Scans:** You should consider the schedules for the daily snapshots of the pair and policy databases and the pair history scan to avoid stopping the Service when a pair is busy with a scan.

If a scan is in progress, wait until the scan is completed. If the Service is disabled at the scheduled start time, the scan is not run.

- ◆ **Merged View:** All clients accessing files through the merged view must log out. Gracefully close user connections to each of the pairs so that the merged view is inactive. This allows users time to save their changes and close the files.

- ◆ **Management Sessions:** Discontinue use of any Management Console sessions, client commands, and utilities.

After the Service activities are quiescent, you can continue with stopping or restarting the Service.

Stopping the Service

IMPORTANT: Before you begin, make sure that you have met the requirements in "Prerequisites for Stopping or Restarting the Service" on page 73.

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 In the notification area, right-click the Service Controller icon ( ), then select *Stop service* from the menu.

3 If you are prompted to confirm the Service stop, make sure that all users accessing files with the merged view have logged out, then click *Yes* to continue.

4 (Optional) Verify that the Service has stopped by right-clicking the Service Controller icon in the notification area.

When the service has stopped, Service Controller menu displays *Service disabled* and *Start service* options.

6.4 Configuring the Auditing Service

The Audit Configuration tool allows you to specify the Dynamic File Services management events that are audited for pairs and policies. By default, all of the pair and policy management events are tracked. Each of the selected events generates an audit record in the `..\Dynamic File Services\audit\DswAuditLog.xml` file each time the event occurs. The selected audit events apply globally to each of the pairs and policies on a server.

The Dynamic File Service can be running or not running when you select or deselect events to be audited in the Audit Configuration tool. It is not necessary to restart the Service to apply the changes.

Table 6-2 lists the configurable audit tracking events:

Table 6-2 *Configurable Audit Tracking Events*

Pair Management Events	Policy Management Events
Pair Created	Policy Created
Pair Unlinked	Policy Modified
Policy Associated to Pair	Policy Deleted
Policy Disassociated from Pair	Policy Associated to Pair
Added Exclude/Include Folders to Pair	Policy Disassociated from Pair
Removed Exclude/Include Folders from Pair	Policy Execute Now on Pair
Stop Running Processes on Pair	Policy Preview Now on Pair
Manual Move on Pair	Policy Scheduled to Run on Pair
Change Log Level on Pair	Policy Ran on Pair

To set up the audit tracking events:

1 Log in to the DynamicFS server as the Administrator user or a user with Administrator privileges.

The Dynamic File Services Controller begins automatically and places an icon in the Windows notification area.

2 Right-click the Service Controller ( ) icon, then select *Audit Configuration* to open the *Audit Tracking Events* dialog box.
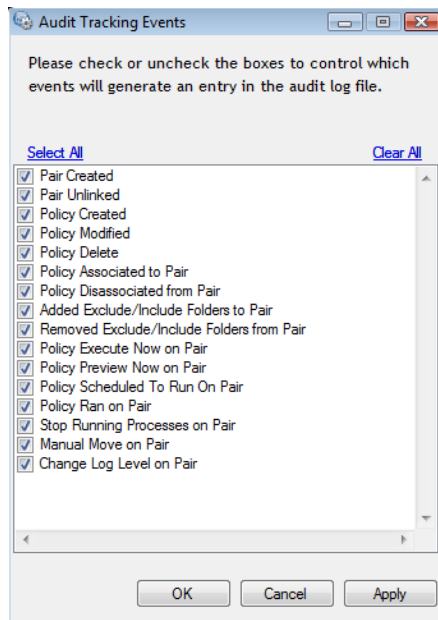
3 Select or deselect the check box next to an event type to control which events are tracked.

You can also use the *Select All* link to select all check boxes, or use the *Clear All* link to deselect all check boxes.

All events are selected by default. For a list of available audit events, see Table 6-2, "Configurable Audit Tracking Events," on page 75. Only the selected event types are tracked.

4 Click *Apply* or *Ok* to save and apply the changes.

The changes take effect without needing to restart the Service.

6.5 Configuring the Notification Service

Storage or system administrators might want to receive notices for Dynamic File Services pair and policy management events or for policy run events. The Notification Service allows you to configure which events trigger notifications and where the notification messages are sent. The notification messages include information about the event, such as the server name, pair name, policy name, a brief description of the event, and the event timestamp.

The Email add-on to the Notification Service allows you to set up one or multiple e-mail addresses where you want to send notifications about pair and policy events. The Global Events Configuration option allows you to specify which pair and policy events can trigger a notification. The selected notification events apply globally to each of the pairs and policies on a server.

The Dynamic File Service can be running or not running when you configure notifications. It is not necessary to restart the Service to apply the changes.

- Section 6.5.1, "Enabling or Disabling Notifications," on page 76
- Section 6.5.2, "Setting Up Notification Events," on page 76
- Section 6.5.3, "Setting Up E-Mail Notifications," on page 78

6.5.1 Enabling or Disabling Notifications

Notifications are disabled by default. Notification messages are sent only if notifications are enabled and a notification method has been configured.

To enable or disable notifications:

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 Right-click the Service Controller icon (🔵) in the notification area, then do one of the following:

- **Enable:** Select *Notification Configuration > Enable*.

  A check mark appears next to the *Enabled* field in the menu.

- **Disable:** Select *Notification Configuration > Disable*.

  A check mark appears next to the *Disabled* field in the menu.

3 Continue with Section 6.5.2, "Setting Up Notification Events," on page 76

6.5.2 Setting Up Notification Events

When notifications are enabled, you can use the *Global Events Configuration* option to specify the event types that trigger notifications. Notification messages for the selected events are sent to recipients only when notifications are enabled.

Table 6-3 lists the configurable notification events:

Table 6-3 *Configurable Notification Events*

Pair Management Events	Policy Management Events
Pair Created	Policy Created
Pair Unlinked	Policy Modified
Policy Associated to Pair	Policy Deleted
Policy Disassociated from Pair	Policy Associated to Pair
Added Exclude/Include Folders to Pair	Policy Disassociated from Pair
Removed Exclude/Include Folders from Pair	Policy Execute Now on Pair
Stop Running Processes on Pair	Policy Preview Now on Pair
Manual Move on Pair	Policy Scheduled to Run on Pair
Change Log Level on Pair (deselected by default)	Policy Ran on Pair

To configure the notification events:

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 Right-click the Service Controller icon (⬤) in the notification area, then select *Notification Configuration > Setup.*

The *Notification Setup* dialog box opens.
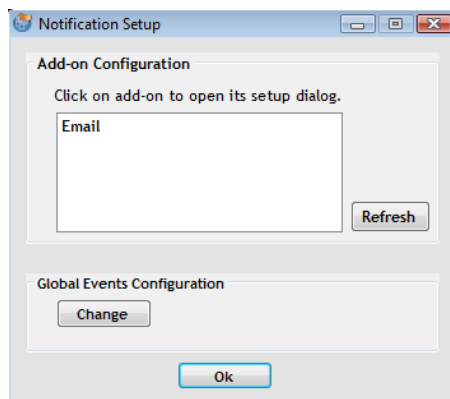
3 In the *Notification Setup* dialog box under *Global Events Configuration*, click *Change* to open the *Notification Events* dialog box.
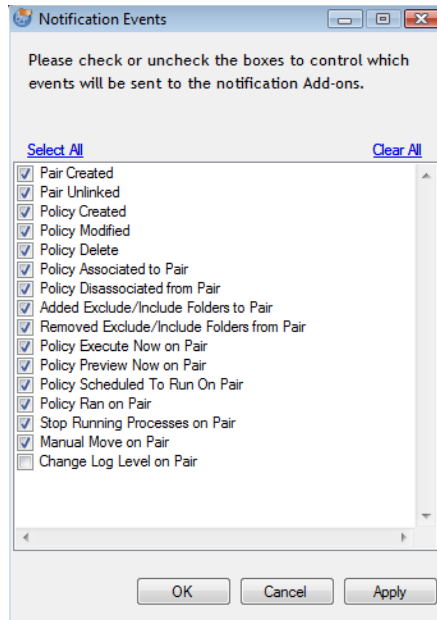
4 Select or deselect the check box next to an event type to control which events can trigger a notification.

You can also use the *Select All* link to select all check boxes, or use the *Clear All* link to deselect all check boxes.

All events are selected by default except *Change Log Level on a Pair*. For a list of available notification events, see Table 6-3, "Configurable Notification Events," on page 77. Only the selected event types trigger notifications.

5 Click *Apply* or *Ok* to save and apply the changes.

The changes take effect without needing to restart the Service.

6 Continue with Section 6.5.3, "Setting Up E-Mail Notifications," on page 78

6.5.3 Setting Up E-Mail Notifications

The Email add-on for the Dynamic File Services Notification Service allows you to set up one to nine e-mail addresses where you want to send notifications about pair and policy events. A single e-mail message is sent to all e-mail addresses.

Before you configure e-mail notifications, the following setup is required:

◆ **Outgoing Mail Service:** You must have an outgoing e-mail service to relay e-mail alerts and notifications.

The Email add-on supports the Simple Mail Transfer Protocol (SMTP), a standard server-to-server protocol that is used to transfer mail between computers. You need the DNS name of the SMTP mail server to use. You can also use an IPv4 IP address if your mail service provider allows it. The SMTP server must have Internet access if you want to send messages to external e-mail addresses.

◆ **Mail Relay:** You must configure the outgoing e-mail service to support and allow mail relay.

The Email add-on supports using either authenticated or anonymous SMTP relay. Your e-mail service provider must support and allow the method you choose.

When you use authenticated mail relay, you must provide a valid e-mail address and password to use for the notification sender. The e-mail address does not need to be the address of a specific individual. It can be a friendly address that is recognizable to recipients, such as `ndfs_administrator@example.com`.

The e-mail address is authenticated against the authentication mechanisms each time notification e-mails are sent. If the password changes for this account, you must update the password in the Email add-on.

◆ **Port:** You must specify the port number of the message submission port to use for the outgoing e-mail service. Typical outgoing ports are 25 and 587. If you have a firewall protecting your perimeter network, you must enable an exception for the port to make sure that the traffic is allowed to pass.

◆ **SSL:** Determine if your outgoing e-mail service provider requires SSL. Security-enhanced communication encrypts the SMTP session, including the user name, the password, and the message data by using SSL encryption.

To configure e-mail notifications:

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 Right-click the Service Controller icon ( ) in the notification area, then select *Notification Configuration > Setup.*

The *Notification Setup* dialog box opens.
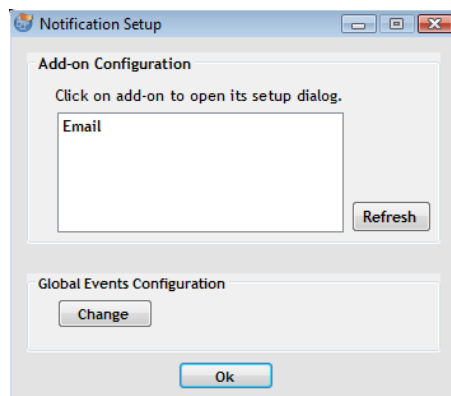
3 Under *Add-on Configuration*, click the Email add-on to open the *Mail Configuration* dialog box.

The Email add-on is disabled by default.
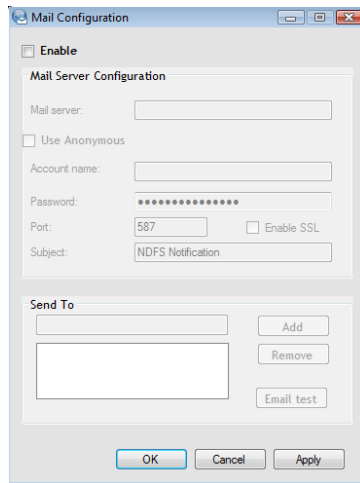
4 Click the *Enable* check box to enable the add-on.
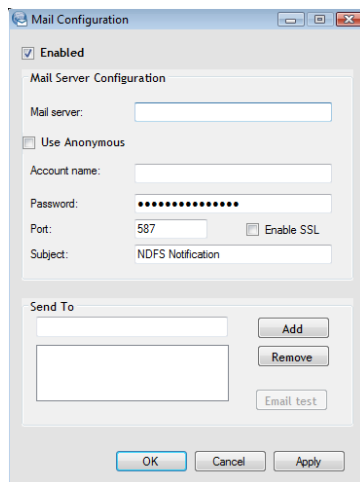
5 Under *Mail Server Configuration*, specify the outgoing e-mail server settings:

Mail Server Parameter	Description	Sample Value
Mail server	Specify the DNS name or IP address (IPv4 format) of the outgoing SMTP mail server used by your e-mail service provider.	smtp.example.com
Use anonymous	You can use anonymous mail relay only if it is supported by your mail service provider. Select the *Use Anonymous* check box. This option disables using an authenticated e-mail address.	

Mail Server Parameter	Description	Sample Value
Account name and password	If you use authenticated mail relay, specify an e-mail address and password for a valid account with the e-mail service provider. This address is used as the sender of outgoing e-mail messages.	bob@example.com password
Port	Specify the port number to use for outgoing e-mail messages that is required by your outgoing e-mail service provider. (Default: 587)	587
Enable SSL	Select the check box next to *Enable SSL* if your service provider requires SSL.	
Subject	Specify the text to use as the default portion of the subject in your outgoing e-mail notification messages. (Default: NDFS Notification) The server name and notification event type are automatically appended to this text.	SiteA NDFS Notification

6 Under *Send To*, specify one to nine e-mail addresses that receive e-mail notifications:

◆ **Add:** Type an e-mail address (such as bob@example.com), then click *Add*.

◆ **Remove:** Select an e-mail address in the list, then click *Remove*.
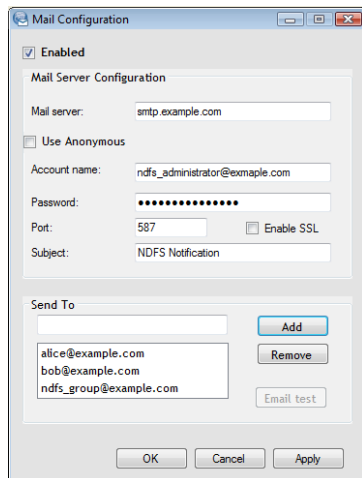
7 (Optional) Select an e-mail address in the list, then click *Email Test* to send a test message.

8 Click *Apply* or *Ok* to save and apply the changes.

The changes take effect without needing to restart the Service.

6.6 Configuring the Service Port

The Dynamic File Service uses port 8999 by default for remote communications between the Management Console (or DynamicFS commands) being run on one computer and the Dynamic File Service running on the server. If you change the port number on the server, you must reconfigure any saved server settings in the Management Console with the newly configured port number.

IMPORTANT: The Service is automatically restarted to apply changes to the Service port setting. Before you begin, make sure that you have met the requirements in "Configuring and Managing the Service" on page 69.

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 In the notification area, right-click the Service Controller icon, then select *Service Port Access*.
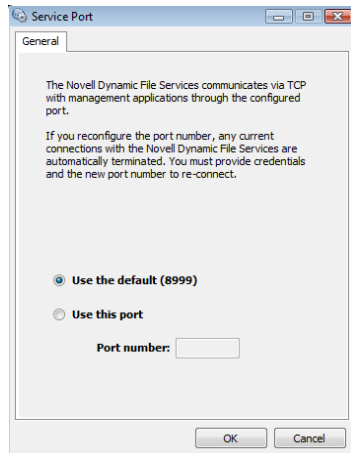
3 Select *Use the default port*, or specify the port number you want to use.

4 Click *OK* to save and apply your changes.

The Service restarts automatically to apply the changes.

5 If you are prompted to confirm the Service restart, make sure that all users accessing files with the merged view have logged out, then click *Yes* to continue.

If you click *No*, the port change is not made.

6 After a successful port change, the next time that you connect to the DynamicFS server from the Management Console or the command line interface, you must use the new configured port number when logging in.

The new configured port is saved in the server's settings in the Management Console server list.

6.7 Configuring Firewall Access for the Service Port

Dynamic File Services allows you to manage the pairs and policies on a server from a different computer when the *Windows Firewall Access* option is enabled (the default). When the option is enabled, Dynamic File Services configures an exception for the configured Service port in the Windows Firewall. When the option is disabled, it removes the firewall exception and the Service cannot be accessed remotely. Firewall access is not required for local management of pairs and policies.

- Section 6.7.1, "Understanding Remote Access," on page 83
- Section 6.7.2, "Enabling or Disabling the Windows Firewall Access," on page 84

6.7.1 Understanding Remote Access

The Windows Firewall allows you to specify exceptions to allow programs to communicate through the firewall. Inbound connections that do not have an exception are blocked. Exceptions to the Windows Firewall allow unsolicited inbound communications through the firewall. Use the *Dynamic File Service Controller > Windows Firewall Access* option to control whether an exception for the configured Service port is allowed in the firewall.

- "Allowing Remote Management" on page 83
- "Denying Remote Management" on page 84

Allowing Remote Management

You enable the *Windows Firewall Access* option to allow remote management of pairs and policies. This is the default setting after install. DynamicFS automatically adds an exception for the configured Dynamic File Service port to the *Windows Firewall > Exceptions* list. The Windows Firewall allows unsolicited inbound communications through the firewall on the configured port. This allows you to manage pairs and policies from another computer through the firewall on the configured Service port.

IMPORTANT: On Windows Server 2008 or later, DynamicFS creates a firewall exception for the *Domain* and *Private* network profiles. The network should be marked as *Private*, or both computers need to be part of a single domain.

For example, in the *Windows Firewall with Advanced Security > Inbound Rules*, the entry might look like this:

```
DswAccessPort
  Profile: Domain
  Enabled: Yes
  Action: Allow
  Override: No
DswAccessPort
  Profile: Private
  Enabled: Yes
  Action: Allow
  Override: No
```

To mark the network as *Private*, log in as a user with Administrator privileges on the machine, go to the *Network and Sharing Center*, click *Customize*, select *Private*, then click *OK*.

Dynamic File Services uses TCP communications over the configured Service port. You must specify the configured port when connecting to the server. If you modify the port number, DynamicFS automatically updates the firewall exception settings to use the new port. For information about changing the port to use, see Section 6.6, "Configuring the Service Port," on page 81.

By default, Dynamic File Services sets the scope of the port exception to *Any computer (including on the Internet)*. You can modify the scope option by going to the *Windows Firewall > Exceptions* page, double-clicking the *Dynamic File Services* exception, then selecting *Change Scope*. Alternative manual settings are *My network (subnet) only* and *Custom list*.

To allow remote management, enable the *Windows Firewall Access* option as described in Section 6.7.2, "Enabling or Disabling the Windows Firewall Access," on page 84.

Denying Remote Management

You disable the *Windows Firewall Access* option to deny remote management of pairs and policies. DynamicFS automatically removes any firewall exceptions from the *Windows Firewall > Exceptions* list that it created for the configured Dynamic File Service port. When the exception is removed, Windows Firewall denies unsolicited inbound communications on the configured port. This prevents you from connecting to the server for remote management sessions.

For security reasons, you might want to disable the exception when you are not actively managing the Dynamic File Service from another computer.

To deny remote management, disable the *Windows Firewall Access* option as described in .

6.7.2 Enabling or Disabling the Windows Firewall Access

IMPORTANT: Before you disable the Windows Firewall Access, close any remote Management Console or command line management sessions with the server.

To enable or disable the firewall exception for the configured Dynamic File Service port:

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 In the notification area, right-click the Service Controller icon, then select *Windows Firewall Access* to open the Firewall Access dialog box.
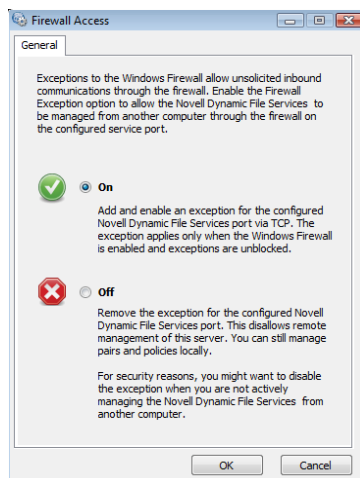
3 In the Firewall Access dialog box, select one of the following:

- ◆ **On (default):** Adds and enables an exception for the configured Dynamic File Service port via TCP. The exception applies only when the Windows Firewall is enabled and exceptions are unblocked.

- ◆ **Off:** Removes the exception for the configured Dynamic File Service port. This disallows remote management of this server. You can still manage pairs and policies locally.

4 Click *OK* to save and apply your changes.

6.8 Configuring a Certificate for Secure Remote Management Sessions

A Dynamic File Services Secure Sockets Layer (SSL) certificate is required to support secure remote sessions between a DynamicFS server and a computer running the Management Console. A self-signed certificate is automatically configured. You can also use the *Certificate Configuration* option in the Serviced Controller to create a new self-signed SSL certificate, or to specify your own signed certificate that you have acquired from a certification authority and added to the Local Computer Personal Store.

6.8.1 Understanding the Certificate

During remote management sessions, a Dynamic File Services SSL certificate is required in order for successful authentication to occur when connecting from the client to the server. The certificate helps assure the client that the server is the intended target. Dynamic File Services supports using self-signed and signed certificates. The remote connection uses standard RSA SHA-1 encryption with a 2048-bit key size.

Self-Signed Certificate

Dynamic File Services automatically creates a self-signed certificate during the install, and provides a Certificate Configuration option where you can create a new self-signed certificate.

The Dynamic File Services installation automatically sets up SSL support by doing the following:

- Creates a Dynamic File Services self-signed certificate (*servername*-DynamicFileServicesSSLCertificate).
- Stores the certificate in the `My` personal certificate store on the local machine.
- Binds the certificate for SSL use to the configured Dynamic File Service port (default 8999).

◆ Configures the following Windows Registry keys for Dynamic File Services in the
`HKEY_LOCAL_MACHINE/Software/Novell/Dynamic File Services/Setup/` folder:

Windows Registry Key	Description
DswSelfSignedCertEnabled	Indicates to the Dynamic File Service whether a signed DynamicFS SSL certificate is in use (value of 0), or if a DynamicFS self-signed SSL certificate is in use (value of 1). Valid values are 0 or 1. The default value is 1.
DswSSLCertThumbprint	Indicates to the Dynamic File Service the current configured certificate. Valid values are a 20-character hex value associated to the certificate. No spaces are permitted. This thumbprint must match the thumbprint of the certificate bound to the configured Dynamic File Service port.
DswSSLEnabled	Indicates to the Dynamic File Service whether SSL is enabled or disabled for the configured Dynamic File Service port. Valid values are 0 (disabled) or 1 (enabled). The default value is 1.

Signed Certificate

Dynamic File Services also supports using a signed certificate that you have acquired from a certification authority and added to the Local Computer Personal Store.

6.8.2 Viewing the Dynamic File Services SSL Certificate

You can view the Dynamic File Services SSL certificate (*servername*-DynamicFileServicesSSLCertificate) by using the Certificates snap-in for the Microsoft Management Console (MMC).

1 Log in to the DynamicFS server as an Administrator user or as a user with Administrator privileges.

2 From the *Start* menu, click *Run*, then type mmc and click *OK* to launch the MMC.

3 Add the Certificates snap-in to the MMC console and configure it to manage Computer Account certificates:

 3a On the *Console* menu, click *Add/Remove Snap-in*.

 3b Select *Certificates* in the *Snap-in* list, click *Add*, select *Computer Account* as the type of certificate you want to manage, then click *Finish* or *Close*.

 3c Click *OK* to close the Add/Remove Snap-in dialog box.

 The Certificates folder is now added to the MMC console.

4 In the Certificates management console, expand the certificate store, then click the *Certificates* folder to see the list of certificates in the store.

5 Right-click *servername*-DynamicFileServicesSSLCertificate, then click *Open* to open the Certificate dialog box.

 You can also view a certificate by double-clicking it.

6 The Certificate dialog box is organized into three tabs:

Tab	Description
General	Identifies the certificate's intended use.
Details	Displays the ITU-T X.509 standard fields, extensions, and properties of the certificate.
Certification Path	The certification path to the source where the certificate was issued.

7 Close the MMC console when you are done.

6.8.3 Prerequisites for Creating, Modifying, or Unbinding the Certificate

The Service is automatically restarted to apply changes made to the Dynamic File Services certificate. Before you attempt to create a new self-signed certificate, modify a signed certificate, or unbind a certificate, make sure you have satisfied all of the requirements for stopping the Service in "Prerequisites for Stopping or Restarting the Service" on page 73.

6.8.4 Creating a Dynamic File Services Self-Signed Certificate

You can use the *Dynamic File Services Certificate Configuration* option to create a new Dynamic File Services self-signed SSL certificate to replace the one created during the install. You might need to do this in the following situations:

- The current certificate is expiring.
- You unbind a signed certificate and want to replace it with a self-signed certificate.

IMPORTANT: The Service is automatically restarted to apply certificate changes. Before you begin, make sure that you have met the requirements in "Prerequisites for Stopping or Restarting the Service" on page 73.

To generate a self-signed certificate:

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 Make sure that no policy runs are in progress on the server, then stop the Dynamic File Service by right-clicking the Service Controller icon in the notification area and selecting *Stop Service*.

For information, see Section 6.3.3, "Stopping the Dynamic File Service," on page 73.

3 Confirm that the Dynamic File Service is stopped by right-clicking the Service Controller icon and verifying that the Service option reads *Service disabled*.

4 Open the Certificate Configuration dialog box by right-clicking the Service Controller icon and selecting *Certificate Configuration.*

5 In the Certificate Configuration dialog box, select *Create a new self-signed certificate*.

6 Click *OK* to save and apply your changes.

The Service restarts automatically to apply the changes.

7 If you are prompted to confirm the Service restart, make sure that all users accessing files with the merged view have logged out, then click *Yes* to continue with the Service restart.

If you click *No*, the certificate is not created.

8 View the message that confirms whether the configuration succeeded or failed, then click *OK* to close the message.

9 After a successful configuration, start the Dynamic File Service by right-clicking the Service Controller icon in the notification area, then selecting *Start Service*.

10 (Optional) Verify that the certificate was successfully bound to a particular port by using the Microsoft Management Console (MMC) to view the certificate as described in .

You can also enter one of the following Windows commands in a command prompt console that has administrator privileges. Select *Start > All Programs > Accessories*, right-click *Command Prompt*, then select *Run as Administrator*.

Windows Server 2003:

```
httpcfg.exe query ssl
```

Windows Server 2008:

```
netsh http show sslcert
```

If the certificate was successfully bound to the port, there is an entry for the certificate in the output response from this command.

6.8.5 Configuring a Signed Certificate for Dynamic File Services

You can use the *Dynamic File Services Certificate Configuration* option to replace the DynamicFS self-signed SSL certificate with one that you have obtained from a certification authority. Use this option if your enterprise security policy requires this level of security.

Additional steps are required when using a signed certificate. You must first generate a certificate signing request, import the certificate from the certification authority into the Local Computer Personal store, then assign the signed certificate to Dynamic File Services.

IMPORTANT: The Service is automatically restarted to apply certificate changes. Before you begin, make sure that you have met the requirements in "Prerequisites for Stopping or Restarting the Service" on page 73.

After you have obtained the certificate from the certification authority and imported it into the Local Computer Personal store:

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 Make sure that no policy runs are in progress on the server, then stop the Dynamic File Service by right-clicking the Service Controller icon in the notification area and selecting *Stop Service*.

For information, see Section 6.3.3, "Stopping the Dynamic File Service," on page 73.

3 Confirm that the Dynamic File Service is stopped by right-clicking the Service Controller icon and verifying that the Service option reads *Service disabled*.

4 Open the Certificate Configuration dialog box by right-clicking the Service Controller icon and selecting *Certificate Configuration*.

5 In the Certificate Configuration dialog box, select *Use your own SSL certificate from the local computer personal store*, select a certificate thumbprint from the drop-down list.

6 Click *OK* to save and apply your changes.

The Service restarts automatically to apply the changes.

7 If you are prompted to confirm the Service restart, make sure that all users accessing files with the merged view have logged out, then click *Yes* to continue with the Service restart.

If you click *No*, the certificate change is not done.

8 View the message that confirms whether the configuration succeeded or failed, then click *OK* to close the message.

9 After a successful configuration, start the Dynamic File Service by right-clicking the Service Controller icon in the notification area, then selecting *Start Service*.

10 (Optional) Verify that the certificate was successfully bound to a particular port by using the Microsoft Management Console (MMC) to view the certificate.

You can also enter one of the following Windows commands in a command prompt console that has administrator privileges. Select *Start > All Programs > Accessories*, right-click *Command Prompt*, then select *Run as Administrator*.

Windows Server 2003:

```
httpcfg.exe query ssl
```

Windows Server 2008:

```
netsh http show sslcert
```

If the certificate was successfully bound to the port, there is an entry for the certificate in the output response from this command.

6.8.6 Unbinding a Signed Certificate from Dynamic File Services

You can use the *Certificate Configuration* option in the Dynamic File Service Controller to unbind a signed certificate from the Service. You can create a new self-signed certificate or specify another signed certificate to replace the one currently in use.

IMPORTANT: The Service is automatically restarted to apply certificate changes. Before you begin, make sure that you have met the requirements in "Prerequisites for Stopping or Restarting the Service" on page 73.

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 Make sure that no policy runs are in progress on the server, then stop the Dynamic File Service by right-clicking the Service Controller icon in the notification area and selecting *Stop Service*.

For information, see Section 6.3.3, "Stopping the Dynamic File Service," on page 73.

3 Confirm that the Dynamic File Service is stopped by right-clicking the Service Controller icon and verifying that the Service option reads *Service disabled*.

4 Open the DynamicFS Certificate Configuration dialog box by right-clicking the Service Controller icon and selecting *Certificate Configuration*.

5 In the DynamicFS Certificate Configuration dialog box, do one of the following:

- Select *Create a new self-signed certificate*.

- Select *Use your own SSL certificate from the local computer personal store*, select a different certificate thumbprint from the drop-down list.

6 Click *OK* to save and apply your changes.

The Service restarts automatically to apply the changes.

7 If you are prompted to confirm the Service restart, make sure that all users accessing files with the merged view have logged out, then click *Yes* to continue with the Service restart.

If you click *No*, the certificate change is not done.

8 View the message that confirms whether the configuration succeeded or failed, then click *OK* to close the message.

9 After a successful configuration, start the Dynamic File Service by right-clicking the Service Controller icon in the notification area, then selecting *Start Service*.

10 (Optional) Verify that the certificate was successfully bound to a particular port by using the Microsoft Management Console (MMC) to view the certificate.

You can also use one of the following Windows commands in a command prompt console that has administrator privileges. Select *Start > All Programs > Accessories*, right-click *Command Prompt*, then select *Run as Administrator*.

Windows XP or Windows Server 2003:

```
httpcfg.exe query ssl
```

Windows Vista or Windows Server 2008:

```
netsh http show sslcert
```

If the certificate was successfully bound to the port, there will be an entry for the certificate in the output response from this command.

6.8.7 Handling Expiring Certificates

A Dynamic File Services self-signed SSL certificate is valid for five years from its creation date. As the date of expiration for a configured certificate nears, DynamicFS provides a notification message as you log in to the server from the Management Console. To replace the expiring certificate, use the *Certificate Configuration* option in the Service Controller to create a new self-signed certificate, or to set up a signed certificate that you have obtained from a certification authority.

6.9 Configuring the Merged View Access

The merged view of the primary and secondary paths gives users access to all of their files in a pair. The *Merged View Access* configuration option allows you to specify whether the merged view is available to users. The setting applies to all pairs on a server.

The following sections describe the option and how to modify it:

6.9.1 Understanding the Merged View Access

When the *Merged View Access* option is enabled (the default), the merged view is available for all pairs on the server. When users access the network share on the primary path, the files in both paths are available to them. This setting is preferred in most environments.

When the *Merged View Access* is disabled, the files in the secondary path are hidden from users. When users access the network share on the primary path, only files in the primary path are available to them. When a policy moves a file to the secondary path, the file disappears from the user's view of the data. The files can be made available to users by applying policies to move them back to the primary location, or by re-enabling the *Merged View Access* option.

You might want to disable the merged view in the following situations:

- You set up pairs in order to migrate files from the primary location to the secondary location where the files are no longer actively available to the users.

  For example, you want to migrate older files to a storage repository where they can be maintained and easily restored to users as required for compliance, legal discovery, or periodic file retention reviews.

- You are restoring files to the secondary location from backup media, and want to allow users to continue to work with files on the primary while the restore operation is in progress.

- If a problem occurs with the filter driver, which is the component that provides the merged view, users can continue to work with files on the primary location until the driver problem is resolved.

6.9.2 Enabling or Disabling the Merged View Access

IMPORTANT: The Service is automatically restarted to apply changes to the Merged View Access setting. Before you begin, make sure that you have met the requirements in "Prerequisites for Stopping or Restarting the Service" on page 73.

1 Log in to the DynamicFS server as the Administrator user or as a user with Administrator privileges.

2 In the notification area, right-click the Service Controller icon, then select *Merged View Access*.
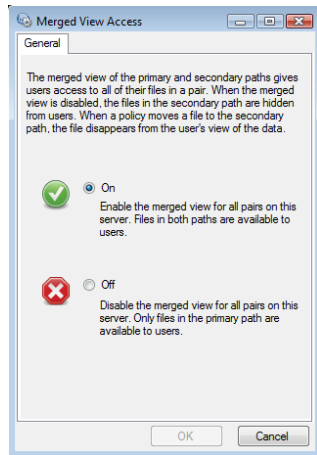
3 Select one of the following options:

On: (Default) Enables the merged view for all pairs on this server. Files in both paths are available to users.

Off: Disables the merged view for all pairs on this server. Only files in the primary path are available to users.

4 Click *OK* to save and apply your changes.

The Service restarts automatically to apply the changes.

5 If you are prompted to confirm the Service restart, make sure that all users accessing files with the merged view have logged out, then click *Yes* to continue with the Service restart.

If you click *No*, the change is not done.

6.10 Configuring the Logging Level for the Service and Standard Policy Log Files

Log level settings determine the type of events that are logged. The Server Properties dialog box allows you to set the logging levels for the Service (DswMcpCore.log) and Standard Policy (DswStandardPolicy.log) log files. The settings are written to the log configuration files for the Service (DswMcpCore.config.xml) and Standard Policy (DswStandardPolicy.config.xml).

The log level options are ordered from the most information reported to no information reported. Each level includes the events specified, plus the events of the levels below it. The messages are listed in order of increasing priority.

Log Level Option	Description
All	Record all events in the specified log file. (This is the same output as for the DEBUG level.)
DEBUG	Record debug, information, warning, error, and fatal events in the specified log file.
INFO	Record information, warning, error, and fatal events in the specified log file.
WARN	(Default) Record warning, error, and fatal events in the specified log file.
ERROR	Record error and fatal events in the specified log file.
FATAL	Record fatal events in the specified log file.
OFF	No events are recorded in the specified log file.

To view or change the Log Levels options:

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Right-click the server, then select *Properties* to open the Server Properties dialog box.

3 Click the *Log Options* tab.
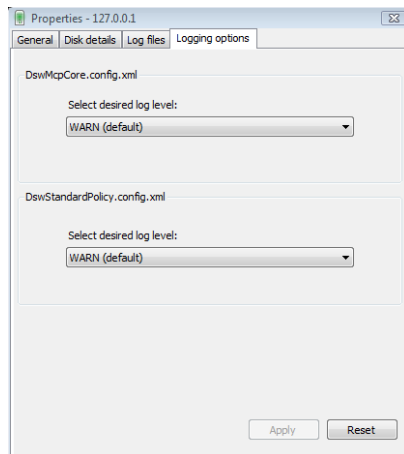
4 From the *Service* drop-down list, select a logging level for the Service log.

5 From the *Standard Policy* drop-down list, select a logging level for the Standard Policy log.

6 Click *OK* to apply the changes.

7 Close the Server Properties dialog box.

6.11 Finding Product Version and Build Information

The About box contains information about the software version and build.

1 Log in to the DynamicFS server.

2 Right-click the Service Controller icon in the notification area.

3 Select *About*.

4 View the following information:

- Company
- Company link
- Product
- Build number
- Installation folder
- Language
- Product version
- Copyright

6.12 What's Next

- Configure and log in to a DynamicFS server. For information, see Chapter 7, "Managing Servers in the Management Console," on page 95.
- Configure pairs on the server. For information, see Chapter 8, "Creating and Managing Pairs," on page 107.
- Configure policies to run on the pair. For information, see Chapter 9, "Creating and Managing Policies," on page 123.
- Monitor the health and history of server disks that are used in pairs, the pairs, and the policies. For information, see Chapter 10, "Monitoring Pairs and Policies," on page 157.

Managing Servers in the Management Console

7

You can set up one or more Novell Dynamic File Services (DynamicFS) servers in the Management Console. The Management Console can be running on the same or different computer than the server you want to manage. The configuration settings for the Service, pairs, and policies are stored locally on the server that you are managing. The information is available through the Management Console after you connect to the target server.

This section describes how to set up and manage the DynamicFS servers in the Management Console.

7.1 Setting Up a Server in the Management Console

The Dynamic File Services Management Console is used to manage pairs and policies for the servers where the Dynamic File Service is installed. The console can run on the same computer or a different computer in the same local area network.

7.1.1 Understanding the Server List

The Management Console keeps a list of the DynamicFS servers that you manage from a computer. If different administrator users log in to the same computer to use the Management Console, each user configures a list of servers to manage.

The list of configured servers (`DswUIServers.xml` file) is stored in the local application data folder for the currently logged-in user on the computer where the Management Console is running. This folder location is based on the operating system as follows:

Operating System	Server List Location
Windows Server 2008 Windows 7 Windows Vista	`C:\Users\`*`username`*`\AppData\Local\Dynamic File Services\DswUIServers.xml`
Windows Server 2003 Windows XP	`C:\Documents and Settings\`*`username`*`\Local Settings\Application Data\Dynamic File Services\DswUIServers.xml`

You can use the import and export features of the Management Console to set up the same server list for multiple administrator users on the same computer, or to set up the same list on different computers. For information, see Section 7.8, "Exporting and Importing a Server List," on page 104.

7.1.2 Prerequisites for Connecting to a Server

In order to connect to a Dynamic File Services server that you want to manage:

* The Dynamic File Service must be installed and running on the server you want to manage.

  For information, see Section 6.3, "Starting and Stopping the Service," on page 72.

* You must be able to provide the following information:
  * **Authentication Credentials:** You must log in to the server as a user that is a member of the `Dynamic File Services` group on the target DynamicFS server, or log in as the Administrator user on that server.

    For information about assigning users to the `Dynamic File Services` group, see Section 6.2.3, "Setting Up Administrators in a Workgroup," on page 72.
  * **DNS Name or IP Address:** You must provide the DNS name or IP address of the server. For local management, you can use `localhost` or `127.0.0.1` (the loop-back address).
  * **Service Port:** You must specify the port number that is configured on the server you want to manage. The default is port 8999.

* For remote management, an exception for the Dynamic File Service port must be enabled in the Windows Firewall on the server you want to manage.

  For information, see Section 6.7, "Configuring Firewall Access for the Service Port," on page 82.

7.1.3 Setting Up the Server

Use the Server Wizard to set up the connection and credentials information for the DynamicFS servers you want to manage.

1 In the Management Console, select *Servers* in the left panel, then click *Actions > Server Wizard*. You can also right-click *Servers* and select *Server Wizard*.
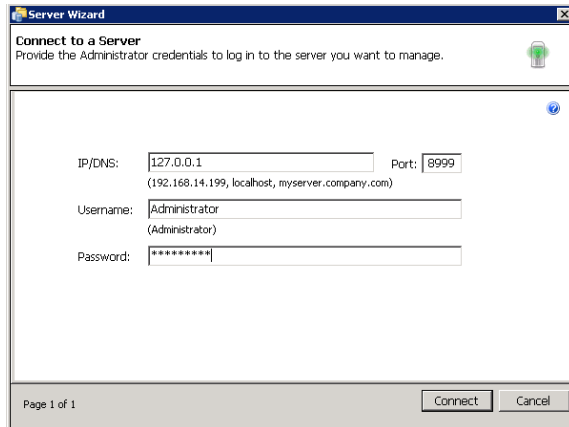
2 In the Server Wizard, provide the credentials of the Administrator user or a user that is a member of the `Dynamic File Services` group on the DynamicFS server that you want to manage.

Option	Description
IP/DNS	Type the IP address or the Domain Name Service (DNS) name of the DynamicFS server where you want to create a pair. The IPv4 format is supported for the IP address. DNS names are case sensitive.
Username	Type the username of the Administrator user or a user that is a member of `Dynamic File Services` group on the target server.
Password	Specify the password of the user you specified in the *Username* field. Passwords are case sensitive.
Port	Specify the port number that is configured for the server that you want to manage. The default Dynamic File Service port is 8999.

3 Click *Connect* to connect to the server.

4 If you are prompted to accept the Dynamic File Services SSL Certificate, view the certificate, then accept it if it is valid.

For information, see Section 7.2, "Accepting a Dynamic File Services Certificate," on page 98.

5 Verify that the server appears in the left panel under the *Servers* container.

You can disconnect from the server when you are not actively managing it. The server remains in the list.

7.2 Accepting a Dynamic File Services Certificate

The default name of the Dynamic File Services self-signed SSL certificate is
servername-DynamicFileServicesSSLCertificate. A self-signed certificate is valid for five
years from the date it is created.

The first time that you connect to a target DynamicFS server from the Management Console, you are
prompted to accept the certificate for the target server. If the server is in a Windows cluster, you are
prompted the first time that a connection is made to each node in the cluster.

The accepted certificate is added to your personal local computer certificates on the management
computer.

Each user that manages pairs and policies on the target server is prompted to accept the certificate
when connecting for the first time to the server.

- Section 7.2.1, "Importing a Certificate to the Default Location," on page 98
- Section 7.2.2, "Importing the Certificate to a Specified Location," on page 98

7.2.1 Importing a Certificate to the Default Location

By default, the SSL certificate is imported to the current user's Personal local computer store.

1 In the Certificate Validation dialog box, view the issuer information:
- Issued to
- Issued by
- Valid from MM/DD/YYYY to MM/DD/YYYY

2 Click *View* to view detailed information about the certificate.

3 In the Certificate Information dialog box, review the information on the *General*, *Details*, and
Certification Path tabs.

4 Close the Certificate Information dialog box.

5 In the Certificate Validation dialog box, click *Accept* to automatically install the certificate to
your Personal local computer store.

7.2.2 Importing the Certificate to a Specified Location

You can specify an alternate location to store the SSL certificate.

1 In the Certificate Validation dialog box, view the issuer information:
- Issued to
- Issued by
- Valid from MM/DD/YYYY to MM/DD/YYYY

2 Click *View* to view detailed information about the certificate.

3 In the Certificate Information dialog box, review the information on the *General*, *Details*, and
Certification Path tabs.

4 If the certificate is valid, on the *General* tab, click *Install certificate* to import the certificate on the local computer.

5 In the Certificate Import Wizard, follow the on-screen instructions to import the certificate.

6 Click *OK* to dismiss the Certificate Information dialog box.

7 Click *Accept* to close the Certificate Validation dialog box.

7.3 Connecting to a Server

After you set up a Dynamic File Services server to be managed as described in Section 7.1, "Setting Up a Server in the Management Console," on page 95, you can connect to the server whenever you want to manage its pairs and policies. Only one administrator at a time should be logged in to a DynamicFS server to manage its pairs and policies.

1 In the Management Console under *Servers*, select the IP address or DNS name of the server that you want to manage, then select *Actions > Connect*. You can also right-click the server name and select *Connect*, or double-click the server name.

The DynamicFS Login dialog box opens for the server.
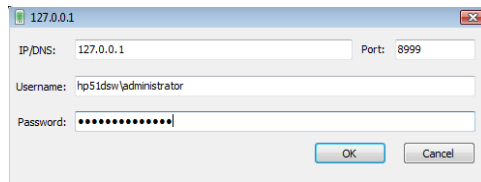
2 If the configured Dynamic File Service port has changed on the target server, specify the configured port.

3 Specify the username and password of the Administrator user or a user that is a member of the `Dynamic File Services` group on the target server.

4 Click *OK* to connect to the server.

When the server is connected, the *Server* icon (🖥) has a green glow in the upper half of the icon.

7.4 Viewing a List of Servers and Their Connection Status

The *Servers* container in the left panel of the Management Console lists all of the servers that you have previously set up on the computer where the Management Console is running. If different administrator users log in to the same computer to use the Management Console, each user configures a personal list of servers to manage. You might see different computers in the list, depending on the username you use when you log in to the desktop.

1 In the Management Console, select the *Servers* container (🗀) in the left panel to expand the list.

You must log in to a server to view the pairs and policies listed below an individual server's container.

2 View the current connection status of the servers.

The Server icon next to a server's IP address or DNS name indicates its connection status:

Server Connection State	Icon	Description
Disconnected		A gray server icon indicates that you are currently disconnected from the target DynamicFS server.
Connected		A green glow on the upper half of the server icon indicates that you are currently connected to the target DynamicFS server.
Connection is lost		A red glow on the lower half of the server icon indicates that you were connected to the server, but the connection has been lost. You must disconnect from the server, then connect to the server again.

7.5 Viewing Server Properties

The Server Properties dialog box in the Management Console retrieves and displays information about the Dynamic File Services servers that you are managing.

- Section 7.5.1, "Accessing the Server Properties," on page 100
- Section 7.5.2, "Viewing General Server Information," on page 100
- Section 7.5.3, "Viewing Disk Details for the Server," on page 101
- Section 7.5.4, "Viewing Log Files for the Server," on page 102
- Section 7.5.5, "Viewing Logging Levels for the Server," on page 103

7.5.1 Accessing the Server Properties

1 In the Management Console, connect to the DynamicFS server you want to manage.

2 In the left panel, select the server, then select *Actions > Properties*. You can also right-click the server, then select *Properties*.

The Server Properties dialog box opens.

3 Continue with Section 7.5.2, "Viewing General Server Information," on page 100.

7.5.2 Viewing General Server Information

1 In the Server Properties dialog box, select the *General* tab to view information about the server operating system and hardware:

Property	Description
System	The operating system and server time zone of the server.
Computer	Server processor and RAM on the server.
Domain	The fully distinguished name of the Active Directory domain, if the server is a member server or controller server in an Active Directory environment. For example: `DC=novell,DC=com`

Property	Description
Version	The release version of the Dynamic File Services software.

2 Continue with .

7.5.3 Viewing Disk Details for the Server

1 In the Server Properties dialog box, select the *Disk Details* tab to view a list of disks on the server and the *Used Space*, *Free Space*, and *Capacity* of each disk.
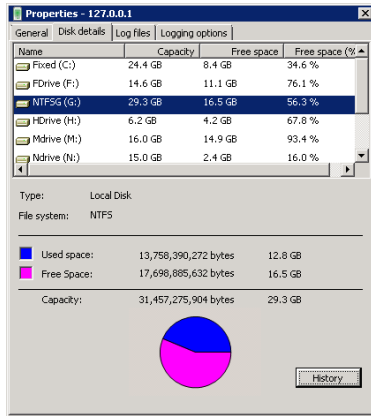
2 (Optional) For each disk, select the disk, then click *History* to view the history of the disk capacity and used space.
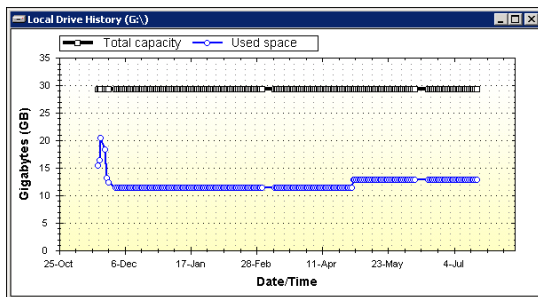
3 (Optional) Save the graphic display by right-clicking anywhere in a graphical area and selecting any of the following options:

- ◆ **Copy:** Copies the selected graph as an image to the clipboard. Open a graphics editor, paste the image, and save the file.

- ◆ **Save Image As:** Opens a Windows Save As dialog box where you can specify a location and filename for the image, select a file format, then save the file.

- ◆ **Page Setup:** Set up the page orientation (portrait or landscape) and printer information for printing the graph.

- ◆ **Print:** Print the selected graph.

4 Continue with Section 7.5.4, "Viewing Log Files for the Server," on page 102.

7.5.4 Viewing Log Files for the Server

1 In the Server Properties dialog box, select the *Log Files* tab to view log information for the following components on the target server:

- ◆ Dynamic File Service component (`DswMpcCore.log`)

- ◆ Standard Policy engine component (`DswStandardPolicy.log`)

- ◆ Install utility (`install.log`)

- ◆ Synchronize Pair utility (`DswSyncPair.exe`)

- ◆ File Inventory utility (`DswInventory.exe`)

Logs for the utilities are available after the utility has been run manually at least one time.
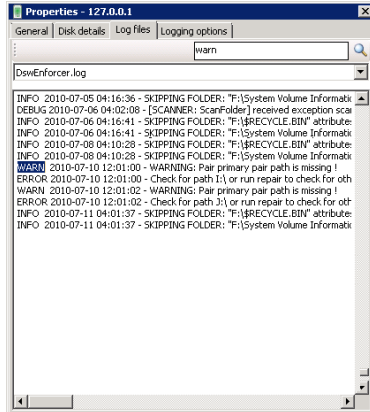
2 (Optional) Search for words in messages by using the Search feature. Type the word or characters, then click the Search icon to jump to each instance of the word in the log file.

3 Continue with Section 7.5.5, "Viewing Logging Levels for the Server," on page 103.

7.5.5 Viewing Logging Levels for the Server

1 In the Server Properties dialog box, select the *Logging options* tab to view the logging level settings for the Service and Standard Policy logs on the server.
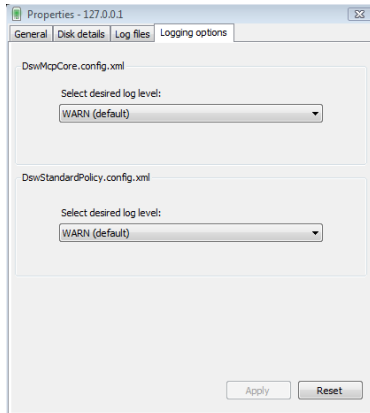
2 If you want to modify the logging levels, continue with Section 6.10, "Configuring the Logging Level for the Service and Standard Policy Log Files," on page 92.

7.6 Disconnecting from a Server

You can disconnect the Dynamic File Services Management Console from the target servers when you are not actively monitoring or managing pairs and policies on them. You might also need to disconnect from a server in order to reconnect to it if the connection is lost during a management session.

1 In the Management Console, if a wizard is open, complete the setup or click *Cancel* to gracefully close the in-progress setup process.

2 In the Management Console under *Servers*, select the DynamicFS server that you want to manage.

3 Select *Actions > Disconnect*. You can also right-click the server name and select *Disconnect*.

When the server is disconnected, the Server icon is dimmed (🔲). All open Properties or Statistics windows for that server are automatically closed.

7.7 Recovering a Lost Connection to a Server

If a connection is lost while you are managing a Dynamic File Services server, the server status changes from Connected (with a green glow on the server icon 🟩) to Connection Lost (with a red glow on the server icon 🟥). Possible reasons for a lost connection are:

- The Service is disabled on the target server.
- The configured Service port is modified on the target server.
- The Windows Firewall exception is disabled on the target server, which denies remote connections.

- A network outage occurs for a remote connection.
- The username that was used to establish the connection is removed from the `Dynamic File Services` group on the target server.

You must disconnect from the server, then connect to the server again to start a new management session. Restart any management tasks that were in progress.

1 In the Management Console under *Servers*, select the DynamicFS server that you want to manage.

2 Select *Actions > Disconnect*. You can also right-click the server name and select *Disconnect*.

When the server is disconnected, the Server icon is dimmed (▯). All open Properties or Statistics windows for that server are automatically closed.

3 Select *Actions > Connect*. You can also right-click the server name and select *Connect*.

4 Provide the login credentials, then click *OK*.

7.8 Exporting and Importing a Server List

The Dynamic File Services Management Console allows you to export and import a server list. This allows you to set up the same list of servers on multiple computers or for multiple administrator users on the same computer.

The *Export server list* option allows you to export a server list to an `.xml` file in a local folder. The default filename is `DswServersList.xml`.

The *Import server list* option allows a currently-logged-in administrator user to import an exported server list to add the servers to a server list that is stored in the user's personal local application data folder. You can also copy an exported list to another computer where the Management Console is installed, then import the server list for use on that computer.

- Section 7.8.1, "Exporting a Server List," on page 104
- Section 7.8.2, "Importing a Server List," on page 104

7.8.1 Exporting a Server List

1 In the left panel of the Management Console, select the *Servers* container.

2 Select *File > Import/Export > Export server list*.

3 Browse to the location on the computer where you want to save the file, specify a name for the file, then click *Save*.

By default, the list of servers is exported in the `DswServersList.xml` file.

4 (Optional) Copy the file to portable storage media that can be used on different computers, then continue with Section 7.8.2, "Importing a Server List," on page 104 to use the list as a different user on the same computer or on a different computer.

7.8.2 Importing a Server List

1 Log in to the Windows server or client where the Management Console is installed.

Log in with the username that you will be using when you use the Management Console.

2 Place a copy of the exported servers list (`DswServersList.xml`) on the computer where you are managing DynamicFS.

3 In the left panel of the Management Console, select the *Servers* container.

4 Select *File > Import/Export > Import server list*.

5 Browse to the location on the computer where you placed the `DswServersList.xml` file, then click *Open*.

The list of imported servers is added to the *Servers* container in the left panel. The servers are added to the server list (`DswUIServers.xml` file) that is stored in the local application data folder for the currently logged-in user.

7.9 Removing a Server from the List

You can remove DynamicFS servers from the *Servers* list. You might need to remove a server from the list if the target server is no longer running Dynamic File Services, or if you are no longer responsible for managing pairs and policies on the server.

1 In the Management Console, if a wizard is open, complete the setup or click *Cancel* to gracefully close the in-progress setup process.

2 In the Management Console under *Servers*, select the DynamicFS server that you want to manage.

3 If you are connected to the server, disconnect from it by selecting *Actions > Disconnect*. You can also right-click the server name and select *Disconnect*.

When the server is disconnected, the Server icon is dimmed ( ).

4 Select the server, then select *Actions > Remove server*. You can also right-click the server name and select *Remove server*.

The server no longer appears in *Servers* list for the currently-logged-in user.

7.10 What's Next

- Configure pairs on the server. For information, see Chapter 8, "Creating and Managing Pairs," on page 107.

- Configure policies to run on the pair. For information, see Chapter 9, "Creating and Managing Policies," on page 123.

- Monitor the health and history of server disks that are used in pairs, the pairs, and the policies. For information, see Chapter 10, "Monitoring Pairs and Policies," on page 157.

Creating and Managing Pairs

8

Novell Dynamic File Services (DynamicFS) transparently manages two storage locations as a single logical data storage repository referred to as a *pair*. This section describes how to create and manage pairs.

8.1 Understanding Pairs

A pair consists of two separate and independent paths in the storage systems that are available to a server where the Dynamic File Service is installed. DynamicFS logically links the two paths to act as a single storage area from the users' point of view. You can create up to 16 pairs on the same server.

The two paths in a pair are referred to as *primary* and *secondary*. The primary location typically contains the most important and most used files. The secondary location typically contains less critical or seldom-used files, very large files, or files that change infrequently. However, it is up to the administrator to determine what files should reside in each location.

Both the primary and secondary locations can reside on devices that are attached directly to the server or via Fibre Channel and iSCSI connections. In addition, the secondary path can reside on remote devices such as network filers. The secondary path might also be on iSCSI devices that are connected over lower-speed connections such as cloud-based iSCSI. The primary location typically resides on higher-performance storage hardware than the secondary location.

The Dynamic File Services filter driver works with a network share on the primary path to give users a merged view of the files on both the primary and secondary locations.

For example, Figure 8-1 shows a primary path of `C:\primary`, a secondary path of `F:\secondary`, and the merged view of the files in the pair as seen by the users via the network share.

Figure 8-1 *Merged View of the Primary and Secondary Paths*
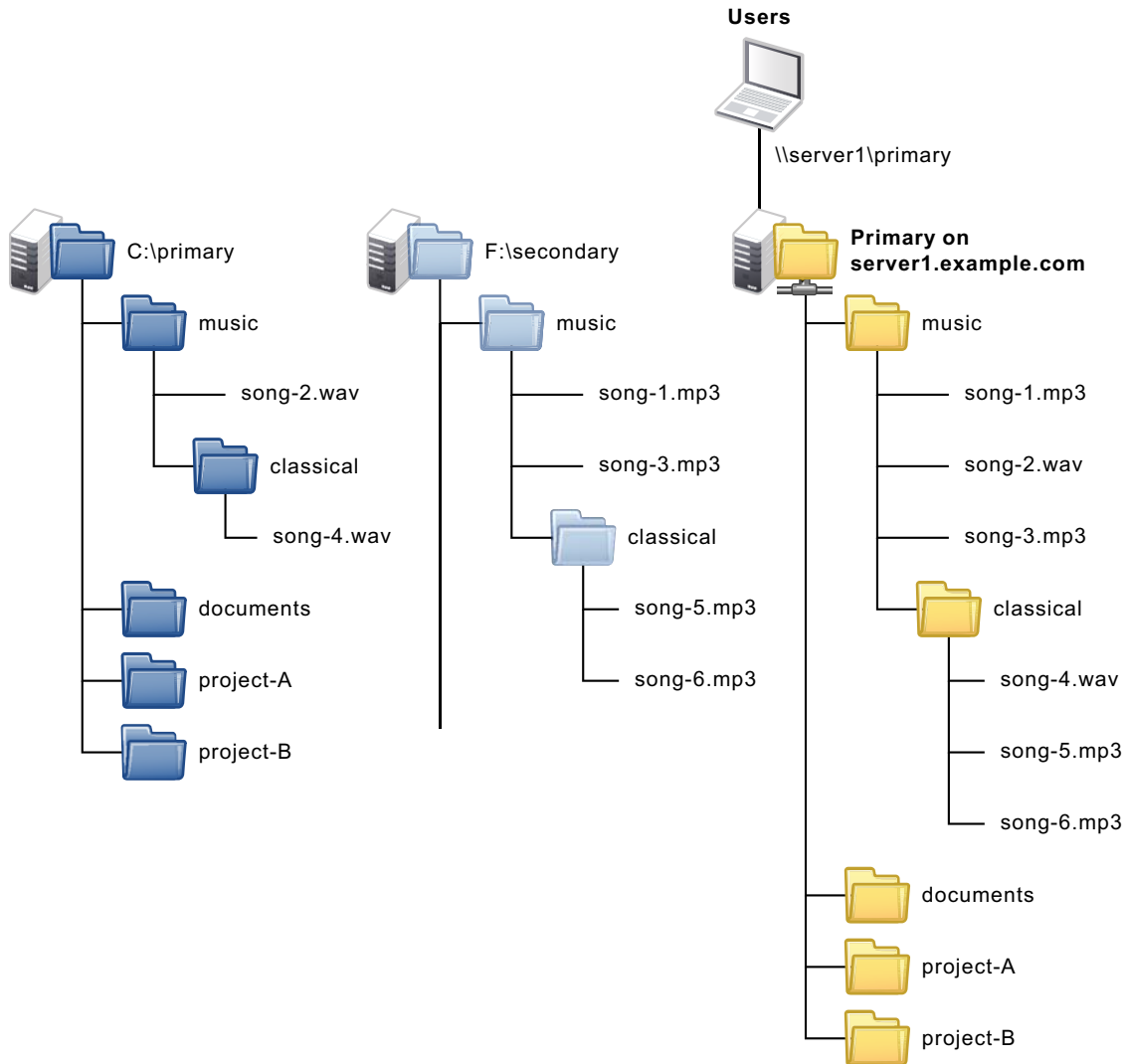
The merged view is not automatically presented to users of a pair. To enable users to see the merged view, you must do the following:

◆ You must use the Microsoft Network Share tool to create a network share on the primary path.

For requirements and guidelines, see Section 4.12, "Merged View for Users," on page 46.

◆ The Merged View Access option must be enabled (the default setting) for the server where the Dynamic File Service is running.

For information, see Section 6.9, "Configuring the Merged View Access," on page 91.

8.2 Creating a Pair

Two wizards are available for configuring Dynamic File Services pairs:

◆ **Setup Wizard:** Sets up a new pair, a new policy for the pair, and automatically associates the pair and policy. The pair is not created until the policy is configured and you click *Finish*. The associated policy is enforced for the pair at its next scheduled run, or you can start policy runs manually by using *Execute now*.

The Setup Wizard opens automatically when you connect to a DynamicFS server if there are no pairs or policies currently defined for the server. The Setup Wizard is convenient to use when you want to create a new pair and its policy at the same time. You can associate additional policies later.

◆ **Pair Wizard:** Sets up a new pair and allows you to select none, one, or multiple existing policies to associate with the pair. The associated policies are enforced for the pair at their next scheduled runs, or you can start policy runs manually by using *Execute now*. You can associate additional policies later.

IMPORTANT: No data is moved between the primary and secondary locations in a pair until you set up policies to do so.

1 If you plan to use a remote share when creating a pair, create the share in the secondary location.

Shares in an Active Directory Domain: You must publish the share as described in Section 8.3, "Preparing Remote Shares for Use in a Pair," on page 112. Make sure your system meets the requirements in Section 4.10, "Remote Shares as Secondary Paths in an Active Directory Domain," on page 43.

Shares in a Workgroup: Make sure your system meets the requirements in Section 4.11, "Remote Shares as Secondary Paths in a Workgroup," on page 44.

2 In the Management Console, connect to the DynamicFS server that you want to manage.

3 Launch the Setup Wizard or the Pair Wizard:

◆ **Setup Wizard:** Select the server, then select *Actions > Setup Wizard*. You can also right-click the server, then select *Setup Wizard*.

If no pairs or policies exist on the server when you connect to it, the Setup Wizard opens automatically.

◆ **Pair Wizard:** Select the *Pairs* folder, then select *Actions > Pair Wizard*. You can also right-click the *Pairs* folder, then select *Pair Wizard*.

The wizard opens to the Pair Paths page.
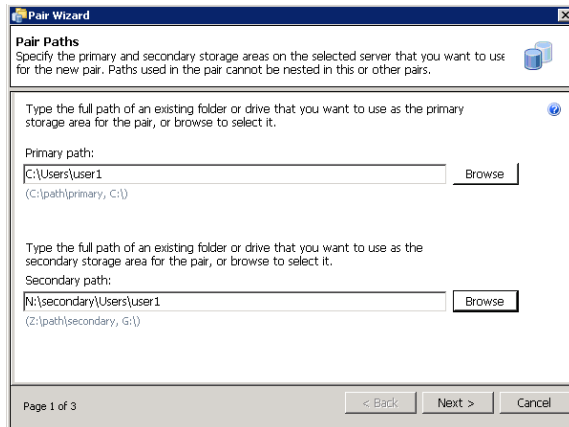
4 On the Pair Paths page, specify the paths to use for the pair.

Paths used in the pair cannot be nested in this pair or other pairs.

　4a Browse to select the primary path.

　4b Browse to select a local path or a remote share as the secondary path.

　　Remote shares are visible in the browser only if they have been published in Active
　　Directory. For information, see Section 8.3, "Preparing Remote Shares for Use in a Pair,"
　　on page 112.
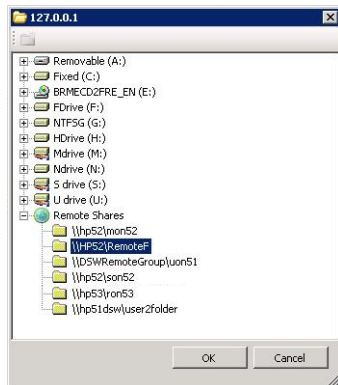
　　You can alternately type the UNC path of a local or remote share. The path name entry is
　　case-insensitive for local paths, but it is case-sensitive for remote paths.

　4c Click *Next* to continue.

5 If a network share does not exist on the primary path, a message pops up to remind you that the
share is required in order to give users a merged view of the files. Click *OK* to dismiss the
message.

You can create the share later. For information, see Section 8.4, "Providing Users with Merged
View Access to Files in a Pair," on page 113.

6 On the Pair Name page, specify a unique name (up to 32 characters) for the pair on the selected server.

For information, see Section 4.13, "Naming Conventions for Pairs and Policies," on page 47.
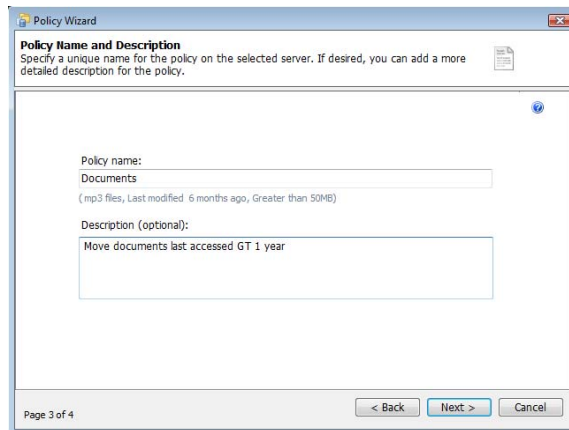
7 On the Pair to Policy Association page, select none, one, or multiple policies to associate with the new pair.
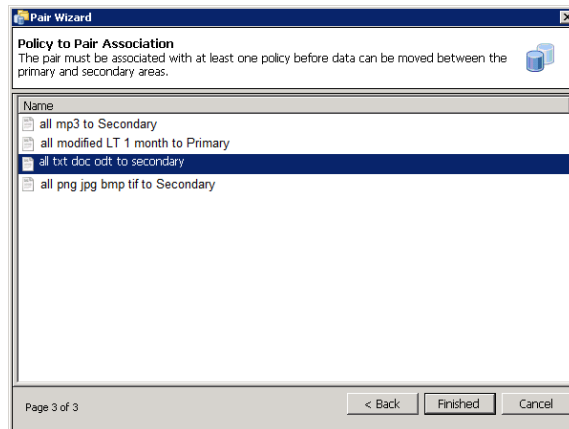
8 If you are using the Setup Wizard, create a policy for the pair:

For details, see Section 9.2, "Creating a Policy," on page 130.

  8a On the Policy Rules page, specify the direction and filter options to apply for this policy, then click *Next*.

  8b On the Policy Schedule page, specify the schedule options, then click *Next*.

  8c On the Policy Name and Description page, specify a unique name for the policy on the selected DynamicFS server, optionally add a more detailed description for the policy, then click *Next* to continue.

  8d The policy is automatically associated with the pair.

9 Click *Finished*.

The pair is created and appears in the *Pairs* list for the server.

If you used the Setup Wizard, the new policy is created and appears in the *Policies* list for the server. If you scheduled the policy, the policy rules are enforced for the pair at the next scheduled run time of the policy. Unscheduled and scheduled policies can be run manually by using the *Execute Now* option.

10 (Optional) Use any of the following methods to associate the pair with other policies.

   ◆ **Policy Wizard:** Use the Policy Wizard to create a new policy and associate it with the pair.

   ◆ **Pair Properties > Associations:** Use the *Pair Properties > Associations* tab to select one or more policies to associate with a selected pair. For information, see Section 9.5.4, "Associating or Disassociating Policies with a Selected Pair," on page 137.

   ◆ **Policy Properties > Associations:** Use the *Policy Properties > Associations* tab to select one or more pairs to associate with a selected policy. For information, see Section 9.5.3, "Associating or Disassociating Pairs with a Selected Policy," on page 136.

11 If a network share does not exist on the primary path, continue with Section 8.4.1, "Creating a Network Share for the Primary Path," on page 114.

8.3 Preparing Remote Shares for Use in a Pair

In an Active Directory environment, Dynamic File Services 1.6 allows you to use a remote share as the secondary path in a file. A remote share must be published in Active Directory before you can specify it as the secondary path in a pair. To do this, you must share the folder as a network share, publish the remote share in Active Directory, then add the Dynamic File Services Storage Rights group to the share and grant it all permissions.

IMPORTANT: For requirements and guidelines for using remote pairs, see Section 4.10, "Remote Shares as Secondary Paths in an Active Directory Domain," on page 43.

   ◆ Section 8.3.1, "Creating a Network Share on the Remote Device," on page 112
   ◆ Section 8.3.2, "Publishing the Remote Share," on page 112
   ◆ Section 8.3.3, "Adding the DFSStorageRights Group to the Remote Share," on page 113

8.3.1 Creating a Network Share on the Remote Device

1 On the remote device, locate the folder you want to use as the secondary path.

2 Right-click the folder, then choose *Sharing*.

3 Configure the share properties as needed to control access to the share.

4 If the share resides on an NTFS volume, configure the NTFS permissions for the share and any subfolders to fine-tune security as needed.

5 Continue with Section 8.3.2, "Publishing the Remote Share," on page 112.

8.3.2 Publishing the Remote Share

After the folder is shared on the remote device, you can publish it in Active Directory.

1 Open the Active Directory Users And Computers tool on the server that will host your primary path.

2 Select the *Computers* link to view the member servers in your Active Directory environment.

3 Locate the container in which you want to publish the folder, right-click the container, and choose *New > Shared Folder*.

4 Specify the resource name.

The resource name is the name by which the shared folder is listed in the folder and the name Dynamic File Services sees when it accesses the folder.

5 Specify the share name in UNC form, such as `\\`*`servername`*`\`*`sharename`*.

6 Do the following to just make sure that the publishing of the share worked.

Net Use a drive to the server with the remote share.

```
net use * \\servername\sharename
```

7 Continue with .

8.3.3 Adding the DFSStorageRights Group to the Remote Share

After you create the remote share and publish it in Active Directory, you must add the `DFSStorageRights` group to the remote share and grant the group all permissions. Alternately, you can use the `NDFS-<`*`servername`*`>` proxy user described in .

1 Add the Dynamic File Services Storage Rights (`DFSStorageRights`) group to the remote share.

2 Grant the group all permissions.

8.4 Providing Users with Merged View Access to Files in a Pair

Dynamic File Services allows users to access files on both the primary and secondary paths via a network share that you create for the primary path. When users access the share, they see a merged view of the file trees for the primary path and the secondary path. The merged view gives users access to all of their files in a pair. In addition, the *Merged View Access* configuration option allows you to control at a server level whether users can see the merged view of files or see only the files on the primary path.

-
-

8.4.1 Creating a Network Share for the Primary Path

Use *Windows Network Sharing and Security* to create a network share on a Dynamic File Services pair's primary storage location. When users map a drive on their computers to the share, they can see a merged view of the files stored on the pair.

- A network share is needed on the primary path in order to provide a merged view of the pair. You can add shares above or below the network share for the primary path.

- Network shares on, above, or below the secondary path should be removed, or they must be restricted from direct access by users.

To create a network share:

1 Use *Windows Network Sharing and Security* to create a network share on the primary storage location.

See the Microsoft Windows documentation for information about how to set up network sharing on the computers where DynamicFS is running.

2 Map a drive to the network share, and verify that the users can see a merged view of the two locations that make up the pair.

8.4.2 Setting the Merged View Access Option

By default, the *Merged View Access* option is enabled so that users see the merged view of files on the primary and secondary paths. This setting is preferred in most environments. It applies to all pairs on the server.

Disabling the *Merged View Access* option causes the files on the secondary location to be hidden from users. When users access the network share for a pair, only the files on the primary path are available to them.

For information and instructions, see Section 6.9, "Configuring the Merged View Access," on page 91.

8.5 Including or Excluding Folders from a Pair's Policy Runs

For a Dynamic File Services pair, you can specify one or more folders in the pair path that you want to include or to exclude from the policy runs. For a given pair, you can include folders, or you can exclude folders, but not both. The include/exclude setting applies only to the policies for the pair that are run against the primary path. That is, the include/exclude feature applies to policies that are moving data with a *Direction* setting of *Primary to Secondary*.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Right-click the pair that you want to manage, then select *Properties* to open the Pair Properties dialog box.

3 Select the *Include/Exclude* tab.
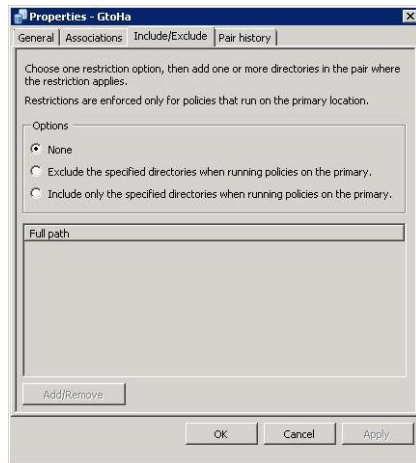
4 In *Options*, select only one of the following restriction options per pair:

None: The *Include/Exclude* option is disabled for the pair.

Exclude: Enable the *Exclude* option. Policies do not consider any content in the specified folders in the pair for policies that run on the primary path.

Include: Enable the *Include* option. Policies run only on the specified folders in the pair for policies that run on the primary path.

5 For each path in the pair where you want to apply the restriction, click *Add* to browse to and select a path to be restricted, then click *OK*.

The browser presents the folders on the primary path from which you select the folders to be included or excluded.

6 For each path in the pair where you want to remove the restriction, click *Remove* to browse to and select a path to be restricted, then click *OK*.

8.6 Viewing a List of Pairs

You can use the Dynamic File Services Management Console to view a list of all of the pairs that are defined for a server.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 In the left panel, select the *Pairs* folder (🗁) for the server, then view the list of pairs (🗐) in the right panel.

The *Pairs* list reports the following information for each pair:

- ◆ *Pair name*
- ◆ *Status* (*Idle*, *Running*)
- ◆ *Primary Path*
- ◆ *Secondary Path*
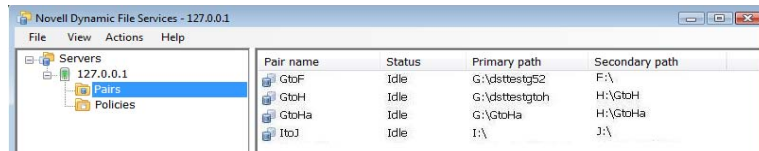
3 Click a column heading to sort the list by that parameter.

8.7 Viewing the Pair Status

The pair status indicates whether a Dynamic File Services file scan is being run against the pair at that time. Status conditions are reported as *Idle* or *Running*. Scans that might be in progress include scans for policy runs and the disk history. Only one scan at a time can be run against a pair.

Some actions, such as stopping the Service, require that all pairs be idle before you perform the action.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 In the left panel, select the *Pairs* folder ( ) for the server, then view the list of pairs in the right panel.

A pair's status (*Idle*, *Running*) appears to the right of the pair name.

8.8 Viewing Properties for a Pair

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Select the *Pairs* folder for the server, then view the list of pairs that are defined.

3 Right-click a pair, then select *Properties*.

The Properties dialog box opens to the *General* tab. It reports the following information:

- ◆ *Pair name*
- ◆ *Primary*
    - ◆ *Type* (the device type)

◆ *Primary path*

  ◆ *Share name*

  ◆ *Secondary*

  ◆ *Type* (the device type)

  ◆ *Secondary path*

4 Click the *Associations* tab to view a list of the policies that are currently associated with the pair. You can also add and remove policies from the *Policy associations* list.
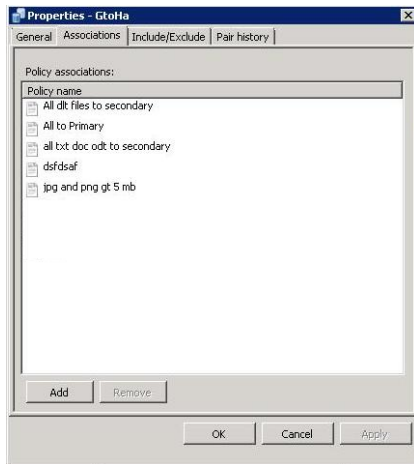
5 Click the *Include/Exclude* tab to view a list of directories on the primary path of the pair that are either included or excluded from policy runs. You can also add and remove directories from the include or exclude list.
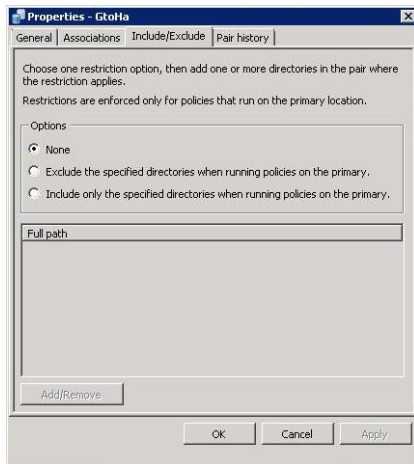
For information, see Section 8.5, "Including or Excluding Folders from a Pair's Policy Runs," on page 114.

6 Click the *Pair history* tab to view or modify the frequency and time that the pair history scan is run.
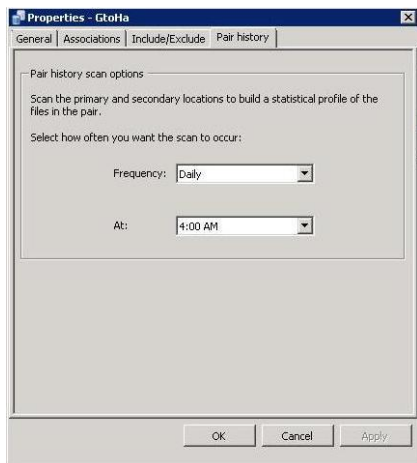
For information, see Section 8.10, "Scheduling the Pair History Scan," on page 119.

8.9 Moving Selected Files or Folders

The Manual Operations option for a pair allows you to build a list of files and folders that you want to move between the two paths. The specified files or folders are moved immediately. This is a one-time selection and move of the specified files. The display for selection supports up to 50,000 files in a folder, and shows them in groups of 10,000 at a time.

1 In the Management Console, connect to the server you want to manage.

2 Select the pair, then select *Actions > Properties* to open the Pair Properties dialog box.

3 On the *Manual* tab, click *Manual operations* to open the Manual Operations dialog box.

4 Create a list of the files and folders that you want to move manually.

    4a At the top of the page, specify the direction that you want to move the files and folders that you will add to the list.

    The manual operation moves files in one direction at a time. The direction determines which path you can browse for files to be moved:

Direction	Path to Browse
Primary to secondary	Primary path
Secondary to primary	Secondary path

    4b Under the list, click *Add files* to open a file browser interface for the selected path.

    4c Browse to locate the file or folder you want to move, then select it by checking the box next to it.

    You can select multiple files and folders at a time.

    If you select a folder, the folder's entire contents will be moved, including any subfolders in it.

    4d Click *OK* to add the selected folders to the list.

    The selected files and folders are appended to the list as you add them.

4e You can remove files or folders from the move list by selecting the entry in the list, then clicking *Remove files*.

4f Review the compiled list of files and folders to make sure it is accurate, and repeat the *Add files* and *Remove files* options as needed.

5 Do one of the following:

- ◆ **OK:** Click *OK* to move the specified files and folders now.

- ◆ **Cancel:** Click *Cancel* to abandon the procedure. The list you created is not retained.

8.10 Scheduling the Pair History Scan

The Dynamic File Services File System Inventory utility scans each pair on the server to collect file statistics for the pair history. History scans can be run hourly, daily (default), or weekly. By default, the history scan runs once daily at 4:00 a.m. The scans are run until completion. You can configure the scan to run more or less often on a given pair by configuring the pair's Pair History Scan.

To change the frequency and time of day the Pair History Scan on a given pair:

1 In the Management Console, connect to the server you want to manage.

2 Select the pair, then select *Actions > Properties* to open the Pair Properties dialog box.

3 Select the *Pair History* tab.

4 Specify the frequency and the time to run.

Hourly: The scan runs every hour on the hour.

Daily: The scan runs once daily at the specified starting hour. Select a time between midnight and 11:00 p.m. The default is 4:00 a.m.

Weekly: The scan runs once weekly on the specified day and starting hour. Select a time between midnight and 11:00 p.m. The default is Sunday at 4:00 a.m.

8.11 Reporting Conflicts for Attributes and ACL Permissions on Folders

You should use the merged view when setting attributes and ACL (access control list) permissions on folders in a Dynamic File Services pair. In a pair, an instance of each folder is stored in both the primary path and the secondary path as files are moved between the two paths.

For information about how metadata on the two folder instances can become out of synchronization, see Section 4.16, "Duplicate Folders," on page 48.

To identify conflicts for attributes and ACL settings on folders, you can run the DynamicFS Synchronize Pair tool (DswSyncPair.exe) with the -folders option to detect the metadata differences between the two instances of a folder and report them. You must log in as a user with rights to all of the paths in the pair. For information, see "Dynamic File Services Synchronize Pair Utility" in the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.

1 Log in to the DynamicFS server as a user with file system rights on the primary and secondary paths in the pair you want to manage.

If remote shares are being used, make sure that you have sufficient access rights on the secondary locations.

2 Open the Management Console, select the pair, then verify that the pair status is in the Idle state.

Policies must not be running against the pair when you start the Synchronize Pair utility. If policies are running, wait until they are done, or stop them manually. Wait until the pair status is idle before continuing.

3 Open a Command Prompt console, then change directory to go to the C:\Program Files\Dynamic File Services folder (or the folder where you installed Dynamic File Services). Select *Start > All Programs > Accessories*, then click *Command Prompt*.

4 At the command prompt, enter:

```
DswSyncPair.exe -pair="<pairname | guid>" -folders [-xml="reportname"]
[-csv="reportname"]
```

For example, to identify mismatches for the attributes and ACLs for the folders in a pair named MyPair and to create an output report named myXmlReport in XML format, enter the following command:

```
DswSyncPair.exe -pair="MyPair" -folders -xml="myXmlReport"
```

This command looks in the pair database for the source and target paths of the pair named MyPair. It checks for folders that have mismatched attributes and ACLs on the source and target paths. It produces a report in XML format in the myXmlReport.folders.xml file.

5 When you are prompted, enter the username of a user with rights to all of the paths in the pair.

8.12 Reporting Conflicts for Duplicate Files

You should always use the merged view when creating, modifying, or deleting files in a pair. Dynamic File Services manages a file so that a single instance of it exists on either the primary or secondary location.

For information about how duplicate files can occur and how Dynamic File Services handles them, see Section 4.17, "Duplicate Files," on page 48.

- Section 8.12.1, "Viewing Errors in the Policy Execution History," on page 121
- Section 8.12.2, "Generating a Duplicate Files Report," on page 121

8.12.1 Viewing Errors in the Policy Execution History

If a policy run is interrupted because one or both of the media become unavailable during the policy run, you can check the policy run history to find out which file move might not have been completed. An `Invalid File Handle` error is reported in the policy move log in the *Statistics > Policy execution history > Files not moved > Comment* field for the file. The valid file is the instance on the source location of the move.

8.12.2 Generating a Duplicate Files Report

To identify duplicate file conflicts, you can also run the Dynamic File Services Synchronize Pair tool (`DswSyncPair.exe`) with the `-files` option to detect duplicate instances of a file that exist on the primary and secondary paths, and report them. You must log in as a user with rights to all of the paths in the pair. For information, see "Dynamic File Services Synchronize Pair Utility" in the *Dynamic File Services 1.6 Client Commands and Utilities Reference*.

To generate a duplicate files report:

1 Log in to the Dynamic File Services server as a user with file system rights on the primary and secondary paths in the pair you want to manage.

  If remote shares are being used, make sure that you have sufficient access rights on the secondary locations.

2 Open the Management Console, select the pair, then verify that the pair status is in the Idle state.

  Policies must not be running against the pair when you start the Synchronize Pair utility. If policies are running, wait until they are done, or stop them manually. Wait until the pair status is idle before continuing.

3 Open a Command Prompt console, then change directory to go to the `C:\Program Files\Dynamic File Services` folder (or the folder where you installed Dynamic File Services). Select *Start > All Programs > Accessories*, then click *Command Prompt*.

4 At the command prompt, enter:

  `DswSyncPair.exe -pair="<pairname | guid>" -files [-xml="reportname"] [-csv="reportname"]`

  For example, to identify duplicate files in a pair named `MyPair` and to create an output report named `myXmlReport` in XML format, enter the following command:

  `DswSyncPair.exe -pair="MyPair" -files -xml="myXmlReport"`

This command looks in the pair database for the source and target paths of the pair named `MyPair`. It checks for files that have same path and filename in the source and target paths. It produces a report in XML format in the `myXmlReport.files.xml` file.

5 When you are prompted, enter the username of a user with rights to all of the paths in the pair.

8.13 Unlinking the Paths in a Pair

Unlinking a Dynamic File Services pair removes the pair relationship between the primary path and the secondary path. When the two locations are unlinked, the files in the two locations remain where they are on the primary path or secondary path. Removing the link automatically disassociates the policies from the pair; it does not delete the policies.

You might want to unlink a pair for any of the following reasons:

- You no longer need the pair.
- You want to modify one of the paths used in the pair.

  You cannot modify the paths that define the pair. Instead, you unlink the current pair, and create a new pair that uses the desired paths.

To unlink the paths in a pair:

1 In the Management Console, connect to the DynamicFS server that you want to manage.
2 Create one or more policies to move data between the primary and secondary locations so that the data is where you want it to be when you remove the link between the two locations.
3 Run the policies, then verify that the files have moved by viewing the *Statistics > Policy Execution History > Run History*, or by using the Windows Explorer to browse the file paths.
4 Select *Pairs*, right-click the pair, then select *Unlink*.

8.14 What's Next

- Configure policies to run on the pair. For information, see Chapter 9, "Creating and Managing Policies," on page 123.
- Monitor the health and history of the pairs, the policies, and the server disks that are used in pairs. For information, see Chapter 10, "Monitoring Pairs and Policies," on page 157.

Creating and Managing Policies

9

Novell Dynamic File Services (DynamicFS) policies control which data is moved, what direction the data moves, and when the policy is enforced. No data is moved between the primary and secondary location for a pair unless you assign a policy to it The policy can be scheduled or run on demand. You can assign multiple policies to a pair. A policy can be assigned to multiple pairs.

9.1 Understanding Policies

Policies define what data to move, the direction to move the data, and when to move it. The rules defined in the policy are enforced when the policy is run. You can configure the following parameters in a policy:

9.1.1 Policy Direction

The *Policy Direction* option determines whether the policy is enforced against files on the primary path or the secondary path. The policy run scans the original location for files that meet the filter criteria, then moves those files to the destination location. If all of the specified filter options in the policy are true for a file, the file is moved in the specified direction.

For example, if you are moving data from primary to secondary, the policy is enforced against the files on the primary path. If all of the selected filter options are true for a file, the file is moved from the primary path to the secondary path.

Table 9-1   *Policy Direction Options*

Option	Description
Primary to Secondary	The policy is enforced against the files in the primary location. Files that match the policy rules are moved from the primary path to the secondary path. This is the default.
Secondary to Primary	The policy is enforced against the files in the secondary location. Files that match the policy rules are moved from the secondary path to the primary path.

9.1.2 Policy Filter Options

The *Policy Filter* options identify which files are to be moved by the policy. Dynamic File Services moves files between the primary path and the secondary path when the policies that are associated with the pair are enforced. When a file is moved, it remains in the destination location until a policy moves it in the other direction.

By creating different policies for a pair, you can move files that meet different conditions. If you configure multiple policies for a pair to run at the same time, the Standard Policy engine does the following:

1. Groups the policies according to the direction that the data is being moved: From primary to secondary or from secondary to primary.
2. Scans the primary path, and enforces policies that move files to the secondary path.
3. Scans the secondary path, and enforces policies that move files to the primary path.

When a policy is enforced, a file is moved only if it satisfies all of the filter options set for that policy. (That is, the filters in a given policy are enforced as AND operations.)

When multiple policies are enforced in a single run, a file is moved if it satisfies the rules in any one of the policies in that group. (That is, multiple concurrently scheduled policies are enforced as OR operations.)

You must enable and configure at least one of the following filter options in each policy. If you specify other filter options and do not enable *File patterns* or *File types*, the specified filters to apply to all files.

For examples of how to create policy rules to achieve your storage goals, see Section 9.14, "Examples of Policy Rules," on page 146.

- ◆ "File Size" on page 125
- ◆ "Last Accessed" on page 125
- ◆ "Last Modified" on page 125
- ◆ "File Patterns" on page 125
- ◆ "File Types" on page 126
- ◆ "File Owners" on page 127

File Size

Select the check box to enable the option, then create a rule that moves a file only if its size is greater than or less than the specified file size.

Last Accessed

Select the check box to enable the option, then create a rule that moves a file only if the elapsed time since it was last accessed is greater than or less than the specified time period.

Last Modified

Select the check box to enable the option, then create a rule that moves a file only if the elapsed time since it was last modified is greater than or less than the specified time period.

File Patterns

File patterns are used to evaluate the filename and extension of files in the pair.

IMPORTANT: The File Types option and the File Patterns option cannot be used together.

Select the check box to enable the option, then create a rule that moves a file only if the file has one of the specified file patterns. If you specify other filter options, only files that satisfy the pattern and that also meet the other criteria are moved.

Regular expressions that you use in the *File patterns* field work like expressions you might use in the dir function on the Windows command line. The asterisk (*) is a wildcard character can be used to represent a sequence of any number of characters in the name. The question mark (?) character can be used to represent a single character.

The pattern search is case insensitive.

Separate multiple file patterns with a comma and no spaces. If you include spaces in a pattern, the spaces are interpreted as part of the pattern you seek.

Examples

These two search patterns find the same files:

```
*aBa_*
*ABA_*
```

In the following patterns, spaces within a pattern are considered part of the filename. The spaces after a comma are part of the next pattern.

```
test many files*, many*, 12??*,dsw*.?2*
```

In the following patterns, the asterisk is used for the filename to indicate that files with a specified extension should be moved:

```
*.mp3,*.png,*.jpg
```

To move all files with and without extensions, specify All files (*.*) in the *File patterns* field.

To move files with no extension, specify "*." in the *File patterns* field.

Table 9-2 shows examples of regular expressions that are used as file patterns and the files found:

Table 9-2   *Sample File Patterns*

File Pattern	File Found
`*jpg*`	`testjpg.txt`
`test.?`	`test.1`
`proc*test.jpg`	`procisatest.jpg`
`*_?.text`	`p_1.text`
`*ap*.???`	`apache.aaa`

File Types

File types are the content types of files based on the standard MIME (Multipurpose Internet Mail Extensions) types that are registered by applications when they are installed on the server. The content types in use on the server and the file extensions that have been associated with those content types can vary, depending on what applications are installed on a server.

IMPORTANT: The File Types option and the File Patterns option cannot be used together.

On the Policy Filter page, select the check box to enable the option, then create a rule that moves a file only if the content type of the file matches one of the specified file types. Select one or more file types from the *File types* drop-down menu. Hold down the Control key to select multiple options. Hold down the Shift key to select multiple contiguous options.

Dynamic File Services determines the content types that are in use on a server by scanning the file type settings in the Windows Registry. The content types in use are based on the standard MIME type definitions. DynamicFS also considers perceived file types if an installed application sets the `Perceived-Type` parameter. Perceived types refer to broad categories of file format types, rather than to specific types of files. Perceived types include images, text files, audio files, and compressed files.

If users are running different applications on their workstations than those installed on the server, it is possible that stored files can have file extensions that have not been mapped to content types in the server's Windows Registry. In this case, the File Types filter does not move files with that file extension during a policy run.

IMPORTANT: Make sure you understand what content types are in use on the server and what file extensions are associated to those content types in the server's Windows Registry.

An application maps file extensions to content types by adding an entry in the server's Windows Registry under the `HKEY_CLASSES_ROOT\<file_extension>` key. For example:

```
HKEY_CLASSES_ROOT\.gif
  Content Type = "image/gif"
```

Content types are also listed in the Windows Registry under `HKEY_CLASSES_ROOT\MIME\Content Type\<type>\<subtype>` key.

Common file types and a list of the file extensions that are typically associated with them are provided in Table 9-3. The list is not intended to be exhaustive. The application must be installed on the server to be a valid example for your system.

Table 9-3 *Common Content Types and Their Associated File Extensions*

Standard Content Type	Sample of the Associated File Extensions		
application	`.accdb`	`.docx`	`.pps`
	`.ai`	`.gz`	`.ppt`
	`.ani`	`.odp`	`.pptx`
	`.csv`	`.odt`	`.xls`
	`.doc`	`.pdf`	`.zip`
audio	`.aiff`	`.mmv`	`.wav`
	`.mid`	`.mp3`	
compressed (perceived type)	`.arc`	`.cab`	`.zip`
image	`.bmp`	`.jpeg`	`.png`
	`.gif`	`.jpg`	`.tiff`
message	HTTP, HTTPS, SIP		
model	`.iges`	`.mesh`	`.vrml`
system	`.386`	`.chk`	
text	`.css`	`.rtf`	`.txt`
	`.htm`	`.sgm`	`.xml`
	`.html`	`.sgml`	`.xms`
video	`.avi`	`.mpeg`	
	`.mp3`	`.wmv`	

File Owners

You can browse or type one or more valid usernames in order to move files based on file ownership. For usernames, files are moved if they are owned by any of the specified users. Invalid usernames are ignored when the policy runs.

9.1.3 Policy Schedule

The policy *Schedule* setting determines if the policy is scheduled or unscheduled. If the schedule is enabled, the schedule options specify when and how often the policy runs. The schedule applies for all pairs that are associated with the policy. Unscheduled policies are not enforced unless you run them manually by using *Execute now*. Scheduled and unscheduled policies can be run at any time by using *Execute now*.

You can schedule policies for a pair to run at different times or at the same time. If policies are not run together, make sure that you allow sufficient time for a policy run to complete before the start time of another policy.

IMPORTANT: For information about planning policy schedules, see Section 4.19, "Policy Schedules," on page 50.

- ◆ "Scheduled or Unscheduled" on page 128
- ◆ "Schedule Options" on page 128

Scheduled or Unscheduled

You can associate scheduled and unscheduled policies with one or more pairs.

Select the *Scheduled* check box to enable the schedule. You must select one scheduling option, then specify when to run it. For information, see "Schedule Options" on page 128.

Deselect the Scheduled check box to disable the schedule. Unscheduled policies are not enforced unless you run them manually.

Schedule Options

If scheduling is enabled, you must specify one of the schedule options. A policy can be enforced hourly, daily, weekly, monthly, or yearly. Select one scheduling option, then specify when to run it. The default is weekly on Sunday at 12:00 a.m.

Table 9-4   *Policy Schedule Options*

Option	Description
Hourly	Select the *Hourly* check box to run the policy every hour at hh:00:00.
Daily	Select the *Daily* check box, then specify the time of day to start the policy and how long you want it to run.
	Start determines at what time on that day the run should begin. Start times are available in 15-minute increments (hh:00, hh:15, hh:30, hh:45). The default is 12:00 a.m.
	Duration specifies how long to run the policy in one-hour increments, or until complete. The default is *Until complete*.
Weekly (default)	Select the *Weekly* check box, then specify the day of the week, the start time, and duration to run the policy.
	Day determines which day of the week to enforce the policy. The default is *Sunday*.
	Start determines at what time on that day the run should begin. Start times are available in 15-minute increments (hh:00, hh:15, hh:30, hh:45). The default is 12:00 a.m.
	Duration specifies how long to run the policy in one-hour increments, or until complete. The default is *Until complete*.

Option	Description
Monthly	Select the *Monthly* check box, then specify the calendar day of the month, the start time, and duration to run the policy.
	Day determines which calendar day of the month to enforce the policy. Options are 1 to 31. The default is day 15.
	Start determines at what time on that day the run should begin. Start times are available in 15-minute increments (hh:00, hh:15, hh:30, hh:45). The default is 12:00 a.m.
	Duration specifies how long to run the policy in one-hour increments, or until complete. The default is *Until complete*.
Yearly	Select the *Yearly* check box, then specify the month, the calendar day of the month, the start time, and duration to run the policy. The month and day are required to be set.
	Month determines in which calendar month to enforce the policy. Options are the 12 months of the Gregorian calendar year. You must specify the month; no default is defined.
	Day determines which calendar day of the month to enforce the policy. Options are 1 to 31. You must specify the day; no default is defined.
	Start determines at what time on that day the run should begin. Start times are available in 15-minute increments (hh:00, hh:15, hh:30, hh:45). The default is 12:00 a.m.
	Duration specifies how long to run the policy in one-hour increments, or until complete. The default is *Until complete*.

9.1.4 Policy Name and Description

Each policy name must be unique to the DynamicFS server. If you plan to export a policy for use across multiple DynamicFS servers, the name should be unique across all of the servers.

Table 9-5   *Policy Name and Description Options*

Option	Description
Policy Name	Policy names can be up to 32 characters.
	For information about naming restrictions, see Section 4.13, "Naming Conventions for Pairs and Policies," on page 47.
Description	If desired, you can add a more detailed human-interpretable description of the policy. The description is displayed next to the policy name in the *Policy* list.

9.1.5 Pair to Policy Associations

Select one or more pairs from the list of pairs. No data is moved between the primary and secondary locations in a pair until you associate it with at least one policy and the policy. The policy can be scheduled or run on demand. A single pair can be associated with multiple policies. A single policy can be associated with multiple pairs.

IMPORTANT: The policy must be associated with at least one pair before it can be run. A policy is enforced only for its associated pairs.

You can configure the Include Folders setting for a pair to specify folders in the pair where its assigned policy apply. You can configure the Exclude Folders setting for a pair to specify folders in the pair where its assigned policy do not apply. For information, see Section 8.5, "Including or Excluding Folders from a Pair's Policy Runs," on page 114.

9.2 Creating a Policy

Two wizards are available for configuring policies:

- ◆ **Setup Wizard:** Sets up a new pair, a new policy for the pair, and automatically associates the pair and policy.

  The pair is not created until the policy is configured and you click *Finished*. The associated policy is enforced for the pair at its next scheduled run, or you can start a policy manually by using *Execute now*.

  The Setup Wizard opens automatically when you connect to a DynamicFS server if no pairs are currently defined for the server. The Setup Wizard is also convenient to use when you want to create a new pair and a policy for it at the same time. You can associate additional policies later.

- ◆ **Policy Wizard:** Sets up a new policy and allows you to select none, one, or multiple existing pairs to associate with the policy.

  The policy is enforced for the associated pairs at the policy's next scheduled run, or you can the start policy for a pair manually by using *Execute now*. You can associate additional pairs later.

IMPORTANT: The policy must be associated with at least one pair before it can be run. A policy is enforced only for its associated pairs.

For information on the different fields in the policy, see Section 9.1, "Understanding Policies," on page 123.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Open one of the following wizards:

- ◆ **Setup Wizard:** Use any of the following methods to open the Setup Wizard.

  - ◆ Select the server, then select *Actions > Setup Wizard*.
  - ◆ Right-click the server, then select *Setup Wizard*.
  - ◆ If no pairs or policies exist on the server when you connect to it, the Setup Wizard opens automatically.

  Create the pair, then click *Next*.

  For information about creating a pair, see Section 8.2, "Creating a Pair," on page 109.

* **Policy Wizard:** Use either of the following methods to access the Policy Wizard.
  * Select *Policies*, then select *Actions > Policy Wizard*.
  * Right-click *Policies*, then select *Policy Wizard*.

3 On the Policy Rules page, specify the direction and filter options to apply for this policy:
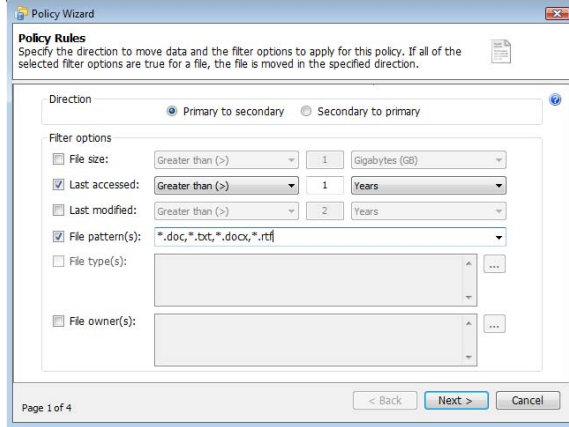
3a In the Direction area, specify *Primary to Secondary* (the default) or *Secondary to Primary*.

3b In the *Filter options* area, specify the search criteria to use to identify the files to be moved when the policy is enforced.

You must enable and configure at least one of the filter options:

Option	Description
File size	Select the check box, then create a rule that moves a file only if its size is greater than or less than the specified file size.
Last accessed	Select the check box, then create a rule that moves a file only if the elapsed time since it was last accessed is greater than or less than the specified time period.
Last modified	Select the check box, then create a rule that moves a file only if the elapsed time since it was last modified is greater than or less than the specified time period.
File patterns	Select the check box, then create a rule that moves a file only if its filename uses one of the specified file patterns. Separate multiple file patterns with a comma and no spaces. If you include spaces in a pattern, the spaces are interpreted as part of the pattern you seek.
File types	Select the check box to enable the option, then create a rule that moves a file only if the internal format of the file matches one of the specified file types. Select one or more file types from the *File types* drop-down menu by clicking the type once. To deselect a file type, click it again.
File owners	Specify one or more usernames of file owners. Only files owned by the specified users are moved. Usernames that are invalid at run time are ignored.

3c Click *Next* to continue.

4 On the Policy Schedule page, specify the schedule options:
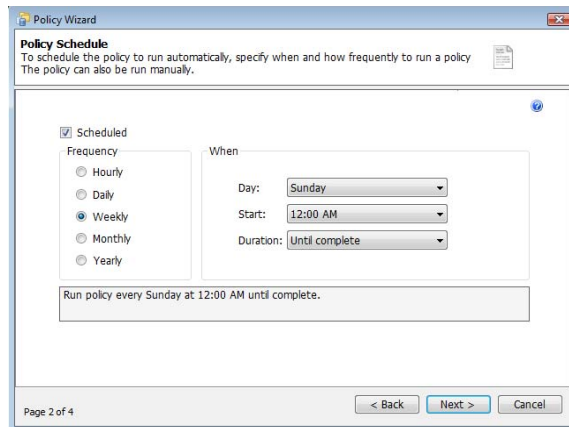
- **Not Scheduled:** Deselect *Scheduled* to disable scheduling, then click *Next* to continue.

  Unscheduled policies are not enforced unless you run them manually by using *Execute now*.

- **Scheduled:** Select *Scheduled* to enable scheduling, set the schedule for the policy, then click *Next* to continue.

  Scheduled policies can also be run at other times by using *Execute now*.

  A policy can be enforced hourly, daily, weekly, or monthly. Select one scheduling option, then specify when to run it.

Option	Description
Hourly	Select the *Hourly* check box to run the policy every hour at hh:00:00.
Daily	Select the *Daily* check box, then specify the time of day to start the policy and how long you want it to run.
Weekly (default)	Select the *Weekly* check box, then specify the day of the week, the start time, and duration to run the policy.
Monthly	Select the *Monthly* check box, then specify the calendar day of the month, the start time, and duration to run the policy.
Yearly	Select the *Yearly* check box, then specify the month, the calendar day of the month, the start time, and duration to run the policy. The month and day must be set.

5 On the Policy Name and Description page, specify a unique name for the policy on the selected DynamicFS server, optionally add a more detailed description for the policy, then click *Next* to continue.
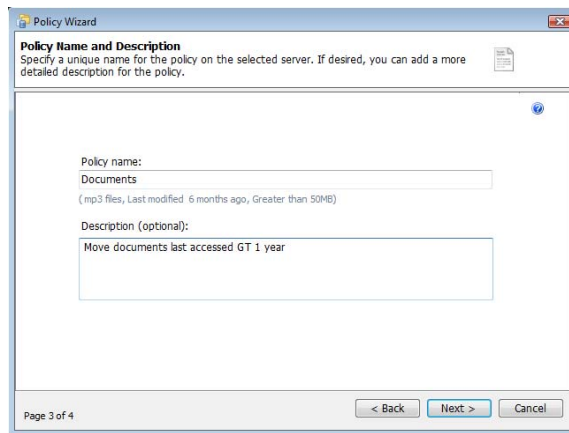
6 On the Pair to Policy Association page, select one or more pairs that you want to associate with this policy.
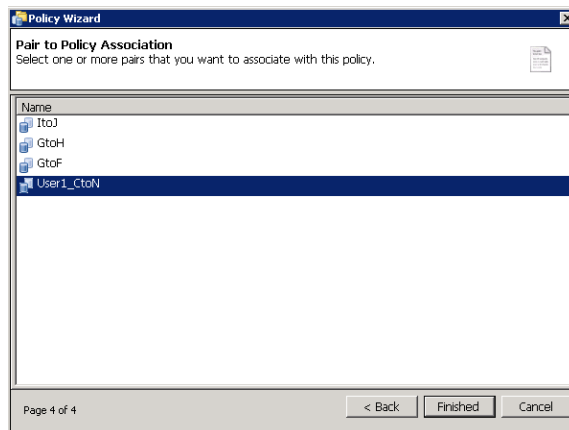
The policy must be associated with at least one pair to be able to run. The policy is enforced only for its associated pairs. If no pairs exist, you can use the Pair Wizard later to create a pair and associate it to the policy. For information about managing pair and policy associations, see Section 9.5, "Associating or Disassociating Pairs and Policies," on page 135.

7 Click *Finished* to create the policy, or click *Cancel* to abandon the setup.

If a pair has been associated with the policy, a scheduled policy is enforced at its next scheduled run time, or you can run it at any time by using *Execute now*.

8 (Optional) Associate the policy with other pairs.

For information, see Section 9.5, "Associating or Disassociating Pairs and Policies," on page 135.

9.3 Viewing a List of Policies

You can view a list of all of the policies that are defined for a server by using the Dynamic File Services Management Console.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 In the left panel, select the *Policies* folder ( ) for the server, then view the list of policies ( ) that are defined.
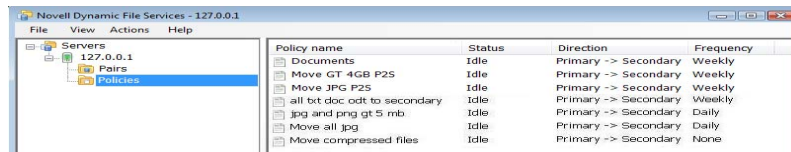
The *Policies* list reports the following information for each policy:

- ◆ *Policy name*
- ◆ *Status* (*Idle*, *Running*)
- ◆ *Direction* (*Primary to Secondary*, *Secondary to Primary*)
- ◆ *Frequency* (*None* (not scheduled), *Hourly*, *Daily*, *Weekly*, *Monthly*, *Yearly*)

3 (Optional) Click a column heading to sort the list by that parameter.

9.4 Viewing Properties for a Policy

You can view the settings for an existing policy in its Policy Properties dialog box.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 In the left panel, select the *Policies* folder ( ) for the server, then view the list of policies that are defined.

3 Right-click a policy, then select *Properties*.

4 View the information on the *General* tab.
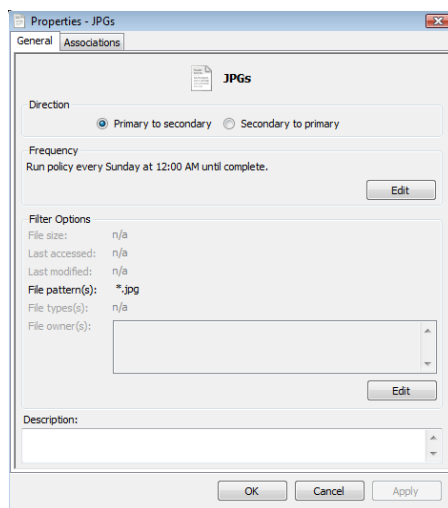
The *General* tab in the Policy Properties dialog box reports the following information:

- *Policy name*
- *Direction*
- *Frequency*
- *Filter options*

  Unused filter options are dimmed and marked as `n/a`.

- *Description*

For information about the fields, see Section 9.1, "Understanding Policies," on page 123.

5 View the information on the *Associations* tab.
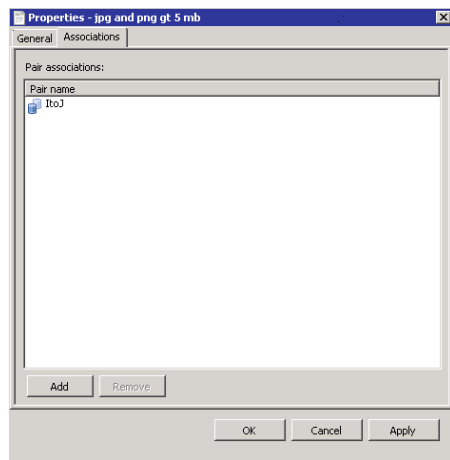
The *Associations* tab lists the pairs that are currently associated with the policy. You can also add and remove pairs from the list.

9.5 Associating or Disassociating Pairs and Policies

Dynamic File Services pairs and policies must be associated before any data can be moved between the primary and secondary paths. A single pair can be associated with multiple policies. A single policy can be associated with multiple pairs.

- Section 9.5.1, "Viewing a List of Pairs Associated with a Policy," on page 135
- Section 9.5.2, "Viewing a List of Policies Associated with a Pair," on page 136
- Section 9.5.3, "Associating or Disassociating Pairs with a Selected Policy," on page 136
- Section 9.5.4, "Associating or Disassociating Policies with a Selected Pair," on page 137

9.5.1 Viewing a List of Pairs Associated with a Policy

You can view a list of the pairs associated with a policy in the Policy Properties dialog box.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Click the *Policies* folder under the server to view the list of policies for the server in the right panel.

3 Right-click a policy, then select *Properties*.

4 Click the *Associations* tab to view a list of the pairs that are currently associated with the policy.

9.5.2 Viewing a List of Policies Associated with a Pair

You can view a list of the policies associated with a pair in the pair's Properties dialog box or Statistics dialog box.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Click the *Pairs* folder under the server to view the list of pairs for the server in the right panel.

3 Use either of the following methods to see a list of policies associated with a pair:

- ◆ Right-click a pair, select *Properties*, then select the *Associations* tab to view a list of the policies that are currently associated with the pair.

- ◆ Right-click a pair, select *Statistics*, then view a list of the policies that are currently associated with the pair in the *Policies associated to pair* area.

  This view has the added benefit of showing the current state of the policy and information about the last time the policy was run.

9.5.3 Associating or Disassociating Pairs with a Selected Policy

You can associate or disassociate pairs with a selected policy by using the policy's Properties dialog box. When you disassociate a pair from a policy, the policy must not be running on the pair.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Click the *Policies* folder under the server to view the list of policies for the server in the right panel.

3 Right-click a policy and select *Properties* to open its Policy Properties dialog box, then select the *Associations* tab.

4 (Optional) Associate one or more pairs to the selected policy:

4a On the *Associations* tab, click *Add* to open the Select Pairs dialog box.

The Select Pairs dialog box displays a list of all pairs that are defined on the server that are not already associated with the selected policy.

4b Select one or more pairs that you want to add to the *Associations* list, then click *OK*.

5 (Optional) Disassociate one or more pairs from the selected policy:

5a Make sure that the selected policy is not currently running on any of the pairs you want to disassociate from it.

The policy should both report an *Idle* state in the Management Console window. You can wait until the policy run ends, or you can manually stop the running process.

5b Select one or more pairs that you want to remove from the *Associations* list for the selected policy, then click *Remove*.

6 Click *Apply* or *OK* to save and apply your changes.

The policy is enforced for its associated pairs at the policy's next scheduled run time. Scheduled and unscheduled policies that are associated with a pair can be run manually by using the *Execute now* option.

9.5.4 Associating or Disassociating Policies with a Selected Pair

You can associate or disassociate policies with a pair by using the pair's Properties dialog box or Statistics dialog box. When you disassociate a policy from a pair, the policy must not be running on the pair.

- ◆ "Using the Pair Properties dialog box to Add or Remove Policy Associations" on page 137
- ◆ "Using the Pair Statistics Dialog Box to Add or Remove Policy Associations" on page 137

Using the Pair Properties dialog box to Add or Remove Policy Associations

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Click the *Pairs* folder under the server to view the list of pairs for the server in the right panel.

3 Right-click a pair and select *Properties* to open its Pair Properties dialog box, then select the *Associations* tab.

4 (Optional) Associate one or more policies to the selected pair:

4a On the *Associations* tab, click *Add* to open the Select Policies dialog box.

The Select Policies dialog box displays a list of all policies that are defined on the server that are not already associated with the selected pair.

4b Select one or more policies that you want to add to the *Associations* list, then click *OK*.

5 (Optional) Disassociate one or more policies from the selected pair:

5a Make sure that the policies that you want to disassociate from the pair are not currently running on the pair.

The policy should both report an *Idle* state in the Management Console window. You can wait until the policy run ends, or you can manually stop the running process.

5b Select one or more policies that you want to remove from the *Associations* list for the selected pair, then click *Remove*.

6 Click *Apply* or *OK* to save and apply your changes.

The policies associated with the pair are enforced at each policy's next scheduled run time. Scheduled and unscheduled policies that are associated with a pair can be run manually by using the *Execute now* option.

Using the Pair Statistics Dialog Box to Add or Remove Policy Associations

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Click the *Pairs* folder under the server to view the list of pairs for the server in the right panel.

3 Double-click the pair to open its Statistics dialog box.

4 (Optional) Add a new policy association:

4a Use either of the following methods to open the Select Policies dialog box:

- ◆ From the Statistics dialog box toolbar, select *Actions > Add policy association*.
- ◆ Right-click in the *Policies associated to pair* area, select *Add policy association* from the pop-up menu.

The Select Policies dialog box displays a list of all policies that are defined on the server that are not already associated with the selected pair.

4b In the Select Policies dialog box, select one or more policies to associate with the pair, then click *OK*.

The policies are enforced for the selected pair at the each policy's next scheduled run time. Scheduled and unscheduled policies that are associated with a pair can be run manually by using the *Execute now* option.

5 (Optional) Remove a policy association:

5a Make sure the policy is not currently running on the pair.

You can wait until the policy run ends, or you can manually stop the running process.

5b In the *Policies associated to pair* area, select one or more idle policies that you want to disassociate from the pair.

5c Use either of the following methods to remove the association between the selected policies and the selected pair:

- From the Statistics dialog box toolbar, select *Actions > Remove policy association*
- Right-click and select *Remove policy association*.

6 When you are done, close the Statistics dialog box.

9.6 Modifying Policy Rules

Policy rules govern what files are moved and when. You configure the policy rules when you create the policy. You can modify the policy rules later.

For information the different fields in the policy, see Section 9.1, "Understanding Policies," on page 123.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

**2** Select the *Policies* folder for the server, then view the list of policies that are defined.

3 Right-click the policy that you want modify, then select *Properties*.
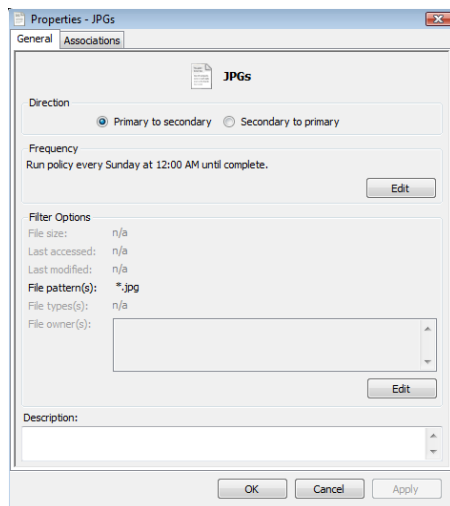
4 On the *General* tab under *Direction*, specify the direction to move data, then click *Apply* to save the change.

Specify *Primary to Secondary* (the default) or *Secondary to Primary*. The direction determines whether the policy is enforced against files on the primary location or the secondary location.

5 On the *General* tab under *Filter options*, click *Edit* to open the *Modify filter* dialog box.

6 Specify one or more filter options to apply for this policy.

For information, see Section 9.1.2, "Policy Filter Options," on page 124.

Option	Description
File size	Select the check box, then create a rule that moves a file only if its size is greater than or less than the specified file size.
Last accessed	Select the check box, then create a rule that moves a file only if the elapsed time since it was last accessed is greater than or less than the specified time period.
Last modified	Select the check box, then create a rule that moves a file only if the elapsed time since it was last modified is greater than or less than the specified time period.
File patterns	Select the check box, then create a rule that moves a file only if its filename uses one of the specified file patterns. Separate multiple file patterns with a comma and no spaces. If you include spaces in a pattern, the spaces are interpreted as part of the pattern you seek.
File types	Select the check box to enable the option, then create a rule that moves a file only if the internal format of the file matches one of the specified file types. Select one or more file types from the *File types* drop-down menu by clicking the type once. To deselect a file type, click it again.
File owners	Specify one or more usernames of file owners. Only files owned by the specified users are moved.

7 Click *OK* to save your changes and close the *Modify filter* dialog box, then click *OK* to save your changes.

The policy rule changes apply when the policy runs at its next scheduled interval. For information, see Section 9.7.1, "Understanding How Changes Affect the Scheduled Run Interval," on page 140.

9.7 Modifying Policy Schedules

You can use the Dynamic File Services Management Console to modify the frequency that a policy runs. Schedule changes do not affect any currently running instances of the policy. If a schedule is enabled, the policy runs at its next scheduled interval for each pair. You can also use *Execute Now* to run the edited policy as needed for its associated pairs.

- Section 9.7.1, "Understanding How Changes Affect the Scheduled Run Interval," on page 140
- Section 9.7.2, "Rescheduling the Policy," on page 141
- Section 9.7.3, "Unscheduling a Policy for All Pairs," on page 142
- Section 9.7.4, "Disabling the Schedule for Selected Pairs," on page 142

9.7.1 Understanding How Changes Affect the Scheduled Run Interval

The next scheduled run interval depends on the current run state for the policy and the frequency setting.

For example, a policy runs daily at 10:00 a.m. At 10:15 a.m., you modify the policy to run daily at 11:00 a.m. The policy has already run for that day, so its next scheduled run occurs the following day at 11:00 a.m.

For example, a policy runs monthly on day 15 at 2:00 a.m. At 8:00 a.m. you modify the policy to run monthly on day 30. The policy has already run for that month, so its next scheduled run occurs the following month at 2:00 a.m on day 30. If you need to run the policy a second time in the current month, you can manually run the policy on day 30 of the current month by using *Execute Now*.

Table 9-6 describes the behavior of DynamicFS when determining the next scheduled interval for the policy.

Table 9-6 *Determining the Next Scheduled Run Interval*

Run State	Next Scheduled Run Interval
The run is in progress.	The current run finishes. The next scheduled run is:
	Hourly: The next hour.
	Daily: Tomorrow at the new time.
	Weekly: The new time and day of the week in the following week.
	Monthly: The new time and day of the month in the following month.
	Yearly: The new time and day of the year in the following year.
The run is completed for the current hour or day.	The next scheduled run is:
	Hourly: The next hour.
	Daily: Tomorrow at the new time.
	Weekly: The new time and day of the week in the following week.
	Monthly: The new time and day of the month in the following month.
	Yearly: The new time and day of the year in the following year.

Run State	Next Scheduled Run Interval
The run has not started, and it is within 20 minutes after the scheduled start time.	The next scheduled run is: **Hourly:** The current hour if possible. If the pair is busy, the run is scheduled for the next hour. **Daily:** As scheduled if possible. If the pair is busy, the run is scheduled for tomorrow at the new time. **Weekly:** As scheduled if possible. If the pair is busy, the next run is scheduled for the new time and day of the week in the following week. **Monthly:** As scheduled if possible. If the pair is busy, the next run is scheduled for the new time and day of the month in the following month. **Yearly:** As scheduled if possible. If the pair is busy, the next run is scheduled for the new time and day of the year in the following year.
The run has not started, and it is more than 20 minutes after the scheduled start time.	The next scheduled run is: **Hourly:** The next hour. **Daily:** Tomorrow at the new time. **Weekly:** The new time and day of the week in the following week. **Monthly:** The new time and day of the month in the following month. **Yearly:** The new time and day of the year in the following year.

9.7.2 Rescheduling the Policy

Modifying the schedule applies the changes for all pairs associated with the policy. The modified policy runs at its next scheduled time. Unscheduled policies are not enforced unless you run them manually. You can associate scheduled and unscheduled policies with one or more pairs.

For information the different fields in the policy, see Section 9.1.3, "Policy Schedule," on page 127.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Right-click the policy you want modify, then select *Properties*.

3 On the *General* tab under *Frequency*, click *Edit* to open the *Modify frequency* dialog box.

4 If the schedule is disabled, select the *Scheduled* check box.

5 Specify the new frequency.

A policy can be enforced hourly, daily, weekly, or monthly. Select one, then specify when to run it.

Option	Description
Hourly	Select the *Hourly* check box to run the policy every hour at hh:00:00.
Daily	Select the *Daily* check box, then specify the time of day to start the policy and how long you want it to run.
Weekly (default)	Select the *Weekly* check box, then specify the day of the week, the start time, and duration to run the policy.

Option	Description
Monthly	Select the *Monthly* check box, then specify the calendar day of the month, the start time, and duration to run the policy.
Yearly	Select the *Yearly* check box, then specify the month, the calendar day of the month, the start time, and duration to run the policy. The month and day are required to be set.

6 Click *OK* to save your changes and close the *Modify frequency* dialog box, then click *OK* to save your changes.

The policy runs at its next scheduled interval. For information, see Section 9.7.1, "Understanding How Changes Affect the Scheduled Run Interval," on page 140.

9.7.3 Unscheduling a Policy for All Pairs

To disable a policy's schedule for all of its associated pairs:

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Right-click the policy you want modify, then select *Properties*.

3 On the *General* tab under *Frequency*, click *Edit* to open the *Modify frequency* dialog box.

4 Deselect the *Scheduled* check box to disable the policy from running automatically.

5 Click *OK* to save your changes.

The policy does not run automatically. You can use *Execute Now* option to run the policy as needed. For information, see Section 9.8, "Starting a Policy Run," on page 142.

9.7.4 Disabling the Schedule for Selected Pairs

To disable the policy's schedule from running on some pairs, you can disassociate the pair from the policy, then re-associate the pair and policy when you are ready for the policy to run on the pair again. For information, see Section 9.5.3, "Associating or Disassociating Pairs with a Selected Policy," on page 136.

9.8 Starting a Policy Run

Policies can be enforced automatically based on the schedule that is configured for the policy, or they can be run on demand.

- Section 9.8.1, "Scheduling a Policy Run," on page 142
- Section 9.8.2, "Running a Policy on Demand for a Selected Pair," on page 143

9.8.1 Scheduling a Policy Run

For information about scheduling a policy to run, see Section 9.7, "Modifying Policy Schedules," on page 139.

9.8.2 Running a Policy on Demand for a Selected Pair

To manually start a policy run for a selected pair:

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Click the *Pairs* folder under the server to view the list of pairs for the server in the right panel.

3 Make sure the pair is in the *Idle* state.

If other policies are running, you can wait until the policy run ends, or you can manually stop the policy run.

4 Double-click the pair name to open the Statistics dialog box.

5 Select one or more policies, then right-click and select *Execute now*.

To select multiple policies, hold down the Shift key or Control key while selecting policies. The policy run applies only for the selected pair.

6 Monitor the policy run by viewing the progress in the *Scan Progress* bar.

7 After the run is complete, you can view statistical information about the run by clicking the *Policy Execution History* tab and pressing F5 to refresh the screen.

You can also close the Statistics dialog box and re-open it to get the updated view of the policy run.

9.9 Previewing a Policy Run

The *Preview now* option allows you to test a policy run against a Dynamic File Services pair without moving any files. It scans the files to determine which files would be moved if the policy were to be enforced. It reports statistics about the move, such as how many megabytes would be moved and a list of files that would be moved.

◆ Section 9.9.1, "Starting a Policy Preview," on page 143
◆ Section 9.9.2, "Viewing the Preview Results," on page 144

9.9.1 Starting a Policy Preview

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Click the *Pairs* folder under the server to view the list of pairs for the server in the right panel.

3 Make sure the pair is in the *Idle* state.

If other policies are running, you can wait until the policy run ends, or you can manually stop the policy run.

4 Use either of the following methods to start the preview:

◆ Double-click the pair you want to manage to open its Statistics dialog box, select one or more policies, then select *Preview now*.

◆ Under the *Pairs* folder, right-click the pair name, select *Preview now*, then select one or more policies to run for the preview. The *Status* for the policies changes to *Running*, but the pair's Statistics dialog box does not open automatically.

5 When the preview run is completed, open the Statistics dialog box, then click *View > Preview results* to open the Preview dialog box.

6 In the Preview dialog box, click the *Files to be moved* link to see a list of the files.

7 Use the left-arrow and right-arrow to page through the list of files. You can also specify a sequence of letters in the *Filter* field to find a specific file.

8 Close the Preview dialog box when you are done.

9.9.2 Viewing the Preview Results

The latest run of a policy preview for a pair can be viewed until another policy preview is started for the same pair.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Double-click the pair you want to manage to open its Statistics dialog box.

3 Select *View > Preview results* to see information about the last preview results.

4 Click the *Files to be moved* link to see a list of the files.

5 Use the left-arrow and right-arrow to page through the list of files. You can also specify a sequence of letters in the *Filter* field to find a specific file.

6 Close the Preview dialog box when you are done.

9.10 Stopping a Policy Run

You can stop a policy run that is in progress by using the *Actions > Stop running process* option from the pair's Statistics dialog box. This gracefully stops all policy runs that are currently in progress on the pair. After a policy run is stopped, the data that has already moved remains in the new location. The unmoved data remains in the old location. The next time the policy runs, the scan begins the policy enforcement process at the beginning.

To stop a policy run that is in progress:

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Select the pair you want to manage to open its Statistics dialog box.

3 Select the policy, then select *Actions > Stop running process*.

To ensure that a policy is not run again, go to the policy's Properties dialog box and unschedule it. For information, see:

9.11 Exporting and Importing Policies on a Dynamic File Services Server

Dynamic File Services allows you to export and import a policy configuration to make it easier to set up management on multiple computers. You can set up multiple policies in the Management Console on one computer, then export them to .xml files. The default name of the exported file is the same as the policy name.

You can import a policy on another computer to automatically set it up there. If you manage the two computers from the same Management Console, the file is easily exported and imported between the two computers by exporting to a local folder. You can also copy the exported .xml file to a different computer and import it there.

9.11.1 Exporting a Policy

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Under the *Policies* folder for the server, right-click the policy, then select *Export*.

You can also select the policy, then select *File > Import/Export > Export policy*.

3 Browse to the location on the local computer where you want to save the file, specify a name for the file, then click *Save*.

By default, the policy is exported as a .xml file and the filename is the same as the policy name.

4 Continue with .

9.11.2 Importing a Policy

1 Place a copy of the exported policy on the computer where you are managing DynamicFS.

For information, see .

2 In the Management Console, connect to the DynamicFS server where you want to import the policy.

3 Right-click the *Policies* folder for the server, then select *Import policy*.

You can also select the *Policies* folder, then select *File > Import/Export > Import policy*.

4 Browse to the locate and select the exported policy file, then click *Open*.

The Policy Wizard opens to the Policy Rules page.

5 On the Policy Rules page, verify or modify the *Direction* and *Filter options* settings, then click *Next*.

6 On the Policy Schedule page, verify or modify the schedule *Frequency* and *When* settings, then click *Next*.

7 On the Policy Name and Description page, specify a unique name for the policy on this server, then click *Next*.

8 On the Pair to Policy Association page, select one or more pairs on the selected server that you want to associate with the policy, then click *Finished*.

The policy is added to the *Policies* list for the selected server.

9.12 Deleting a Policy

You can delete policies when you no longer need them. A policy must be idle before it can be deleted.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Open the *Policies* folder for the server.

3 If the policy is in a *Running* state, do one of the following:

- ◆ Wait until the policy completes the run and returns to the *Idle* state.
- ◆ Stop the policy run on each of the pairs that are associated with the policy.

  For instructions, see Section 9.10, "Stopping a Policy Run," on page 144.

4 After the policy is in the *Idle* state, right-click the policy, then select *Delete*.

9.13 Troubleshooting Policy Conflicts

There is no automated check to determine if the policies associated with a pair are moving files back and forth in the same or different runs. When you plan policies for a pair, consider the file extensions and types that occur in the pair and how the filter options are enforced. Make sure that the policies assigned to a pair move files where you expect them to be moved, and that they are not counter-productive.

For example, if one policy moves files to the secondary path based on the file extension, and another policy moves files to the primary path based on the last accessed time, some files might move both ways.

You can use the following methods to understand what files are moved during a policy run:

- ◆ **Preview Now:** You can use the *Preview Now* option to view the files that would be moved in a run without actually moving any files. For information, see Section 9.9, "Previewing a Policy Run," on page 143.
- ◆ **Policy Execution History:** You can inspect the Policy Execution History for a pair to examine lists that show what files were moved in the last several runs. For information, see Section 10.2, "Viewing the Policy Execution History for a Pair," on page 158.

Use this information to refine the policies as needed to achieve your storage goals.

9.14 Examples of Policy Rules

The examples in this section can help you understand how to configure policy rules to achieve your desired outcome for moving data in a pair:

- ◆ Section 9.14.1, "Example: Move All Files Larger than 10 Megabytes," on page 147
- ◆ Section 9.14.2, "Example: Move All MP3 Files Larger than 10 Megabytes," on page 147
- ◆ Section 9.14.3, "Example: Move All MP3 Files Larger than 10 Megabytes That Were Last Accessed More than 6 Months Ago," on page 148
- ◆ Section 9.14.4, "Example: Move All Files," on page 148
- ◆ Section 9.14.5, "Example: Separate Files Based on Last Accessed Dates," on page 149
- ◆ Section 9.14.6, "Example: Separate Files Based on Last Modified Dates," on page 150
- ◆ Section 9.14.7, "Example: Move All Files from Older to Newer Storage," on page 152
- ◆ Section 9.14.8, "Example: Move Active Files from Older to Newer Storage and Maintain the Active/Inactive Separation," on page 152

9.14.1 Example: Move All Files Larger than 10 Megabytes

In this example, the filter identifies files with sizes of at least 10 megabytes. All files that meet this file size criterion are moved in a specified direction, such as from primary to secondary. The file access and modification times and file patterns are not considered.

Table 9-7 *Policy to Move All Files Larger than 10 Megabytes*

Option	Setting
Direction	Primary to secondary
File size	Select the check box, then: 1. Select *Greater than (>)* from the drop-down list. 2. Specify `10` in the unit field. 3. Select *Megabytes* from the drop-down list.
Last accessed	Not selected.
Last modified	Not selected.
File patterns	Not selected.
File types	Not selected.

9.14.2 Example: Move All MP3 Files Larger than 10 Megabytes

In this example, the filter identifies files with sizes of at least 10 megabytes and with a file extension of `.mp3`. Only the files that meet both the size and extension criteria are moved in the specified direction, such as from primary to secondary. The file access and modification times are not considered.

Table 9-8 *Policy to Move All MP3 Files Larger than 10 Megabytes*

Option	Setting
Direction	Primary to secondary
File size	Select the check box, then: 1. Select *Greater than (>)* from the drop-down list. 2. Specify `10` in the unit field. 3. Select *Megabytes* from the drop-down list.
Last accessed	Not selected.
Last modified	Not selected.
File patterns	Select the check box, then specify `*.mp3` in the field.
File types	Not selected.

9.14.3 Example: Move All MP3 Files Larger than 10 Megabytes That Were Last Accessed More than 6 Months Ago

In this example, the filter identifies files with sizes of at least 10 megabytes, with a Last Accessed setting that is at least 6 months ago, and with a file extension of .mp3. Only the files that meet all three criteria are moved in a specified direction, such as from primary to secondary. The file modification times are not considered.

Table 9-9 Policy to Move All MP3 Files Larger than 10 Megabytes That Were Last Accessed More than 6 Months Ago

Option	Setting
Direction	Primary to secondary
File size	Select the check box, then:
	1. Select *Greater than (>)* from the drop-down list.
	2. Specify 10 in the unit field.
	3. Select *Megabytes* from the drop-down list.
Last accessed	Select the check box, then:
	1. Select *Greater than (>)* from the drop-down list.
	2. Specify 6 in the unit field.
	3. Select *Months* from the drop-down list.
Last modified	Not selected.
File patterns	Select the check box, then specify *.mp3 in the field.
File types	Not selected.

9.14.4 Example: Move All Files

In this example, the filter identifies all files with any extension and moves them in the specified direction, such as from primary to secondary. All files are moved because there are no other filters to be considered.

Table 9-10 Policy to Move All Files

Option	Setting
Direction	Primary to secondary
File size	Not selected.
Last accessed	Not selected.
Last modified	Not selected.
File patterns	Select the check box, then specify *.* in the field to move all files with and without file extensions. To move only files with no extensions, specify *. in the field.

Option	Setting
File types	Not selected.

9.14.5 Example: Separate Files Based on Last Accessed Dates

In this example, assume that you want to keep recently accessed files on the faster storage where the primary path resides. You decide to separate the files in a pair based on the file Last Accessed dates, with recently accessed files on the primary path and dormant files on the secondary path. As noted elsewhere, files are served to users directly from the location where the file resides when the file is accessed via the network share on the primary path. If a file is accessed on the secondary path, its Last Accessed date changes, but it is not automatically moved back to the primary path.

To achieve the goal, set up one policy to move the files with older access dates from the primary path to the secondary path, and one policy to move recently accessed files from the secondary path to the primary path. Independently of DynamicFS, make sure that the *Last Accessed* field for a file is not modified during backups.

- ◆ "Move Files That Were Last Accessed More than 1 Month Ago from Primary to Secondary" on page 149
- ◆ "Move Files That Were Last Accessed Less than 1 Week Ago from Secondary to Primary" on page 150

Move Files That Were Last Accessed More than 1 Month Ago from Primary to Secondary

In this policy, specify a direction of primary to secondary, and a last accessed date of greater than 1 month. Run this policy weekly (or at a preferred frequency) during non-peak hours (such as Sunday at 12:00 a.m. until complete) to locate and move dormant files to the secondary path.

Table 9-11   *Policy to Move Files That Were Last Accessed More than 1 Month Ago from Primary to Secondary*

Option	Setting
Direction	Primary to secondary
File size	Not selected.
Last accessed	Select the check box, then: 1. Select *Greater than (>)* from the drop-down list. 2. Specify 1 in the unit field. 3. Select *Months* from the drop-down list.
Last modified	Not selected.
File patterns	Not selected.
File types	Not selected.

Move Files That Were Last Accessed Less than 1 Week Ago from Secondary to Primary

In this policy, specify a direction of secondary to primary, and a last accessed date of less than 1 week. Run this policy weekly during non-peak hours (such as Sunday at 12:00 a.m. until complete) to locate and move recently accessed files to the primary path.

Table 9-12   *Policy to Move Files That Were Last Accessed Less than 1 Week Ago from Secondary to Primary*

Option	Setting
Direction	Secondary to primary
File size	Not selected.
Last accessed	Select the check box, then: 1. Select *Less than (<)* from the drop-down list. 2. Specify 1 in the unit field. 3. Select *Weeks* from the drop-down list.
Last modified	Not selected.
File patterns	Not selected.
File types	Not selected.

9.14.6 Example: Separate Files Based on Last Modified Dates

In this example, assume that you want to keep recently modified files on the faster storage where the primary path resides. You separate the files in a pair based on the file Last Modified dates, with recently modified files on the primary path and the static files on the secondary path. As noted elsewhere, files are served to users directly from whichever location the file resides when the file is accessed via the network share on the primary path. If a file is modified on the secondary path, its Last Modified date changes, but it is not automatically moved back to the primary path.

To achieve the goal, you set up one policy to move static files from the primary path to the secondary path, and one policy to recently modified files from the secondary path to the primary path.

- "Move Files That Were Last Modified More than 1 Year Ago from Primary to Secondary" on page 151
- "Move Files That Were Last Modified Less than 1 Week Ago from Secondary to Primary" on page 151

Move Files That Were Last Modified More than 1 Year Ago from Primary to Secondary

In this policy, specify a direction of primary to secondary, and a last modified date of greater than 1 year. Run this policy monthly (or at a preferred frequency) during non-peak hours (such as Sunday at 12:00 a.m. until complete) to locate and move static files to the secondary path.

Table 9-13 *Policy to Move Files That Were Last Modified More than 1 Year Ago from Primary to Secondary*

Option	Setting
Direction	Primary to secondary
File size	Not selected.
Last accessed	Not selected.
Last modified	Select the check box, then:
	1. Select *Greater than (>)* from the drop-down list.
	2. Specify 1 in the unit field.
	3. Select *Years* from the drop-down list.
File patterns	Not selected.
File types	Not selected.

Move Files That Were Last Modified Less than 1 Week Ago from Secondary to Primary

In this policy, specify a direction of secondary to primary, and a last modified date of less than 1 week. Run this policy weekly during non-peak hours (such as Sunday at 12:00 a.m. until complete) to move recently modified files back to the primary path.

Table 9-14 *Policy to Move Files That Were Last Modified Less than 1 Week Ago from Secondary to Primary*

Option	Setting
Direction	Secondary to primary
File size	Not selected.
Last accessed	Not selected.
Last modified	Select the check box, then:
	1. Select *Less than (<)* from the drop-down list.
	2. Specify 1 in the unit field.
	3. Select *Weeks* from the drop-down list.
File patterns	Not selected.
File types	Not selected.

9.14.7 Example: Move All Files from Older to Newer Storage

In this example, suppose that you have existing storage and you want to move all files to a newer, faster storage disk. You do not plan to keep the existing storage after the move.

To achieve the goal, you set up a pair where the primary path is on the new disk, and the secondary path is on the old disk. The network share is configured (or reconfigured) for the primary path, which gives users access to all of the files via the merged view while DynamicFS migrates the files in off-peak hours.

You set up a policy with `*.*` (Move all files) in the *File patterns* filter option, and specify a direction of secondary to primary. This moves files with and without file extensions. Run the policy nightly during non-peak hours (such as at 12:00 a.m. for 4 hours). After all of the files have been moved to the primary location, the pair can be unlinked.

Table 9-15   *Policy to Move All Files from Older to Newer Storage*

Option	Setting
Direction	Secondary to primary
File size	Not selected.
Last accessed	Not selected.
Last modified	Not selected.
File patterns	Select the check box, then specify * . * in the field.
File types	Not selected.

9.14.8 Example: Move Active Files from Older to Newer Storage and Maintain the Active/Inactive Separation

In this example, suppose that you have existing storage and your goal is to move active files to a faster storage disk. You want to move recently accessed or modified files from the older disk to the newer disk. You plan to keep both disks to store the data. You also want to periodically check the fast disk for files that have not been accessed or modified during the past year so that they can be moved back to the older disk.

To achieve the goal, you set up a pair where the primary path resides on the new disk, and the secondary path resides on the old disk. The network share is configured (or reconfigured) for the primary path, which gives users access to all of the files via the merged view while DynamicFS migrates the files in off hours.

You set up the following policies that are scheduled to start at the same time:

- ◆ Move files accessed in the past month from the secondary to the primary path.
- ◆ Move files modified in the past 6 months from the secondary to the primary path.
- ◆ Move files that have not been accessed in the past year from the primary to the secondary path.

Two policies are required for moving files from the secondary to the primary path because you want to move files that meet one or the other of the criteria. If both filters are in the same policy, both conditions must be met for a file to move; only files that were accessed in the past month that also were modified in the past 6 months would be moved.

Only one policy is needed for moving inactive files from the primary to the secondary. If a file has been modified in the past year, it has also been accessed, so it automatically satisfies the Last Accessed filter criterion.

Move Files That Were Last Accessed Less than 1 Month Ago from Secondary to Primary

In this policy, specify a direction of secondary to primary, and a last accessed date of less than 1 month. Run this policy weekly during non-peak hours (such as Sunday at 12:00 a.m. for 4 hours) to locate and move recently accessed files to the primary path.

Table 9-16 *Policy to Move Files That Were Last Accessed Less than 1 Month Ago from Secondary to Primary*

Option	Setting
Direction	Secondary to primary
File size	Not selected.
Last accessed	Select the check box, then: 1. Select *Less than (<)* from the drop-down list. 2. Specify 1 in the unit field. 3. Select *Months* from the drop-down list.
Last modified	Not selected.
File patterns	Not selected.
File types	Not selected.

Move Files That Were Last Modified Less than 6 Months Ago from Secondary to Primary

In this policy, specify a direction of secondary to primary, and a last modified date of less than 6 months. Run this policy weekly during non-peak hours (such as Sunday at 12:00 a.m. for 4 hours) to move recently modified files to the primary path.

Table 9-17   Policy to Move Files That Were Last Modified Less than 6 Months Ago from Secondary to Primary

Option	Setting
Direction	Secondary to primary
File size	Not selected.
Last accessed	Not selected.
Last modified	Select the check box, then:
	1. Select *Less than (<)* from the drop-down list.
	2. Specify 6 in the unit field.
	3. Select *Months* from the drop-down list.
File patterns	Not selected.
File types	Not selected.

After the all of the most recently modified files have moved, you can disassociate this policy from the pair. Any new modifications that occur on the secondary path will satisfy the Last Accessed policy and be moved to the primary.

Move Files That Were Last Accessed More than 1 Year Ago from Primary to Secondary

In this policy, specify a direction of primary to secondary, and a last accessed date of greater than 1 year. Run this policy monthly (or at a preferred frequency) during non-peak hours (such as Sunday at 12:00 a.m. until complete) to locate and move inactive files to the secondary path.

Table 9-18   Policy to Move Files That Were Last Accessed More than 1 Year Ago from Primary to Secondary

Option	Setting
Direction	Primary to secondary
File size	Not selected.
Last accessed	Select the check box, then:
	1. Select *Greater than (>)* from the drop-down list.
	2. Specify 1 in the unit field.
	3. Select *Years* from the drop-down list.
Last modified	Not selected.
File patterns	Not selected.

Option	Setting
File types	Not selected.

9.15 What's Next

For information about monitoring the health and history of server disks that are used in pairs, the pairs, and the policies, see .

Monitoring Pairs and Policies

<div style="text-align: right">10</div>

Novell Dynamic File Services (DynamicFS) provides several monitoring features that can help you understand the current and historical status of pairs and policies. This section describes the statistics, history, logging, and auditing features and how to use the information they provide to monitor your DynamicFS solution.

10.1 Viewing the Pair Statistics

The Dynamic File Service scans each pair hourly and reports information about the pair's status, such as statistics for the last policy that was run and the status of policies assigned to a pair. This information can be viewed in the pair's Statistics dialog box. Each pair's Statistics dialog box opens in a separate window.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 In the left panel, select the *Pairs* folder to view the list of pairs in the right panel.

3 Double-click the pair name to open its Statistics dialog box.

4 On the *General* tab, view the status of the pair and the statistics for the last policy run.

The *Pair Status* area reports the following information. If a scan is currently running, the *Current Status* bar shows activity for that policy run.

Statistic	Description
Current status	Provides the status of whether a scan is currently running against the pair, or if it is idle.
Last run task	Indicates whether the last scan was initiated by a health check, a manual policy run of selected policies, or a scheduled run of selected policies.
Start time	Specifies the date and time that the last scan was started.
Elapsed time	Specifies the time elapsed for the scan in hours, minutes, and seconds.
Files scanned	Specifies the number of files scanned across both the primary and secondary locations.

Statistic	Description
Files to be moved	Specifies the number of files that are waiting to be moved.
Total size to be moved	Specifies the combined size of the files that are waiting to be moved.

5 View information about the policies that are associated with the pair.

The *Policies associated to pair* area lists the policies that are associated with the pair and reports the following information about them:

Statistic	Description
Name	Specifies the name given to the policy by the administrator.
Status	Indicates the current status of the policy, such as *Idle* or *Running*.
Last run	Specifies the date (MM/DD/YYYY) and time (HH:MM:SS AM or PM) that the policy was last run.
Elapsed time	Specifies the elapsed time for the scan in hours, minutes, and seconds.

6 Continue with the following tasks to view more statistical information for the pair:

10.2 Viewing the Policy Execution History for a Pair

The *Policy Execution History* tab in a pair's Statistics dialog box provides information about the most-recent 16 runs of policies on the pair. You can examine which policies were run and when. For each policy run, you can view lists of which files were moved and which files should have moved but didn't. This helps you to understand if policies are moving the files you expect to be moved.

When policies are run at the same time, the policies are grouped and run together by direction: *Primary to Secondary* and *Secondary to Primary*. Statistics for a policy run are aggregated based on the two direction categories, not by individual policies.

To view and explore the policy execution history for a pair:

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 In the left panel, select the *Pairs* folder to view a list of pairs in the right panel.

3 Double-click the pair name to open its Statistics dialog box, then select the *Pair execution history* tab.
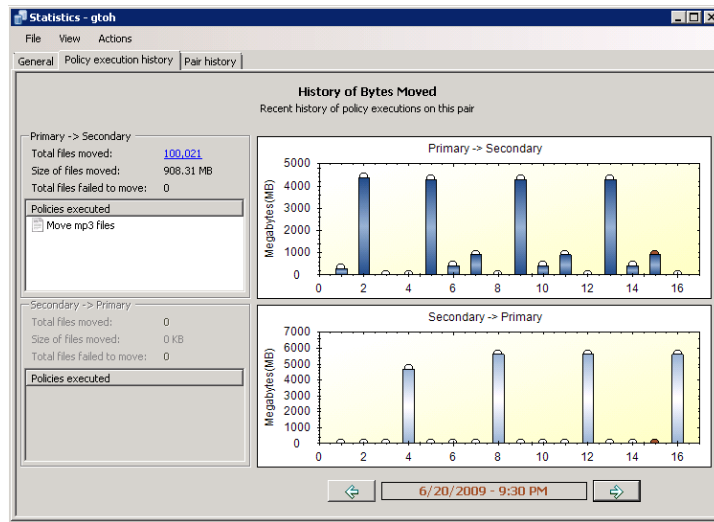
4 In the *Date and Time* area at the bottom of the page, use the left-arrow and right-arrow to select the run you want to explore.

The selected run is highlighted with a red disk at the top of its bar in the graph.

5 View the summary on the left that shows the policies that were run and the number of files that were moved or not moved.

Statistic	Description
History of bytes moved	The *History of bytes moved* area graphically displays the statistics for the last policy run, highlighted in red at the top of the bar. The bar charts display the number of megabytes moved from *Primary to Secondary* and *Secondary to Primary* by the policies being enforced in each policy run.
Date and time	The *Date and time* area shows when the policy run occurred. Use the left-arrow and right-arrow to navigate between the runs. Information about the currently selected policy run is displayed in the left panel.
Policies executed	The *Policies executed* area lists the policies that were enforced in that run.
Primary to secondary	The *Primary to secondary* area shows information about the files moved from the primary path to the secondary path for the specified policies. This area is dimmed if no policies in that run were configured to move data in that direction.
Secondary to primary	The *Secondary to primary* area shows information about the files moved from the secondary path to the primary path for the specified policies. This area is dimmed if no policies in that run were configured to move data in that direction.

Statistic	Description
Total files moved	The *Total files moved* field provides a link that opens the Run History dialog box if the value is non-zero. The run history lists each file that was moved in the specified direction. It provides the full path of the filename, the file extension, the file size, and any error messages for each file.
	For information, see Section 10.3, "Viewing a Policy Run History of Files Moved," on page 160.
Total files failed to move	The *Total files failed to move* field provides a link that opens the Run History dialog box if the value is non-zero. The run history lists each file that should have moved in the specified direction, but did not move. It provides the full path of the filename, the file extension, the file size, and any error messages for each file.
	For information, see Section 10.4, "Viewing a Policy Run History of Files that Failed to Move," on page 162.

6 (Optional) Save the graphic display by right-clicking anywhere in a graphical area and selecting any of the following options:

- ◆ **Copy:** Copies the selected graph as an image to the clipboard. Open a graphics editor, paste the image, and save the file.
- ◆ **Save Image As:** Opens a Windows Save As dialog box where you can specify a location and filename for the image, select a file format, then save the file.
- ◆ **Page Setup:** Set up the page orientation (portrait or landscape) and printer information for printing the graph.
- ◆ **Print:** Print the selected graph.

7 (Optional) Click the link for *Total files moved* to open the Run History dialog box where you can view a list of the files moved in a particular direction.

For information, see Section 10.3, "Viewing a Policy Run History of Files Moved," on page 160.

8 (Optional) Click the link for *Total files failed to move* to open the Run History dialog box where you can view a list of the files that should have moved in a particular direction, but that failed to move.

For information, see Section 10.4, "Viewing a Policy Run History of Files that Failed to Move," on page 162.

10.3 Viewing a Policy Run History of Files Moved

During a policy run, the Standard Policy engine records information about any file that is moved between the primary and secondary locations in a pair. A file is moved if it meets all of the filter options in a policy.

When policies are run at the same time, the policies are grouped and run together by direction: *Primary to Secondary* and *Secondary to Primary*. Statistics about the files that moved are aggregated based on the two direction categories, and not by the individual policies in the same policy run.

The *Total files moved* run history statistics for a policy run lists the files that moved in a given direction. For each file, the Run History report includes the full path of the filename, the file extension, the file size, and a comment for any error messages.

A file can appear to not move if you schedule policies to run at the same time that move a file in opposite directions. If the file is not listed in the *Total files failed to move* run history, look for it in the *Total files moved* run histories for the *Primary to secondary* and *Secondary to primary* statistics for the policy run.

To view the run history for files that moved in a policy run:

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 In the left panel, select the *Pairs* folder to view a list of pairs in the right panel.

3 Double-click the pair name to open the pair's Statistics dialog box, then select the *Pair execution history* tab.

4 In the *Date and Time* area at the bottom of the *Pair execution history* page, use the left-arrow and right-arrow to select the run you want to explore.

The selected run is highlighted with a red disk at the top of its bar in the graph.

5 In the left panel under *Primary to secondary* or *Secondary to primary*, click the link for *Total files moved*.

The Run History dialog box opens with a list of files that were moved in the selected direction.

6 Use any of the following options to view information or to locate a file of interest:

Scroll: The list is paged to show up to 1000 files at a time. On each page, scroll down to see up to 1000 filenames listed.

Page: Click the left-arrow and right-arrow to move page-by-page through the run history. You can also use the *Page* drop-down list to jump directly to a page.

Sort: Click the heading of a column to sort the list by filename, file extension, file size, or comment.

IMPORTANT: The sorting is text-based, so it lists the information alphabetically, not numerically.

Filtering: Use the filter option in the upper right corner to type a sequence of letters to find specific files in the list. Specify the sequence in the field, then click the magnifying glass to apply the filter.

In the example below, the files are sorted by filename, and the search has filtered out files that do not contain the sequence of characters "test118".

7 When you are done viewing the list, close the Run History dialog box. (Click the X in the upper right corner, or press Alt+F4.)

10.4 Viewing a Policy Run History of Files that Failed to Move

During a policy run, the Standard Policy engine records information about any file that should move but fails to move. A file should move if it meets all of the filter options in a policy. Reasons that a file might fail to move during a policy run include the following:

- The source file is open and in use.
- Free space on the target disk is insufficient for the file size.
- A file with the same filename is present in the same folder on the target location.
- The source location or the target location of a file move becomes unavailable.
- The Dynamic File Services Storage Rights group or `NDFS-servername` proxy user has insufficient permissions on the remote share or file system in a pair.
- Exceptions caused by timing issues with the Windows file system.

When policies are run at the same time, the policies are grouped and run together by direction: *Primary to Secondary* and *Secondary to Primary*. Statistics about the files that failed to move are aggregated based on the two direction categories, and not by the individual policies in the same run.

The *Total files failed to move* run history statistics for a policy run lists the files that failed to move in a given direction. For each file, the Run History report includes the full path of the filename, the file extension, the file size, and a comment for any error messages.

A file can appear to fail to move if you schedule policies to run at the same time that move files in opposite directions. If the file is not listed in the *Total files failed to move* run history, look for it in the *Total files moved* run histories for the *Primary to secondary* and *Secondary to primary* statistics for the policy run as described in Section 10.3, "Viewing a Policy Run History of Files Moved," on page 160.

To view the run history for files that failed to move in a policy run:

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 In the left panel, select the *Pairs* folder to view a list of pairs in the right panel.

3 Double-click the pair name to open the pair's Statistics dialog box, then select the *Pair execution history* tab.

4 In the *Date and Time* area at the bottom of the *Pair execution history* page, use the left-arrow and right-arrow to select the run you want to explore.

The selected run is highlighted with a red disk at the top of its bar in the graph.

5 In the left panel under *Primary to Secondary* or *Secondary to Primary*, click the link for *Total files failed to move*.

The Run History dialog box opens with a list of files that should have moved in the selected direction but did not move.
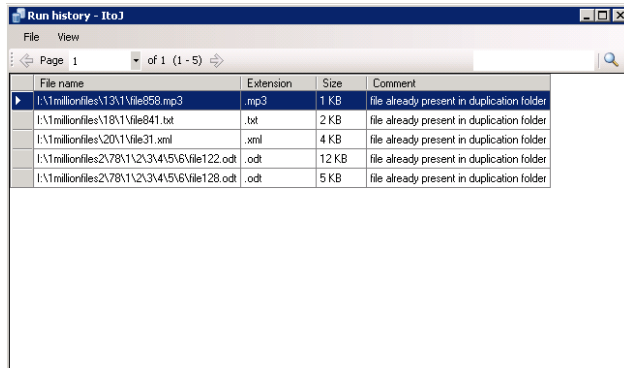
6 Use any of the following options to view information or locate a file of interest:

Scroll: The list is paged to show up to 1000 files at a time. On each page, scroll down to see up to 1000 filenames listed.

Page: Click the left-arrow and right-arrow to move page-by-page through the run history. You can also use the *Page* drop-down list to jump directly to a page.

Sort: Click the heading of a column to sort the list by filename, file extension, file size, or comment.

IMPORTANT: The sorting is text-based, so it lists the information alphabetically, not numerically.

Filter: Use the filter option in the upper right corner to type a sequence of letters to find specific files in the list. Specify the sequence in the field, then click the magnifying glass to apply the filter.

7 When you are done viewing the list, close the Run History dialog box. (Click the X in the upper right corner, or press Alt+F4.)

10.5 Viewing the Pair History

The Pair History tab in a pair's Statistics dialog box shows the amount of space consumed over time on the devices that are used in a pair. You can view a summary of a particular scan event by the file extension, file size, last accessed, last modified, and creation time. You can display each of these graphs by total size consumed or by the number of files. Each scan event opens in a separate window so that you view and compare multiple events.

By default, the pair history scan runs once daily at 4:00 a.m. This setting is configurable. For information, see Section 8.10, "Scheduling the Pair History Scan," on page 119.

For information about the storage status and history for the disks that are used in a pair, see Section 10.6, "Viewing Capacity and Used Space History for Server Disks," on page 165.

1 In the Management Console, connect to the DynamicFS server that you want to manage.

2 Under the *Pairs* folder, double-click the pair name to open the Statistics dialog box, then select the *Pair history* tab.

The Pair History graph shows the total file size over time for the primary location (a dark blue square icon) and the secondary location (a light blue circle icon). A scan event is recorded for each time that the Pair History scan is run.
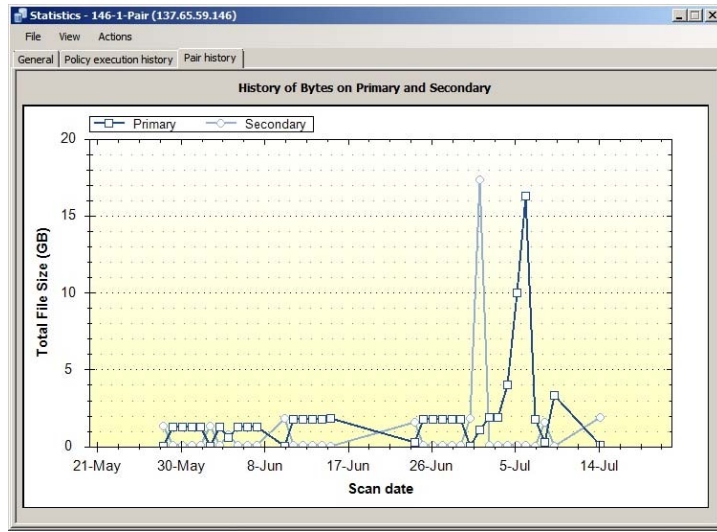
3 Double-click the scan event for the primary (a dark blue square icon) location or the secondary location (a light blue circle icon) to open a graphical summary of the scan in a separate dialog box.

A graph of the scan is displayed by file extension and total file size of all the files moved in that category.

4 In a Summary dialog box, modify the display parameters to view the information of interest:

4a Select *Total Size* (default) to view the information organized by file size in the categories.

4b Select *Number of Files* to view the information organized by number of files in the categories.

4c In the *Graph Option* drop-down box, select one of the following parameters to modify the information that is displayed:

- Accessed
- Creation
- Modified
- File Size
- Extension (default)

5 (Optional) Save a graphic display by right-clicking anywhere in a graphical area and selecting one of the following options:

- **Copy:** Copies the selected graph as an image to the clipboard. Open a graphics editor, paste the image, and save the file.

- **Save Image As:** Opens a Windows Save As dialog box where you can specify a location and filename for the image, select a file format, then save the file.
- **Page Setup:** Set up the page orientation (portrait or landscape) and printer information for printing the graph.
- **Print:** Print the selected graph.

6 (Optional) Compare multiple scan events by opening their Summary dialog boxes side-by-side.

10.6 Viewing Capacity and Used Space History for Server Disks

You can view the capacity and used space information about the disks on a Dynamic File Services server. Viewing the server's disk history can help you understand space usage patterns for a disk for planning purposes.

IMPORTANT: You can view the pair history (as described in Section 10.5, "Viewing the Pair History," on page 163) for each pair to determine how much space is being used by the primary path or secondary path on a disk.

You can also view the policy run history for a pair (as described in Section 10.2, "Viewing the Policy Execution History for a Pair," on page 158) to determine how much data is being moved by different policy runs on the pair.

- Section 10.6.1, "Viewing Disk Details and History," on page 165
- Section 10.6.2, "Sample Disk History for a Primary Disk," on page 167
- Section 10.6.3, "Sample Disk History for a Secondary Disk," on page 167

10.6.1 Viewing Disk Details and History

1 In the Management Console, connect to the DynamicFS server you want to manage.

2 Right-click the server, then select *Properties*.

3 Select the *Disk Details* tab to view the following information for local disks on the target server:

Property	Description
Disks	List of the disks attached as local drives on the server. It shows their capacity, free space in gigabytes, and free space as a percentage.
File system	The file system type, such as NTFS.
Graphical display	A graph of the used space and free space on the selected disk.

Information is displayed by default about the `C:\` drive.

4 Select a disk to view its file system, capacity, and used space information.
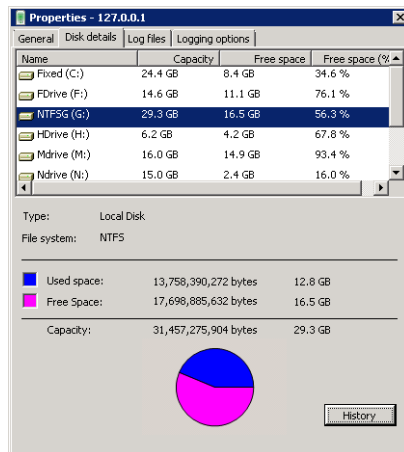
5 Select a disk and click *History* to view information about how the used space has changed over time.
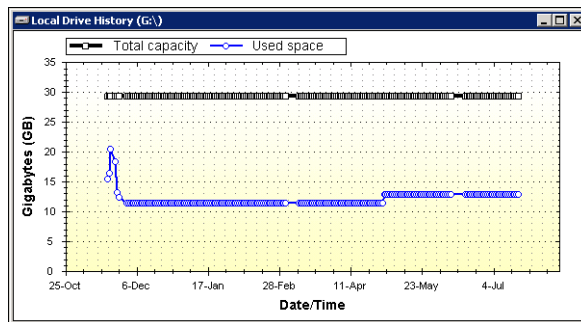
6 (Optional) Save the graphic display by right-clicking anywhere in a graphical area and selecting any of the following options:

- ◆ **Copy:** Copies the selected graph as an image to the clipboard. Open a graphics editor, paste the image, and save the file.

- ◆ **Save Image As:** Opens a Windows Save As dialog box where you can specify a location and filename for the image, select a file format, then save the file.

- ◆ **Page Setup:** Set up the page orientation (portrait or landscape) and printer information for printing the graph.

- ◆ **Print:** Print the selected graph.

10.6.2 Sample Disk History for a Primary Disk

The following sample Local Drive History graph displays the capacity history for a disk that is managed by Dynamic File Services, where the disk contains one or more primary paths of pairs. Policies were scheduled to run during non-peak hours so that the data could be moved over a period of days or weeks, depending on the amount of data to be moved, while allowing users to continue working with the data.
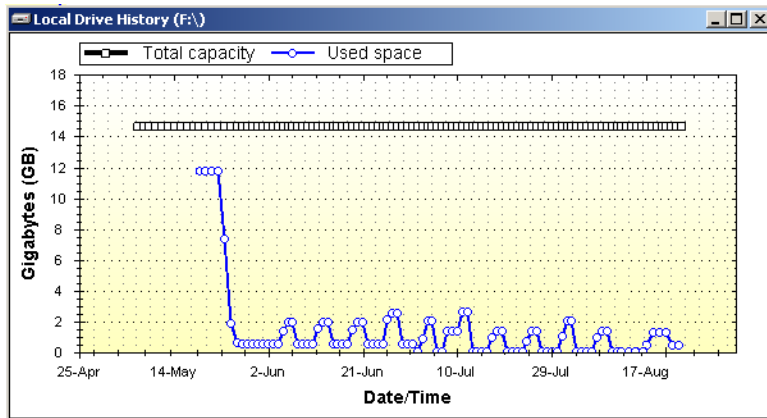
Initially, policies were run daily during non-peak traffic times on each pair to move files by type, size, or date last accessed or modified from the primary disk to a secondary disk (not pictured). Thereafter, the policy schedule was modified to run weekly during non-peak traffic times to move any new files that match the specified criteria from the primary disk to the secondary disk.

10.6.3 Sample Disk History for a Secondary Disk

The following sample Local Drive History graph shows a disk that contains one or more secondary paths of pairs. Initially, the disk contained little or no data. Over time, the disk capacity is being consumed by files that are moved by policies from primary paths on one or more other disks (not pictured) to their secondary paths on this disk.
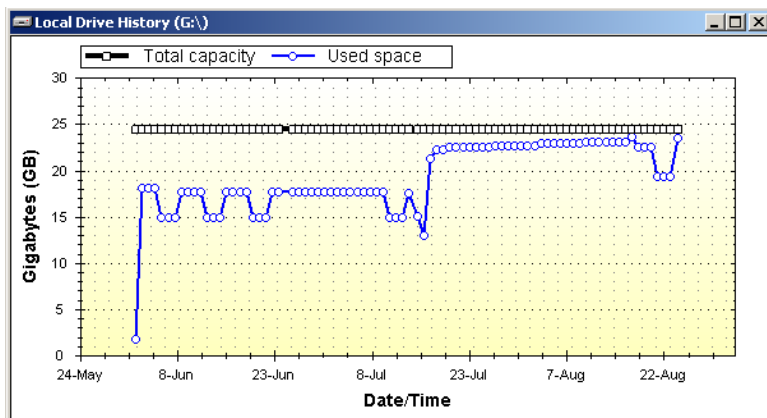
Because the disk capacity is near its maximum, you might need to take one or more of the following actions:

- Stop some policies from running by disabling their schedules, or by disassociating them from some pairs.
- Create new policies to move some data back to the primary paths.
- Stop using the disk as the secondary location for some pairs. This involves the following tasks:
    1. Disassociate a pair from its current policies.
    2. Create a new policy for the pair to move all of the files on the secondary path to the primary path. The policy can be scheduled to run in non-peak hours over several days or weeks, depending on how much data needs to be moved.
    3. After all of the data has been returned to the primary location, unlink the primary path and the secondary path to remove the pair relationship between the two locations. This automatically disassociates the pair from any policies.
    4. Create a new pair that links the primary path to a secondary path on a different disk.
    5. Associate the pair with one or more policies to move specified file types to the new secondary location.

To help determine which pairs need to be modified, you can view the pair history (as described in Section 10.5, "Viewing the Pair History," on page 163) for each pair to determine how much space is being consumed by each pair's secondary path. You can also view the policy run history for the pair (as described in Section 10.2, "Viewing the Policy Execution History for a Pair," on page 158) to determine if a policy is moving more data than you intended to be moved, and to understand how the policy might be modified to better meet your goals.

10.7 Viewing Logged Events

Event logs for the following Dynamic File Services components can be viewed in the *Server Properties > Log Files* page in the Management Console:

Event Log File	Component	Description
DswMpcCore.log	Dynamic File Service	Logs events for the core engine.
DswStandardPolicy.log	Standard Policy engine	Logs events for policy runs.
install.log	Installation	Logs events during the install about setting up the Dynamic File Services group on the local server and the Dynamic File Services Storage Rights (DFSStorageRights) group and the server proxy user in Active Directory.
DswSyncPair.log	Synchronize Pair utility	Logs events each time you manually run the SyncPair utility. The log is created the first time the utility is run.

Event Log File	Component	Description
DswInventory.log	File Inventory utility	Logs events each time you manually run the File Inventory utility. The log file is created the first time the utility is run.

You can modify the logging level for the Service and Standard Policy logs to change the types of events that are logged. For information, see Section 6.10, "Configuring the Logging Level for the Service and Standard Policy Log Files," on page 92.

1 In the Management Console, connect to the DynamicFS server you want to manage.

2 Right-click the server, then select *Properties*.

3 Select the *Log files* tab.

   The available log files are listed in the drop-down list.

4 From the drop-down list, select a log file to view its messages.

   Messages are listed in chronological order in the display window. Scroll down to view the most recent messages.

5 (Optional) In the *Search* field type a sequence of characters that you want to find, then click the *Search* icon to jump to instances of those characters in the log.
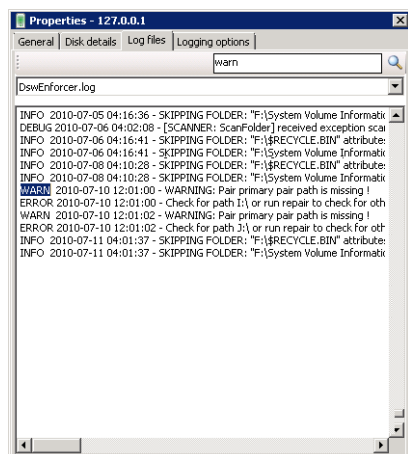
10.8 Viewing Service Events

Dynamic File Services uses the Microsoft Event Viewer for logging events like starting and stopping the Service, and application execution errors. See the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/ee624055(WS.10).aspx) for documentation on viewing events with the Event Viewer snap-in for the Microsoft Management Console (MMC).

10.9 Auditing Management Events

Auditing the management events for the Dynamic File Service, pairs, and policies is integrated with DynamicFS and is provided as a basic benefit. The purpose of the audit log is to record which logged-in user performs major management operations, such as create, delete, and modify (which includes association and disassociation of the policies with pairs).

All Dynamic File Services management actions are audited. All authentication and authorization events are audited, including both authorized and non-authorized management actions. No sensitive information is placed in the audit log. The audit log also reports when the Service is stopped and started.

The audit log reports the user's IP address, name, and the time of access for management events. It reports *System* as the user when scheduled policies are run.

The audit file is protected so that it cannot be deleted or accessed by unauthorized users.

- ◆
- ◆

10.9.1 Viewing Audit Log Events

Dynamic File Services automatically audits the management tasks for creating and managing the Service, pairs, and policies. The following audit logs are by default located in the `\audit` folder in the `C:\Program Files\Dynamic File Services` folder, or in the folder where you installed DynamicFS:

File	Description
DswAuditLog.xml	Logs the management events for the Dynamic File Service, pairs, and policies
DswAuditCfg.xml	Controls the logging behavior for the audit log

There is no special way to view this file. It is an XML file, and most HTTP browsers can display well-formed XML in a readable form. You can also view the file in a text editor.

It is necessary to review information about the audited management events in combination with information reported in the Service log (`DswMpcCore.log`). There might be related Service events that are automatically generated from a single management task. For information about viewing the Service log, see .

For example, if a pair is deleted, the deletion event is recorded in the audit log, and the related automatic disassociations of policies from the deleted pair are recorded in the Service log. The logged disassociation message lists all of the policies with a boolean `true` or `false` indication for each of whether the disassociation occurred for that policy. You would expect a previously associated policy to report a value of `true` after a successful disassociation.

10.9.2 Detecting and Resolving a Corrupted Audit Log

If the audit log file becomes corrupted so that it contains malformed XML, scheduled policies might not run or the local drive history might not function.

Dynamic File Services automatically checks that the audit log file contains well-formed XML whenever an audited event is added to the Audit log file. If malformed XML is detected, the following events automatically occur:

1. The corrupted audit log is renamed by adding a GUID to the end of the filename.

   This allows for multiple instances of the file to be saved in the …`\Dynamic File Services` folder.

2. A new audit log file is started.

3. An entry is added in the new log stating that the audit log was detected to have a problem and a new one was started.

4. An event is sent to the Windows Event Logger stating that an improperly formatted audit log file was detected, and providing the name of the renamed log file.

5. The audited event is written to the new audit log file.

If you are not it if i ed of a corrupted audit log event in the Windows Event Logger, you can view the old renamed audit log file in a text editor to assess the extent of the corruption. No further administrator action is required.

10.10 Generating a Configuration Report

To help with record-keeping and troubleshooting, you can generate a report about the Dynamic File Services configuration on the server. The Configuration Dump utility (`DswDump.exe` command) collects information about the settings for the Service, pairs, policies, and logs on a server, and dumps the information to a file called `Config.txt` in the `C:\Program Files\Dynamic File Services` folder (or the folder where you installed DynamicFS). The command can be run at any time, whether the Service is running or not running.

1 Log in to the DynamicFS server as the Administrator user, or as a user in the `Dynamic File Services` group.

2 Open a command prompt console. Select *Start > All Programs > Accessories*, then click *Command Prompt*.

3 Use the Change Directory (`cd`) command to go to the `C:\Program Files\Dynamic File Services` folder (or the folder where you installed Dynamic File Services).

4 At the command prompt, enter

`dswDump.exe`

The results are written to the `Config.txt` file in the `C:\Program Files\Dynamic File Services` folder (or the folder where you installed Dynamic File Services).

The following progress messages are output to the screen:

```
... starting
... output file = Config.txt

... Configuration Information
... Active Directory Information
... Files Information
... Pairs Information
... Policies Information
... Audit Information
... Microsoft Event Logger
... Log Files
... flushing output file
... perform cleanup
... finished
```

5 View the `Config.txt` report in a text editor such as Notepad.

Repairing the Pair and Policy Databases

11

Novell Dynamic File Services (DynamicFS) provides a repair capability that can help to repair the pair and policy database files in the unlikely event of corruption. It consists of a set of software library functions that are used by the Dynamic File Service. Some of the functions are also available to administrators through the Repair Tool. This section describes how the repair capability is used to help ensure that the pair and policy database files are valid.

11.1 Understanding the Dynamic File Services Repair Capability

The Dynamic File Service requires that the pair and policy database files be valid in order for the Service to run. The repair capability provides the following functions that help the Service to proactively ensure the health of the pair and policy database files. Each of these functions is described in more detail later in this section.

- **Report:** Checks the consistency of configuration information in the pair and policy database files. It reports health information, non-fatal errors, and fatal errors.
- **Repair:** Fixes problems with the pair and policy database files if it can.
- **Snapshot:** Saves a daily snapshot of valid pair and policy database files.

Whenever it is started, the Service uses the Report function to check the consistency of the pair and policy database files. If errors are detected, it uses the Repair function to repair the errors if it can. The Service also runs the Snapshot function daily at a scheduled time to save a valid snapshot of the database files. These actions are performed only if the Service is running.

The *Repair Tool* option in the Service Controller menu allows an administrator to manually run the Report and Repair functions as needed. The tool can be run when the Dynamic File Service is running or not running.

See the following sections to understand how the repair capability is used to detect and repair problems in the pair and policy database files.

11.1.1 What Are the Pair and Policy Database Files?

The pair and policy database files contain configuration information about the pairs and policies that you create on a server. The schedule information for the daily snapshot is also verified with the database files.

Pair Database Files

The …\Dynamic File Services\Pairs folder contains the pairs database file (DswPairDatabase.xml) and a separate subfolder for each pair that you create on the server.

The database file contains the configuration information for all of the pairs on the server. Each pair's information begins with the <DswPairEntry> XML tag and ends with the </DswPairEntry> XML tag.

The subfolder for each pair is named with the pair's GUID (globally unique identifier), such as f59058ea-ae9a-4352-bf3c-cc3a7d7fc443. In this folder, a PairSummaryHistoryTable.xml file stores historical information for the individual pair. The repair capability does not check or repair a pair's folder and historical information file.

Policy Database Files

The …\Dynamic File Services\Policies folder contains the policy database file (DswPolicyDatabase.xml) and a separate configuration file for each policy that you create on the server. It also contains the configuration files for two global policies that you should not alter: the Global Conflict policy and the Global Remove Pair policy.

The database file contains a GUID and name for each policy on the server, including the global policies. For example:

```
8ee0b624-2ac0-44ce-ad54-3eadb2cb4f91
My JPG P2S Policy
```

Each individual policy file is named with the policy's GUID, such as 8ee0b624-2ac0-44ce-ad54-3eadb2cb4f91. A policy file contains the policy's configuration settings in XML format between the <StandardPolicy> and </StandardPolicy> tags.

Database Snapshot Schedule File

The …\Dynamic File Services\DswCore.xml file contains the schedule information for the repair Snapshot function that is run daily by the Dynamic File Service.

11.1.2 What Causes Errors in the Database Files?

Errors in the database files are expected to occur rarely, if at all. Common causes for corruption might be:

- If a connection to the server is lost when you are creating a pair or policy
- If the server crashes while you are creating a pair or policy
- If the file system where the database files are stored becomes corrupted
- If you introduce errors by attempting to manually modify the content of a database file

11.1.3 Checking the Database Consistency at Service Start

When the Dynamic File Service starts, it automatically uses the repair capability to check the consistency of the pair and policy database files and to repair any problems if it can. The Service has all of the permissions and rights necessary to run the Report and Repair functions.

The database check on Service start performs the following tasks:

1. The Report function opens the pair and policy database files (as described in Section 11.1.1, "What Are the Pair and Policy Database Files?," on page 174) and checks the consistency of information in them.
2. If the Report function detects errors, it determines if the errors are non-fatal or fatal.
3. If errors are detected, the Repair function automatically repairs them if possible, using the following repair methods:
   - **Silent Repair:** For non-fatal errors, the Repair function makes the repairs silently (no messages are generated).
   - **Snapshot Rollback Repair:** For fatal errors, the Repair function uses the database snapshots to roll back to the most recent snapshot of the database files.

     For information about the database snapshot process, see Section 11.1.4, "Taking Daily Snapshots of the Pair and Policy Database Files," on page 177.
4. If a snapshot rollback repair effort fails, the Service does not start. An error message is logged in the Windows Event Logger.

Two failure events trigger an entry in the Windows Event Logger:

- The repair capability does not respond when it is called by the Service to begin the database check.
- A snapshot rollback fails because there is no snapshot available to roll back to.

The following sections identify the nature of errors and repair actions:

- "Pair Database Errors" on page 176
- "Policy Database File Errors" on page 176
- "Individual Policy XML File Errors" on page 176

Pair Database Errors

Table 11-1 identifies errors that might occur in the DswPairDatabase.xml file. Fatal errors cause the pair database to remain closed. For fatal errors (not repairable), all database files are rolled back to a previous snapshot.

Table 11-1   *Pair Database XML File Errors*

Error Condition	Repairable or Not Repairable	Automatic Repair Action
DswPairDatabase.xml is not valid XML.	Not repairable	Rolls back database files to the latest snapshot
Any pair GUID is missing or damaged.	Repairable	Repairs silently
Any pair name is missing or damaged.	Repairable	Repairs silently
Any missing results folder in the XML.	Repairable	Repairs silently
Missing primary or secondary folder.	Not repairable	Rolls back database files to the latest snapshot

Policy Database File Errors

Table 11-2 identifies errors that might occur in the DswPolicyDatabase.xml file. Fatal errors cause the policy database to remain closed. For fatal errors (not repairable), all database files are rolled back to a previous snapshot.

Table 11-2   *Policy Database XML File Errors*

Error Condition	Repairable or Not Repairable	Automatic Repair Action
DswPolicyDatabase.xml is not valid XML.	Not repairable	Rolls back database files to the latest snapshot
Any policy GUID is missing or damaged.	Repairable	Repairs silently
Any policy name is missing or damaged.	Repairable	Repairs silently
Corresponding policy XML file is missing or has damaged XML.	Not Repairable	Rolls back database files to the latest snapshot

Individual Policy XML File Errors

Table 11-3 identifies errors that might occur in an individual policy's .xml file. Fatal errors cause the policy database to remain closed. For fatal errors (not repairable), all database files are rolled back to a previous snapshot.

Table 11-3   *Policy XML File Errors*

Error Condition	Repairable or Not Repairable	Automatic Repair Action
The policy XML is not valid XML.	Not repairable	Rolls back database files to the latest snapshot
The policy GUID is missing or damaged.	Repairable	Repairs silently
The policy name is missing or damaged.	Repairable	Repairs silently
The policy type is missing or damaged.	Repairable	Repairs silently
The policy direction is missing or damaged.	Not Repairable	Rolls back database files to the latest snapshot

11.1.4 Taking Daily Snapshots of the Pair and Policy Database Files

Dynamic File Services provides the Snapshot function as a precautionary measure to help resolve fatal errors that might rarely occur in the pair or policy database files. If it is necessary, the Repair function can roll back the pair and policy database files to the most recent set of known-to-be-good set of snapshot files. The Dynamic File Service has all of the permissions and rights necessary to run the Snapshot function.

Each day at a scheduled time, the Dynamic File Service automatically calls the Snapshot function to take a snapshot of the pair database file, the policy database file, and the individual policy configuration files. The Service must be running in order for the snapshot service to be called at its scheduled time and while the snapshot is being taken.

Before a snapshot is taken, the database files are checked for consistency to make sure they are valid, and non-fatal errors are repaired. The known-to-be-good set of files are stored in the …\Dynamic File Services\SnapShot*day_of_the_week* folder. If any one of the database files is found to have fatal errors, a snapshot is not saved.

Only one snapshot for each day of the week is kept at any given time. The snapshots are retained on a seven-day rotation. For information about which files comprise the set of files that are saved in a snapshot, see Section 11.1.1, "What Are the Pair and Policy Database Files?," on page 174.

The snapshots are taken by default between 11:30 p.m. and midnight daily. The time values for when the snapshot is taken are stored in the …\Dynamic File Services\DswCore.xml file. There is no interface to change the time when the snapshots are taken.

11.1.5 Rolling Back the Pair and Policy Database Files to a Snapshot Version

When the repair capability detects a fatal error during the Service start, it automatically attempts to repair the database by rolling back to the most recent snapshot. The rollback process is also used to repair fatal errors when the *Repair Tool* option in the Service Controller is run manually in Repair mode.

The following tasks are performed by the snapshot rollback process:

1. The Repair function checks the previous day's snapshots folder for the database files that were previously known to be good.

2. If the snapshot for the previous day does not exist, the Repair function checks each previous daily snapshot folder in turn for database files.

3. If a snapshot is located, the Repair function rolls back the pair and policy databases to the snapshot version of the files.

   It copies the snapshot version of the `DswPairDatabase.xml` file, the `DswPolicyDatabase.xml` file, and all of the individual policy files to the correct location in the `Pairs` and `Policies` folders.

4. If a snapshot is not available, the Repair function logs an event in the Windows Event Logger.

   The message indicates that the fatal error occurred and that there were no snapshot files available to roll back to.

11.1.6 Manually Repairing the Pair and Policy Database Files

You can manually check the consistency of the pair and policy database files and repair them by selecting the *Repair Tool* option in the Service Controller menu.

The Repair tool can be run by a non-administrator user. When you click *Run*, the tool prompts for the username of a user with rights to all of the paths in the pair. It does not require a password. The tool runs as the username provided. When the report or repair is done, the identity returns to the identity of the currently logged-in user. If the username is left blank or if you click *Cancel* when you are prompted for the username, the tool runs as the user that is currently logged in to the server desktop.

IMPORTANT: Typically, the username provided is a user identity that has Administrator privileges. If a remote secondary path is used in a pair, you must provide the username of a user that also has Administrator privileges on the DynamicFS server, rights on the remote share, and NTFS file system access rights on the secondary path. Otherwise, the secondary location is reported as missing. One way to do this is to add the username as a member of the Dynamic File Services Storage Rights (`DFSStorageRights`) group. It does not matter if the user is also a member of the `Dynamic File Services` group.

The *Repair Tool* GUI menu provides two modes:

 ◆ **Report Mode:** Checks the consistency of the database files, identifies errors, and indicates whether an error is repairable or not. No attempt is made to fix anything.

 ◆ **Repair Mode:** Repairs the errors if it can by using silent repair for non-fatal errors and the rollback repair for fatal errors.

You can run the Report mode and Repair mode for the pair database files, the policy database files, or both.

For information about running the Report tool, see the following

 ◆ **Section 11.2, "Generating a Report for the Pair and Policy Databases," on page 179**
 ◆ **Section 11.3, "Repairing the Pair or Policy Databases," on page 180**

11.2 Generating a Report for the Pair and Policy Databases

When the Dynamic File Service starts, it automatically calls the repair capability to check the consistency of the pair and policy database files. You can manually run the Repair tool in Report mode to check the consistency of the pair and policy database files.

You must be able to provide the username of a user with rights to all of the paths in the pair. For information, see Section 11.1.6, "Manually Repairing the Pair and Policy Database Files," on page 178.

You might need to generate a report if the Service cannot open a pair or policy, or if a database error is reported in the Windows Event Logger after a Service start.

1 Log in to the DynamicFS server as a user with file system rights on both the primary and secondary paths of the pair you want to manage.

If remote shares are being used, make sure that you have sufficient access rights on the secondary locations.

2 On the server, start the Repair tool by right-clicking the Service Controller icon in the notification area and selecting *Repair Tool* from the menu.

3 In the *Repair type* area, select *Report*.
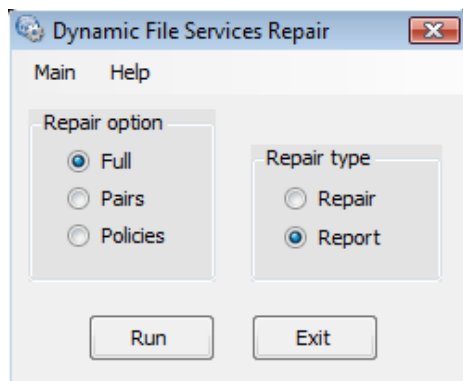
4 In the *Repair option* area, select one of the following options:

Full: Checks the consistency of both the pair and policy database files.

Pairs: Checks the consistency of the pair database files.

Policies: Checks the consistency of the policy database files.

For information about the types of errors reported, see Section 11.1.3, "Checking the Database Consistency at Service Start," on page 175.

5 Select *Run* to begin the report process.

6 When you are prompted, enter the username of a user with rights to all of the paths in the pair, then click *OK*.

If the username is left blank or if you click *Cancel* when you are prompted for the username, the tool runs as the user that is currently logged in to the server desktop.

When the report is completed, the Repair Results dialog box opens.

7 View the report.

The *Repair type* and the *Repair option* that you specified are displayed at the top of the dialog box. A full report includes the following:

- ◆ Policy database status and errors
- ◆ Pair database status and errors
- ◆ `DswCore.xml` file status and errors

8 (Optional) Save the report by using either of the following methods:

- ◆ Click *Copy to clipboard*, then paste the information in any text file.
- ◆ Click *Save to file*, browse to locate the folder where you want to save the file, specify a filename, then click *Save*.

  The default filename is `DswRepair.log`.

9 When you are done, click *Close* to close the Repair Results dialog box.

10 Do one of the following:

- ◆ **No Errors Are Reported:** Click *Exit* to close the Repair tool.
- ◆ **Errors Are Reported:** Continue with Section 11.3, "Repairing the Pair or Policy Databases," on page 180.

11.3 Repairing the Pair or Policy Databases

When the Dynamic File Service starts, the Service automatically calls the repair capability to repair the pair and policy database files if errors are detected during the consistency check. You can manually run the Repair tool in Repair mode to try to repair errors in the pair and policy database files.

You must be able to provide the username of a user with rights to all of the paths in the pair. For information, see Section 11.1.6, "Manually Repairing the Pair and Policy Database Files," on page 178.

You might need to run the Repair tool in *Repair* mode if a database error is reported in a Repair Report that you generated.

The Repair tool repairs any errors that it can fix. If fatal errors cannot be resolved by a snapshot rollback, an event is triggered for the Windows Event Logger to that effect.

1 Log in to the DynamicFS server as a user with file system rights on both the primary and secondary paths of the pair you want to manage.

If remote shares are being used, make sure that you have sufficient access rights on the secondary locations.

2 On the server, start the Repair tool by right-clicking the Service Controller icon in the notification area and selecting *Repair Tool* from the menu.

3 In the *Repair type* area, select *Repair*.
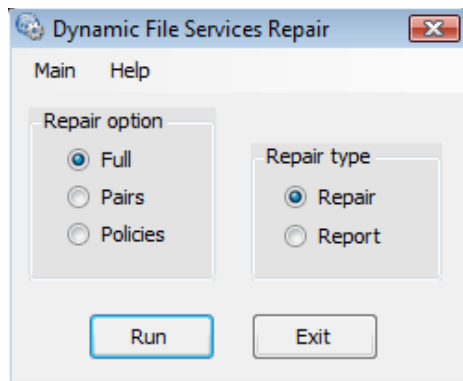
4 In the *Repair option* area, select one of the following options:

Full: Repairs errors if possible in both the pair and policy database files.

Pairs: Repairs errors if possible in the pair database files.

Policies: Repairs errors if possible the policy database files.

5 Select *Run* to begin the repair process.

6 When you are prompted, enter the username of a user with rights to all of the paths in the pair, then click *OK*.

If the username is left blank or if you click *Cancel* when you are prompted for the username, the tool runs as the user that is currently logged in to the server desktop.

When the repair is completed, the Repair Results dialog box opens.

7 View the report.

The *Repair type* and *Repair option* that you specified are displayed at the top of the dialog box. A full report includes the following:

- ◆ Policy database status and errors fixed or not fixed.
- ◆ Pair database status and errors fixed or not fixed.
- ◆ `DswCore.xml` file status and errors fixed or not fixed.

8 (Optional) Save the repair information by using either of the following methods:

- ◆ Click *Copy to clipboard*, then paste the information in any text file.
- ◆ Click *Save to file*, browse to locate the folder where you want to save the file, specify a filename, then click *Save*.

 The default filename is …`\Dynamic File Services\DswRepair.log`.

9 When you are done, click *Close* to close the dialog box, then click *Exit* to close the Repair tool.

10 If a snapshot rollback repair occurs, you should use the Management Console to review the restored pairs and policies to make sure that they reflect any recent configuration changes that you made. For information about repair issues after a successful snapshot rollback repair, see the following:

- ◆ Section 11.4.1, "What If a Pair's Secondary Data Location Appears to Be Missing After a Snapshot Rollback Repair?," on page 182
- ◆ Section 11.4.3, "What If Policies Run or Don't Run as Expected After a Snapshot Rollback Repair?," on page 183

11 If a rollback to a snapshot of the database files fails, a repair event is logged in the Windows Event Logger. Continue to the following sections to manually resolve the corrupted database errors:

- Section 11.4.4, "What If a Pair Database Error Cannot Be Fixed?," on page 183
- Section 11.4.5, "What If a Policy Database Error Cannot Be Fixed?," on page 184

11.4 Troubleshooting Repair Issues

If a snapshot rollback repair occurs, you should use the Management Console to review the recovered pairs and policies to make sure that they reflect any recent configuration changes that you made. This section provides information about what to do after a snapshot rollback repair.

- Section 11.4.1, "What If a Pair's Secondary Data Location Appears to Be Missing After a Snapshot Rollback Repair?," on page 182
- Section 11.4.2, "What If an Old Pair's Secondary Data Appears After a Snapshot Rollback Repair?," on page 182
- Section 11.4.3, "What If Policies Run or Don't Run as Expected After a Snapshot Rollback Repair?," on page 183
- Section 11.4.4, "What If a Pair Database Error Cannot Be Fixed?," on page 183
- Section 11.4.5, "What If a Policy Database Error Cannot Be Fixed?," on page 184

11.4.1 What If a Pair's Secondary Data Location Appears to Be Missing After a Snapshot Rollback Repair?

When a rollback repair occurs, the pair database file rolls back to the latest known-to-be-good version of the file. The recovered file might not contain pair information for a recently created pair. When users access the share on the primary location, they see only the data on the primary location because the pair definition is no longer available.

To resolve this problem, you can create the pair again as described in Section 8.2, "Creating a Pair," on page 109. This adds the pair configuration information to the recovered pair database file. The merged view begins to work, and users see data on both the primary and secondary locations.

11.4.2 What If an Old Pair's Secondary Data Appears After a Snapshot Rollback Repair?

When a rollback repair occurs, the pair database file rolls back to the latest known-to-be-good version of the file. The recovered file might not contain pair information for a recently unlinked pair. When users access a share on the primary location, they see a merged view that includes the old pair's secondary location.

To resolve this problem, you can delete the pair again as described in Section 8.13, "Unlinking the Paths in a Pair," on page 122. This removes the pair configuration information from the recovered pair database file. Users see data only on the primary location.

11.4.3 What If Policies Run or Don't Run as Expected After a Snapshot Rollback Repair?

When a rollback repair occurs, the policy database file and the related policy files roll back to the latest known-to-be-good version of the files. The recovered files might not contain recent changes that were made to the policies. As a result, policies might run or not run as expected.

After a rollback repair occurs, you should review the recovered policies in the Management Console to verify that the recovered policies reflect any recent changes, such as the following:

- New policy
- Deleted policy
- Added or removed pair-to-policy association
- Modified schedule
- Modified filter options
- Modified direction

To resolve this problem, you can make the changes again.

11.4.4 What If a Pair Database Error Cannot Be Fixed?

If the fatal errors in the pair database file cannot be repaired because no snapshot files are available, you can try to clean up the database file, then re-create the pair. However, if the pairs database file is totally corrupted, you must delete the …\Dynamic File Services\Pairs\DswPairDatabase.xml file and re-create all pairs.

To clean up the pairs database file and re-create selected pairs:

1 Identify where the pair errors occurred:

    1a Open the …\Dynamic File Services\DswRepair.log in a text editor.

    1b From the log, note the GUID and name of each pair where fatal errors occurred.

    1c Close the file.

2 Clean up the pair database file:

    2a Open the …\Dynamic File Services\Pairs\DswPairDatabase.xml file in an XML editor.

    2b For each pair that has corrupted information, remove the pair's information from the file.

       A pair's information begins with the <DswPairEntry> XML tag and ends with the </DswPairEntry> XML tag. Remove the tags and the information about the pair in between them.

    2c Save the edited file.

3 In the Pairs folder, delete the pair history subfolders that correspond to the pairs you deleted from the database.

    You need the pair's GUID to recognize which subfolder belongs to a pair.

4 Re-create the pair as described in .

11.4.5 What If a Policy Database Error Cannot Be Fixed?

If the fatal errors in the policy database files cannot be repaired because no snapshot files are available, you can clean up the policy database and individual policy files, then re-create the policies. However, if the files are totally corrupted, you must delete the …\`Dynamic File Services\Pairs\DswPolicyDatabase.xml` file, delete the individual policy XML files, and re-create all policies.

To clean up the policies database files and re-create selected policies:

1 Identify where the policy errors occurred:

   1a Open the …\`Dynamic File Services\DswRepair.log` in a text editor.

   1b From the log, note the GUID and name of each policy where fatal errors occurred.

   1c Close the file.

2 Clean up the policy database files:

   2a Open the …\`Dynamic File Services\Pairs\DswPolicyDatabase.xml` file in an XML editor.

   2b For each policy that has corrupted information, remove the policy's information from the file.

      The database file contains a GUID and name for each policy on the server.

   2c Save the edited file.

3 In the `Policy` folder, delete the individual policy configuration files that correspond to the policies you deleted from the database.

   You need the policy's GUID to recognize which policy configuration file belongs to a policy.

4 Use either of the following methods to re-create the policy:

   ❖ Re-create the policy as described in Section 9.2, "Creating a Policy," on page 130.

   ❖ If you previously exported a policy, you can import the policy to add it back in the database.

FAQs and Troubleshooting

<div style="text-align: right; font-size: 2em;">12</div>

This section answers frequently asked questions about Novell Dynamic File Services (DynamicFS). It also describes workarounds for any known issues.

- Section 12.1, "Why can't I log in to the Dynamic File Services Server?," on page 185
- Section 12.2, "Can I cancel a policy that is running?," on page 185
- Section 12.3, "How do I configure a policy to not run without disassociating it from the pair?," on page 186
- Section 12.4, "How do I see what policies are running or what files have been moved?," on page 186
- Section 12.5, "What can I do if the Service is not running?," on page 186
- Section 12.6, "Why can't users see the data on a remote share?," on page 186
- Section 12.7, "Path Too Long Exception Error in the Standard Policy Log," on page 187
- Section 12.8, "Pair Is Busy Error for Pair with Remote Share as Secondary," on page 187
- Section 12.9, "Invalid File Handle Error for a Policy Run," on page 187
- Section 12.10, "How do I find event ID information?," on page 187

12.1 Why can't I log in to the Dynamic File Services Server?

If you are having trouble logging in to the Dynamic File Services server from the Management Console, check the following configuration settings that are required for login:

- **Dynamic File Services Group:** The Administrator user account and users that have been added as members of the `Dynamic File Services` group are the only authorized administrators for pairs and policies on the target server. See Section 6.2.3, "Setting Up Administrators in a Workgroup," on page 72.

- **Service Port:** The port number (default 8999) must match the configured port on the target server. See Section 6.6, "Configuring the Service Port," on page 81.

- **Windows Firewall Access:** For remote sessions, the *Windows Firewall Access* option must be enabled on the target server to allow an exception in the Windows Firewall for the configured Dynamic File Service port. See Section 6.7, "Configuring Firewall Access for the Service Port," on page 82.

- **SSL Certificate:** For remote sessions, you must accept the valid DynamicFS certificate for the target server in order to set up a secure SSL connection between the client and the target server. See Section 7.2, "Accepting a Dynamic File Services Certificate," on page 98.

  The DynamicFS certificate on the target server must be a valid certificate. See Section 6.8, "Configuring a Certificate for Secure Remote Management Sessions," on page 85.

12.2 Can I cancel a policy that is running?

You can stop a running policy by selecting the pair in the Management Console, then selecting *Actions > Stop running process*. This stops all policies currently running on the pair.

To ensure that a policy does not run at its next scheduled time, go to the policy's Properties dialog box and unschedule it. For information, see Section 9.7.3, "Unscheduling a Policy for All Pairs," on page 142.

To stop the policy from running for a given pair, you can disassociate the policy from the pair. For information, see Section 9.5, "Associating or Disassociating Pairs and Policies," on page 135.

12.3 How do I configure a policy to not run without disassociating it from the pair?

You can modify the policy's schedule to change the schedule for all pairs without disassociating the policy from the pairs. For information, see Section 9.7.3, "Unscheduling a Policy for All Pairs," on page 142.

12.4 How do I see what policies are running or what files have been moved?

In the Management Console, double-click the Dynamic File Services pair to open the Statistics dialog box to see information about what policies are running, the policy execution history, and what files were moved or not moved by each run. For information, see Section 10.2, "Viewing the Policy Execution History for a Pair," on page 158.

12.5 What can I do if the Service is not running?

The Dynamic File Service must be running before you can connect to and manage the server with the Management Console and the DswCLI.exe command. The Service starts automatically after the install and on reboot, except when the server starts in Windows Safe Mode. You can verify that the Service is running by using the Service Controller icon in the notification area or by looking for the DswService.exe process in the Windows Task Manager or the Windows Computer Management tool.

To start the Service, see Section 6.3, "Starting and Stopping the Service," on page 72.

12.6 Why can't users see the data on a remote share?

If you are using a remote share as a secondary location in a pair and users cannot see the data on the secondary location, it might be because you have not properly set up the remote share.

To troubleshoot the problem, verify the following settings:

- The correct UNC path for the remote share is published in Active Directory.
- The Dynamic File Services Storage Rights group has all share permissions on the remote share.
- The Dynamic File Services Storage Rights group has all NTFS file system rights to the remote share location.
- The Service is running as the NDFS-*servername* proxy user that was created during the install, and this user is a member of the Dynamic File Services Storage Rights group.

- The Dynamic File Services Storage Rights group is a member of the Domain Admins group.
- As a Domain Admins user, you can access the UNC path to the secondary location from the DynamicFS server.

12.7 Path Too Long Exception Error in the Standard Policy Log

The Standard Policy engine gives a `PathTooLongException` error if a specified path, filename, or both are too long. It cannot move the file during a policy run if this error occurs. For information, see Section 4.14, "Filename Path Length," on page 47.

12.8 Pair Is Busy Error for Pair with Remote Share as Secondary

If a pair uses a remote share as the secondary path, you might get a message that the pair is busy if the `DFSStorageRights` group has not been added as a user and granted all permissions for the remote share. For information, see Section 4.10, "Remote Shares as Secondary Paths in an Active Directory Domain," on page 43.

12.9 Invalid File Handle Error for a Policy Run

An Invalid File Handle error is reported for a policy run if the connection to either of the storage locations is lost when a file move is in progress. The move is incomplete. Two instances of the file appear in both locations, but only the file instance in the original location is valid. You must delete the invalid instance of the file.

To resolve this duplicate file situation, you can review the *Statistics > Policy execution history > Files not moved* report for the policy run to identify the duplicate file and the target location of the policy run. You can also run the Sync Pair (`dswsyncpair.exe`) utility to find the duplicate file. Your knowledge of the policy direction setting for the policy run where the duplicate file was created will help you know which instance of the file is valid.

For information about how this occurs, see Section 4.17.3, "Losing a Media Connection when Moving Files," on page 49. For information about reporting and resolving duplicate files, see Section 8.12, "Reporting Conflicts for Duplicate Files," on page 121.

12.10 How do I find event ID information?

Dynamic File Services provides event identification codes (event IDs) to help the administrator understand the event that occurred. For error events, you can use event IDs to help identify possible sources and actions for resolution or workaround.

- Section 12.10.1, "Where are event IDs reported?," on page 188
- Section 12.10.2, "Reporting Error Events to Novell," on page 188
- Section 12.10.3, "Event IDs Categories and Sources," on page 188

12.10.1 Where are event IDs reported?

Event IDs are currently reported for events for Dynamic File Services that are logged in the Microsoft Event Viewer. When an error event is reported, it usually indicates that a software or hardware error has occurred that does not allow a component of Dynamic File Services to continue processing.

12.10.2 Reporting Error Events to Novell

To improve the information that Novell has about resolving error events, we need to know when and how users are seeing them occur. Please help us gather this information by doing the following:

1 Record the event ID number.

2 Record the circumstances in which the error event occurred.

3 If you were able to resolve the error event on your own, record what you did to resolve the problem, and share the information with us.

Get It Documented

You can post your resolution by using the User Comments feature at the bottom of this online page, or go to `www.novell.com/documentation/feedback.html` and enter your comments there.

Report the Bug

If the event is one that needs to be fixed in the product, can also report the problem and your resolution in Novell Bugzilla (https://bugzilla.novell.com).

Before filing a bug, use the *Search* option to see if the problem has already been reported.

To create a new bug, select *New*, select *Novell Products* from the *Classification (Product Line)* drop-down list, select *Dynamic Storage Technology* from the *Product* drop-down list, click *Use This Product*, then complete the report form and submit it.

4 Search the Novell Support Knowledgebase (http://www.novell.com/support/) for more information about the error.

You can also find answers to your problem in the Novell Product Support Forum for Novell Dynamic File Services (http://forums.novell.com/novell-product-support-forums/dynamic-file-services/). The forums provide free peer-to-peer and volunteer technical support for Novell Products.

5 If you are unable to resolve the problem and need technical support, please contact a Novell Support Provider (http://support.novell.com/support_options.html).

12.10.3 Event IDs Categories and Sources

Event ID Category	Event Source
100	DswApi
200	DswBuiltIn
300	DswCertificateLib
400	DswCLI

Event ID Category	Event Source
500	DswStandardPolicy
600	DswIoctlsLib
700	DswIpcClient
800	DswIpcCore
900	DswIpcListener
1000	DswLib
1100	DswMcpCore
1200	DswMcpDatabase
1300	DswMcpService
1400	DswMcpServiceController
1500	DswRepair
1600	DswSyncPair
1700	DswCert
1800	DswDump
1900	DswUpgrade
3000	DswInventory

Security Considerations

13

This section describes security issues and recommendations for Novell Dynamic File Services (DynamicFS). It is intended for security administrators or anyone who is responsible for the security of the system. It requires a basic understanding of DynamicFS. It also requires the organizational authorization and the administrative rights to carry out the configuration recommendations.

- Section 13.1, "Security Features," on page 191
- Section 13.2, "Registry Settings," on page 196
- Section 13.3, "Service Configuration File," on page 196
- Section 13.4, "Server Management Configuration File," on page 196
- Section 13.5, "Pair and Policy Database Configuration Files," on page 196
- Section 13.6, "Log Files and Logging Control Files," on page 197

13.1 Security Features

There are a number of security measures available in Dynamic File Services, such as user access via the primary path and enforcement of user access there.

- Section 13.1.1, "Authentication," on page 191
- Section 13.1.2, "User Access to Pairs," on page 192
- Section 13.1.3, "SSL Certificate," on page 193
- Section 13.1.4, "Service Port," on page 194
- Section 13.1.5, "Windows Firewall Access," on page 194
- Section 13.1.6, "Dynamic File Services Group," on page 194
- Section 13.1.7, "Windows User Account Control," on page 195
- Section 13.1.8, "Network Connections," on page 195
- Section 13.1.9, "Network Shares," on page 195
- Section 13.1.10, "Remote Shares," on page 195
- Section 13.1.11, "Auditing Management Events," on page 195
- Section 13.1.12, "Event Logging," on page 196

13.1.1 Authentication

Consider the authentication requirements in this section for setting up and managing Novell Dynamic File Services.

- "Installing Dynamic File Services in an Active Directory Environment" on page 192
- "Configuring and Managing the Service" on page 192
- "Creating Pairs and Policies" on page 192
- "Using Remote Shares in a Pair" on page 192
- "Using the Repair Tool GUI and Synchronize Pair Utility" on page 192

Installing Dynamic File Services in an Active Directory Environment

In Active Directory domains, the installation must be done by a domain user that has local Administrator privileges and Active Directory Administrator rights. This allows the setup of the Dynamic File Services Storage Rights domain group and the `NDFS-servername` domain user. For information, see Section 4.2, "Active Directory Domain Configuration for Dynamic File Services," on page 38.

The domain user is automatically removed if you uninstall the Service component. The domain group is also removed if the domain user is the last member of the group.

Configuring and Managing the Service

In order to modify the configuration settings for the Dynamic File Service or to stop and start the Service, you must be logged in to the server desktop as the Administrator user or as a user with Administrator privileges. It does not matter if the user is a member of the `Dynamic File Services` group.

Creating Pairs and Policies

To connect to a Dynamic File Services server from the Management Console or when issuing pair and policy commands at the command line, you must provide the login credentials (username and password) of a user that is a member of the `Dynamic File Services` group on the target server, or as the Administrator user account of that server. Users with Administrator privileges (not the Administrator user account) must be added to the `Dynamic File Services` group. You can add the Administrator user account as a member of the group.

The DynamicFS administrator user identity can be validated in Workgroup and Active Directory Domain environments.

Using Remote Shares in a Pair

In an Active Directory environment, Dynamic File Services supports the use of remote shares as the secondary location in a pair. The remote share must be published in Active Directory. In addition, you must allow the default setup of the Dynamic File Services Storage Rights domain group and the `NDFS-servername` domain user, or manually set up an equivalent secure domain configuration. For information, see Section 4.2, "Active Directory Domain Configuration for Dynamic File Services," on page 38.

Using the Repair Tool GUI and Synchronize Pair Utility

The Repair Tool GUI and Synchronize Pair utility require that you be logged in as the Administrator user or as a user with Administrator privileges. If remote shares are used in pairs, the administrator user must also have access rights on the remote share and file system permissions on the secondary storage location. Otherwise, the secondary location is reported as missing. One way to do this is to add the administrator user as a member of the Dynamic File Services Storage Rights (`DFSStorageRights`) group.

13.1.2 User Access to Pairs

To see the merged view of the two storage locations, users access the Dynamic File Services pair through a Windows network share that you set up on the primary location.

Users should not access data stored in the pair via the secondary location, so you must not allow users to access the secondary location directly or via a network share. Network shares on, above, or below the secondary path should be removed, or they must be restricted from access by users.

In a Windows cluster, use cluster-managed network shares instead of server-based network shares.

13.1.3 SSL Certificate

The Dynamic File Services remote connection feature supports server-side SSL certificates. You can use a self-signed certificate (the default) or a signed certificate from a certification authority.

Self-Signed Certificates

By default, remote communications between the Management Console running on a client and the Dynamic File Service running on a server are secured by using the SSL protocol. During the installation, DynamicFS creates and configures a self-signed certificate (`servername-DynamicFileServicesSSLCertificate`) for SSL communications to use. The DynamicFS SSL connection uses standard RSA SHA1 encryption with a 2048-bit key size. It binds the SSL connection to the configured Dynamic File Service port (default 8999).

You can also generate a new self-signed certificate after the install by using the *Certificate Configuration* option in the Dynamic File Service Controller. For information, see Section 6.8.4, "Creating a Dynamic File Services Self-Signed Certificate," on page 87.

Signed Certificates

Signed SSL certificates that you acquire through a certification authority are also supported. Use this option if your enterprise security policy requires this level of security. You can set up a signed certificate by using the *Certificate Configuration* option in the Dynamic File Service Controller after the install. For information, see Section 6.8.5, "Configuring a Signed Certificate for Dynamic File Services," on page 88.

Self-Signed Certificates in a Cluster

When you install DynamicFS on a cluster node, a self-signed SSL certificate is created for the Dynamic File Service on that node. You do not associate the SSL certificate with the Dynamic File Service cluster resource because each node of the cluster has a different self-signed SSL certificate.

When the Management Console connects to a Dynamic File Service cluster resource for remote management, DynamicFS uses the SSL certificate that is configured on the active node in the cluster. You are prompted to accept the certificate for the active server if it has not been previously accepted.

Accepting Certificates

The first time that an authorized administrator connects to a target DynamicFS server from the Management Console, the user is prompted to accept the DynamicFS SSL certificate for the target server. If the server is in a Windows cluster, the user is prompted the first time that a connection is made to each node in the cluster.

The accepted certificate is added to the user's personal local computer certificates on the management computer.

Each user that manages DynamicFS on a target server is prompted to accept the certificate when connecting for the first time to the server.

13.1.4 Service Port

During the install, Dynamic File Services provides an option to modify the port to use for remote management of the Dynamic File Service. By default, DynamicFS uses port 8999. This port can be modified during or after the install. For information, see Section 6.6, "Configuring the Service Port," on page 81.

13.1.5 Windows Firewall Access

During the install, Dynamic File Services provides an option to enable an exception in the server firewall for the configured Dynamic File Service port (default 8999). The firewall exception is enabled by default. Disabling the firewall exception effectively disables the remote management capability for the Dynamic File Service. You can also enable and disable the firewall exception after the install. For information, see Section 6.7, "Configuring Firewall Access for the Service Port," on page 82.

When the *Windows Firewall Access* option is enabled, DynamicFS automatically configures an exception for the configured Dynamic File Service port (default 8999) in the Windows Firewall. By default, the scope of the exception is set as *Any computer (including on the Internet)*. You can modify this manually by using the Windows Firewall dialog box. Other scope options can be found by going to the *Windows Firewall > Exceptions* page, double-clicking the exception to edit it, then selecting *Change Scope*. The alternative manual settings are *My network (subnet) only* and *Custom list*.

13.1.6 Dynamic File Services Group

During the install, a new administrator user group called `Dynamic File Services` is created on computers where you install Service component. The `Dynamic File Services` group is a local group, not a domain group. Initially, there are no members assigned to the `Dynamic File Services` group. Only the users that you explicitly assign to be members of the `Dynamic File Services` group and the Administrator user account on the machine are allowed to manage DynamicFS. For information, see Section 4.1, "Dynamic File Services Group," on page 38.

When you use Dynamic File Services in a Windows cluster, make sure to assign the same users in the `Dynamic File Services` group on each node so they can log in on whatever node is active.

Logins to the Dynamic File Service are authenticated by using Kerberos in a Windows domain, or by using NTLM (NT LAN Manager) if a Windows domain is not present.

13.1.7 Windows User Account Control

Windows User Account Control is available on some Windows platforms. If it is enabled, Windows User Account Control typically prompts you for permission to run an application when the application starts. If you are prompted for an administrator password or confirmation, specify the username and password of the Administrator user or a user with Administrator privileges.

13.1.8 Network Connections

You can run the Management Console on the same server where you are configuring pairs, or from a different Windows server or workstation. If you use a different computer to manage pairs, you must have an IP-based network connection set up between the two computers.

DynamicFS supports connections for IP addresses that use the IPv4 format. It also supports the use of DNS (Domain Name Service) names.

13.1.9 Network Shares

You must create a single network share on the primary folder of the pair in order to give users a merged view of the data. Users map a drive on their computers to the network share.

For secure access and authentication, users should access the data in the pair only via the network share that is set up on the primary path. If users directly access the primary path or secondary path, potential issues can arise with duplicate files or with access rights and attributes being out of synchronization between primary and secondary folders.

To prevent these issues, make sure to remove network shares for the secondary path. In addition, shares must not be nested above or below the primary path or secondary path.

In an Windows cluster, always use the Windows cluster management tool and not Windows Explorer to manage file shares to folders on shared drives. Otherwise, changes made by using Windows Explorer are lost when these file shares fail over to other nodes in the cluster. Workstations should be in an Active Directory domain to access the cluster-managed file shares.

13.1.10 Remote Shares

You must publish a remote share in Active Directory in order to use it as the secondary location in a pair. For requirements, see . For setup information, see .

13.1.11 Auditing Management Events

Auditing of the management of the Dynamic File Service, pairs, and policies is integrated with DynamicFS and is provided as a basic benefit. The following audit logs are by default located in the `\audit` folder in the `C:\Program Files\Dynamic File Services` folder, or in the folder where you installed DynamicFS:

File	Description
DswAuditLog.xml	Logs the management events for the Dynamic File Service, pairs, and policies

File	Description
DswAuditCfg.xml	Controls the logging behavior for the audit log

All Dynamic File Services management actions are audited, including authorized and non-authorized management actions. All authentication and authorization events for DynamicFS are also audited. No sensitive information is placed in the audit log.

13.1.12 Event Logging

DynamicFS uses the Microsoft Event Viewer for logging the Dynamic File Service start/stop events and fatal errors such as application exceptions. See the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/ee624055(WS.10).aspx) for documentation on viewing events with the Event Viewer snap-in for the Microsoft Management Console (MMC).

13.2 Registry Settings

The Dynamic File Services configuration settings are stored in the Windows registry in the following location:

HKEY_LOCAL_MACHINE\Software\Novell\Dynamic File Services

13.3 Service Configuration File

By default, Dynamic File Services stores configuration information about the Dynamic File Service in the following .xml file:

C:\Program Files\Dynamic File Services\DswCore.xml

13.4 Server Management Configuration File

By default, Dynamic File Services stores configuration information about the servers set up in the Management Console in the following .xml file:

C:\Program Files\Dynamic File Services\DswServers.xml

13.5 Pair and Policy Database Configuration Files

By default, Dynamic File Services stores information about pairs and policies in the following .xml files:

C:\Program Files\Dynamic File Services\Pairs\DswPairDatabase.xml

C:\Program Files\Dynamic File Services\Policies\DswPolicyDatabase.xml

The schedule for taking snapshots of the pair and policy database files is stored in the C:\Program Files\Dynamic File Services\DswCore.xml file.

13.6 Log Files and Logging Control Files

Dynamic File Services provides log files for monitoring the software, management, and policy enforcement events. The default location of log files is the `C:\Program Files\Dynamic File Services` folder.

Component	Log File	Logging Control File
Standard Policy	`DswStandardPolicy.log`	`DswStandardPolicy.config.xml`
File System Inventory	`DswInventory.log`	`DswInventory.config.xml`
Service	`DswMcpCore.log`	`DswMcpCore.config.xml`
Synchronize Pair	`DswSyncPair.log`	`DswSyncPair.config.xml`

DynamicFS uses Apache log4net open source software to provide some of the logging Services. It is installed automatically with DynamicFS.

DynamicFS automatically configures the recommended logging settings for each of the logging control files with the information contained in the `<log4net></log4net>` XML tags within each file. The default logging level is the WARN level.

IMPORTANT: If you modify the log4net settings in a logging control file, do not modify information that is outside of the `<log4net></log4net>` XML tags.

The log4net software supports the following logging levels in order of increasing priority:

ALL
DEBUG
INFO
WARN (default setting for the Dynamic File Services logs)
ERROR
FATAL
OFF

For information about log4net software and the logging levels, see the *Apache Logging Services: log4net Manual* (http://logging.apache.org/log4net/release/manual/configuration.html).

Using iSCSI Targets in a Cloud Storage Environment

A

You can use a cloud-based iSCSI target device as the secondary location for Novell Dynamic File Services pairs. Novell supports multiple cloud storage and IaaS (Infrastructure as a Service) solution providers.

IMPORTANT: Refer to the third-party vendor documentation for detailed information about how to subscribe to and use cloud-based computing and storage resources.

This section provides one example of how to set up a Linux iSCSI Target server and storage devices in the cloud. The iSCSI target devices are connected to a Windows Server 2008 server running iSCSI Initiator software in your local network. After you attach the iSCSI devices to your local server, you can use them as the secondary storage location in a Dynamic File Services pair.

The example iSCSI target solution is based on the following components:

- Amazon Elastic Compute Cloud (Amazon EC2) environment, including the following:
  - a Linux virtual machine instance (http://aws.amazon.com/ec2/#instance)
  - an Elastic Block Store volume (http://aws.amazon.com/ebs/)
  - an Elastic IP address (http://aws.amazon.com/ec2/#features)
- openSUSE 11 SP2 Linux server operating system on the virtual machine
- Linux iSCSI Target software installed on the virtual machine
- Microsoft iSCSI Software Initiator Version 2.08 installed on your Windows Server 2008 computer
- Microsoft `iSCSICLI` command line tool

Use the following procedures to set up the cloud-based Linux iSCSI Target server and target devices:

- Section A.13, "Creating a Dynamic File Services Pair with the Cloud-Based iSCSI Device," on page 211
- Section A.14, "Additional Information," on page 211

A.1 Guidelines for Using iSCSI Targets in the Cloud

Consider the following guidelines for your cloud-based iSCSI target solution:

- Section A.1.1, "Secure Connections in the Cloud," on page 200
- Section A.1.2, "Secure Access to iSCSI Target Devices," on page 200
- Section A.1.3, "Backup in the Cloud," on page 200
- Section A.1.4, "Costs for Cloud Services," on page 200

A.1.1 Secure Connections in the Cloud

In this example, access to files occurs across the public Internet. A production environment typically requires a more secure cloud solution. Other IaaS cloud environments provide secure solutions.

For example, the Amazon Virtual Private Cloud (Amazon VPC) extends your own network segment into the cloud across a VPN (virtual private network) connection. This allows you to use your own IP address ranges and keeps all communications secure in a VPN tunnel as files travel across the public Internet.

In a production environment, you should use IPSec for connections (or use a secure solution like the Amazon VPC) to make sure that your data cannot be snooped on the wire.

A.1.2 Secure Access to iSCSI Target Devices

In this example, authentication is not configured for the iSCSI target device. In a production environment, you should configure and require authentication for each iSCSI target device so no one else can attach to your iSCSI target.

A.1.3 Backup in the Cloud

The Amazon EBS solution provides a snapshot option that you can enable to create snapshots in the cloud for your EBS volume.

You can also create a snapshot of your configured VM instance. It is easier to restore the VM from a snapshot than to re-create it.

A.1.4 Costs for Cloud Services

Refer to the pricing information on the Amazon EC2 Web site (http://aws.amazon.com/ec2/#pricing) to determine your potential costs for the cloud-based openSUSE Linux VM, EBS volumes, and the related traffic.

A.2 Don't Have an Existing Amazon EC2 Account?

If you do not have an Amazon EC2 account, you need to sign up for one. You must provide credit card information, provide a phone number where you can enter a confirmation pin number, and sign up for an Amazon Web Services (AWS) account. You must also create an X.509 certificate. AWS uses the private certificate and key to verify and authenticate your identity as you manage your cloud resources.

1 In a Web browser, go to the Amazon EC2 Web Services page (http://aws.amazon.com/ec2/), then select *Sign up for an Amazon EC2*.

2 Provide your identity information.

3 Provide your credit card information.

4 Provide your phone contact information.

5 When you receive an automated phone call that asks you for a confirmation pin number, enter the number that appears on the computer screen.

6 Follow the on-screen instructions to sign up for an Amazon Web Services account.

When the sign-up is complete, you receive the following message on the screen, and you receive an e-mail stating that you have signed up for the Service.

```
Thank you for signing up for Amazon EC2.

We will e-mail you a confirmation when the web services are available for
you to use. In order to begin using this service, you will need a X.509
certificate. You can Create a New X.509 Certificate or Upload Your X.509
Certificate on the Security Credentials page.
```

7 On the Thank You page, select *Create a New X.509 Certificate*, then click *Yes* to create the new certificate and key files.

You can access this page later by opening the Amazon EC2 Web Services page (http://aws.amazon.com/ec2/) in a Web browser, logging in to your account, then selecting *Account > Security Credentials > Access Credentials > X.509 Certificates > Create a New X.509 Certificate*.

8 On the Certificate page, save the `certxxxxxxx.pem` and `pk-xxxxxxxxxxxx.pem` files to a secure location on your local computer.

9 Continue with Section A.3, "Already Have an Existing Amazon EC2 Account?," on page 201

A.3 Already Have an Existing Amazon EC2 Account?

1 In a Web browser, go to the Amazon Web Services console (https://console.aws.amazon.com/ec2/home), then log in with your AWS identity and credentials.

2 Create a key pair:

   2a In the left pane under *Networking and Security*, click *Key Pairs*.

   2b Click *Create a Key Pair*.

   2c Type a name for the key (such as `xxxkey`), then click *Create*.

2d Save the `xxxkey.pem` file to a secure location on your local computer.

This key is used later to connect via SSH (Secure Shell) to the Linux iSCSI Target virtual machine.

3 Continue with Section A.4, "Launching an openSUSE Linux VM Instance," on page 202.

A.4 Launching an openSUSE Linux VM Instance

1 Continuing in the Amazon Web Services console, in the left pane under *Instances*, click *Instances*.

2 Click *Launch Instance* to start the Request Instances Wizard.

3 Under *Community AMIs*, search all images for openSUSE AMIs. (Select *All Images*, type SUSE in the *Search* field, then press Enter.)

4 Click *Select* next to an AMI for the openSUSE 11 SP2 Linux virtual machine that you want to use.

For example, we selected AMI 37b9555e, which created the following instance:

```
ID= "ami-37b9555e" Manifest= elihullc/ami/openSuSE-11.2-ec2-server.i386-
1.0.0.ami.manifest
```

5 In *Number of Instances*, select 1.

6 Specify the *Availability Zone*. For example, select *us-east-1b*.

IMPORTANT: Make sure to choose the same availability zone later for the volume you create for the iSCSI NTFS file system.

7 Select the *Instance Type*. For example, select *Small(m1.small,1.7GB)*.

8 Select *Launch Instances*, then click *Continue*.

9 Specify the following settings for the openSUSE Linux Server VM instance, then click *Continue*:

Instance Settings	Sample Value
Kernel ID	Select *Use Default*.
RAM Disk ID	Select *Use Default*.

10 Select *Choose from your existing key pairs*, choose the key you created (`xxxkey.pem`) from the drop-down menu, then click *Continue*.

11 In *Security Groups*, select *Default* or your preferred setting, then click *Continue*.

12 Click *Launch*.

13 Close the Request Instances Wizard, then wait until the instance of your openSUSE 11 SP2 Linux virtual machine is started and running.

14 Continue with Section A.5, "Setting Up an Elastic IP Address," on page 203.

A.5 Setting Up an Elastic IP Address

An Elastic IP address is a public IP address that allows you to access this virtual machine via the public Internet.

1 Continuing in the Amazon Web Services console, in the left pane under *Networking and Security*, click *Elastic IPs*.

2 Click *Allocate New Address*, then click *Yes, allocate*.

A newly assigned public IP address appears in the list. Keep a record of this IP address.

3 Select the check box next to the new IP address, then click *Associate*.

4 Select the instance ID for the openSUSE Linux VM (the currently running AMI instance), then click *Associate*.

5 Continue with .

A.6 Creating an Elastic Block Store Volume

1 Continuing in the Amazon Web Services console, in the left pane under *Elastic Block Store*, click *Volumes*.

2 Click *Create Volume*, then specify the volume settings:

Volume Setting	Sample Value
Size	Specify 100 GiB (gibibyte, the IEC standard unit).
Availability Zone	From the drop-down menu, select *us-east-1b*. **IMPORTANT:** Use the same same value that you specified for the virtual machine.
Snapshot	Select *No Snapshot*.

3 Click *Create*, then wait for the volume to be created.

This might take several minutes. The time varies according to the size of the EBS volume. The volume appears in the list with a status of *creating* (yellow icon). Click *Refresh* periodically until the volume status shows a status of *available* (blue icon)

4 Select the check box next to the newly created volume.

5 Click *Attach Volume*.

6 Select the openSUSE Linux VM (the currently running AMI instance).

7 In *Device*, specify the device path.

The default path is /dev/sdf. You can use the default path if it is the first volume you are attaching to the VM. If you add more EBS volumes, specify a different path for each one.

8 Click *Attach*.

The EBS volume is attached to the openSUSE Linux VM (the running AMI instance). The status changes to *in use* (green icon).

9 Continue with .

A.7 Opening Ports for iSCSI Communications

1 Continuing in the Amazon Web Services console, in the left pane under *Networking and Security*, click *Security Groups*, then click *Default*.

2 Scroll to the bottom of the page to view the *Connection Methods* table.

3 From the *Connection Methods* drop-down menu, select *SSH*, specify 22 as the *From Port* and the *To Port*, set the *Source IP* to `0.0.0.0/0`, then click *Save*.

The `0.0.0.0/0` setting for the Source IP leaves the SSH connection open to access from any IP address. To be more secure, set the *Source IP* to the IP address of the Windows server from which you use SSH to access the VM.

4 Create a custom port 3260 for the iSCSI communications.

To be more secure, set the *Source IP* to the IP address of the Windows server that will be accessing the iSCSI targets.

   4a From the *Connection Methods* drop-down menu, select *Custom*, select *TCP*, specify 3260 as the *From Port* and the *To Port*, set the *Source IP* to `0.0.0.0/0`, then click *Save*.

   4b From the *Connection Methods* drop-down menu, select *Custom*, select *UDP*, specify 3260 as the *From Port* and the *To Port*, set the *Source IP* to `0.0.0.0/0`, then click *Save*.

5 Continue with .

A.8 Connecting to the iSCSI Target Virtual Machine via SSH

To manage the newly created virtual machine, connect to the server via SSH from the local computer where you downloaded the xxxkey.pem file. In the initial SSH session, you connect as the root user. Later, you can create other identities on the server for administration purposes and log in to the session with a different username.

A.8.1 Getting the SSH Syntax Information

The syntax to use for your SSH connection is provided by the *Instances* option in the Amazon Web Services console.

1 Continuing in the Amazon Web Services console, in the left pane under *Instances*, click *Instances*, then select the check box next to the openSUSE Linux VM (the currently running AMI instance).

2 From the *Instance Actions* drop-down menu, select *Connect*.

The pop-up dialog box provides the syntax information you need to connect via SSH to your virtual machine.

The general syntax to SSH is:

```
ssh -i xxxkey.pem root@ec2-xxx-xxx-xxx-xxx-xx.xxxxxx-x.amazonaws.com
```

3 Use one of the following methods to connect via SSH to the virtual machine:

A.8.2 Using SSH on Windows

When working with the key file (`xxxkey.pem`) on a Windows machine, you need to convert the key to use a file format that is compatible with the SSH connection method you plan to use.

This section describes how to use PuTTY software for the SSH connection. PuTTY cannot directly open PEM key files. You must convert the key file to PPK format. The setup is a one-time process. After you set up an SSH session in PuTTY, you can easily connect to the VM at any time.

- "Downloading the PuTTY Software" on page 205
- "Converting the PEM Key File to PPK Format" on page 205
- "Setting Up the Key File and Passphrase in the Pageant Authentication Agent" on page 206
- "Configuring an SSH Session in PuTTY" on page 206
- "Connecting via SSH with PuTTY" on page 207

Downloading the PuTTY Software

1 In a Web browser, go to the PuTTY Download page (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).

2 Download the following software to your Windows machine:

Software	Filename	Description
PuTTY	`putty.exe`	A Telnet and SSH client
PuTTYgen	`puttygen.exe`	An RSA and DSA key generation utility
Pageant	`pageant.exe`	An SSH authentication agent for PuTTY

3 Continue with "Converting the PEM Key File to PPK Format" on page 205.

Converting the PEM Key File to PPK Format

1 Launch the PuTTYgen software by double-clicking the `puttygen.exe` file, or by right-clicking the file and selecting *Run as administrator*.

2 In the PuTTY Key Generator window, click *Load*, then select the `xxxkey.pem` file that you downloaded to your local computer in Section A.3, "Already Have an Existing Amazon EC2 Account?," on page 201.

3 After the key information is loaded, specify a key comment and passphrase.

The *Key passphrase* and *Confirm passphrase* fields allow you to choose a passphrase for your key that is used to encrypt the key on the disk. Use a strong passphrase for a more secure solution. Do not forget your passphrase. There is no way to recover it.

You must enter the passphrase when you use the key to connect via SSH to the virtual server. To avoid entering the passphrase each time you start an SSH session, you can set up the key and passphrase in Pageant, as described in "Setting Up the Key File and Passphrase in the Pageant Authentication Agent" on page 206.

4 Save the private key in `.ppk` format.

The converted key is saved as `xxxkey.ppk`. Make sure that you store the `xxxkey.pem` and `xxxkey.ppk` key files in a secure location on your local computer.

5 Continue with "Setting Up the Key File and Passphrase in the Pageant Authentication Agent" on page 206.

Setting Up the Key File and Passphrase in the Pageant Authentication Agent

Pageant is an SSH authentication agent. It holds an authentication key in memory, already decoded, so that you can start SSH sessions often without needing to type a passphrase each time. PuTTY automatically retrieves the decoded key from Pageant when you start your SSH session with the virtual machine. When you stop the Pageant from running, the decoded key is removed from memory.

1 Launch the Pageant software by double-clicking the `pageant.exe` file, or by right-clicking the file and selecting *Run as administrator*.

The Pageant authentication agent starts running and places an icon in the notification area.

2 In the notification area, right-click the *Pageant PuTTY authentication agent* icon, then select *Add Key*.

3 In the Select Private Key File dialog box, browse to locate and select the `xxxkey.ppk` file you created in "Converting the PEM Key File to PPK Format" on page 205, then click *Open*.

4 When you are prompted, specify the passphrase for the `xxxkey.ppk` file.

The key appears in the *Pageant Key List*.

The Pageant authentication agent must be running when you connect to the virtual machine with a PuTTY SSH session in order for Pageant to provide decoded key information.

5 Continue with "Configuring an SSH Session in PuTTY" on page 206.

Configuring an SSH Session in PuTTY

1 Launch the PuTTY software by right-clicking the `putty.exe` file, then selecting *Run as Administrator*.

2 In the left pane, select *Session*.

3 In *Host Name (or IP address)*, specify the Elastic IP address that you set up for the virtual machine.

You can alternately use the public DNS name of the virtual machine. You can find the DNS name by looking at the virtual machine instance in the Amazon AWS Management Console.

4 In *Protocol*, select *SSH*.

5 Set up the authentication settings:

5a In the left pane, select *Connection > SSH*.

5b In the left pane, select *Connection > SSH > Auth*.

5c Under *Authentication methods*, select *Attempt authentication using Pageant*. This is selected by default.

5d In *Private key file for authentication*, browse to locate and select the `xxxkey.ppk` file you converted in "Converting the PEM Key File to PPK Format" on page 205, then click *Open*.

6 In the left pane, select *Session*.

7 Under *Saved Sessions*, specify a name for this connection (such as `iSCSI_Target_VM`), then click *Save*.

The name appears in the list under *Saved Sessions*.

8 Close PuTTY.

The PuTTY SSH session setup is complete. You can use PuTTY to connect to the virtual machine with your saved SSH session at any time.

9 Continue with "Connecting via SSH with PuTTY" on page 207.

Connecting via SSH with PuTTY

After you have set up the SSH session in PuTTY, you can use PuTTY to run the authenticated SSH session at any time.

1 Launch the PuTTY software by double-clicking the `putty.exe` file, or by right-clicking the file, then selecting *Run as Administrator*.

2 In the PuTTY window, double-click the saved SSH session for the virtual machine, or select the session and click *Open*.

If you are not running Pageant, you are prompted for the passphrase for the authentication key. Provide the passphrase to continue.

A Login dialog box pops up for your OpenSSH session.

3 When you are prompted, log in as the `root` user.

After you are successfully connected, you are presented with a terminal console prompt for the virtual machine.

4 Continue with Section A.9, "Installing the iSCSI Target Software on the openSUSE Linux VM," on page 208.

A.8.3 Using SSH on Linux

1 On the local machine, open a terminal console, then log in as the `root` user.

2 Go to the folder where you saved the `xxxkey.pem` file. At the terminal console prompt, enter

`cd /path_to_key_file_folder`

3 Connect via SSH to the virtual machine.

The general syntax to SSH is:

`ssh -i xxxkey.pem root@ec2-xxx-xxx-xxx-xxx-xx.xxxxxx-x.amazonaws.com`

4 Click *Yes* to connect to the virtual machine.

5 Keep the console open and do not terminate the SSH session.

6 Continue with Section A.9, "Installing the iSCSI Target Software on the openSUSE Linux VM," on page 208.

A.9 Installing the iSCSI Target Software on the openSUSE Linux VM

Use YaST 2 to install the iSCSI Target software. This step is done only once to set up the software on the VM.

1 Continuing in your SSH session with the virtual machine, launch YaST 2 by entering

```
yast2
```

The AMI image instance has no GUI installed by default.

2 Go to *Software Management*.

3 If you are prompted with the *Update License* message, select *Import* to accept and import the GNUI Key.

4 Wait until the Package Manager is loaded.

It takes a few minutes to load the Package Manager and to download the package list.

5 In the Package Manager, search for the iSCSI packages. (In the *Search* field, type `iscsi`, then press Enter.)

6 From the list of iSCSI packages, select the following iSCSI Target software packages:

```
iscsitarget
yast2-iscsi-server
```

7 Select *Accept* (lower right corner), then select *OK* to continue with the install.

Wait until the install is complete.

8 Select *Quit* to exit YaST, which allows the installation of the iSCSI Target management plug-in to YaST 2.

9 Keep the console open and do not terminate the SSH session.

10 Continue with Section A.10, "Configuring the iSCSI Target Device," on page 208.

A.10 Configuring the iSCSI Target Device

1 Continuing in your SSH session with the virtual machine, launch YaST 2 by entering

```
yast2
```

2 In YaST 2, go to *Network Services > iSCSI Target*.

YaST opens to the iSCSI Target Overview page with the *Service* tab selected.

3 Under *Service Start*, select *When booting*.

This option is needed to automatically start the Linux iSCSI Initiator service on subsequent server reboots.

4 Go to the *Global* section by pressing Alt+G.

5 In the *Global* section, leave the target device open for anonymous connections by selecting *No Authentication*.

In a production environment, you can set credentials to make the connection more secure.

6 Go to the *Target* section by pressing Alt+T.

7 In the *Target* section, select *Add* by pressing Alt+A.

An example iSCSI target device (`iqn.2001-04.com.example:storage.disk2.sys1.xyz`) appears in the list. This is not your device. Each device you create will have its own unique IQN (iSCSI qualified name).

8 Press Alt+A to add a new iSCSI target.

9 Specify the *LUN* settings for the iSCSI target device:

   9a Specify the LUN value. The default is 0.

   9b Specify *Type* as *fileio*. This is the default.

   9c Specify the *Path* as `/dev/sdf` (or the path value you specified in the EBS setup).

   9d Select *OK* to continue.

10 Select *Next*, select *OK*, then select *Yes* when you are prompted to restart the iSCSI Target service with the following command:

`rciscsitarget restart`

11 Select *Quit* to exit YaST.

12 Use either of the following methods to view the IQN for the iSCSI device you created:

   ◆ Launch YaST 2, and go to *Network Services > iSCSI Target*.

   ◆ View the device entry in the `/etc/ietd.conf` file by using the `cat` command.

The target device's IQN has a fixed syntax that looks like the following:

`iqn.yyyy-mm.<reversed domain name>:unique_id`

13 (Optional) Modify the IQN by opening the `/etc/ietdf.conf` file in a `vi` text editor to specify a `unique_id` value that satisfies your company naming conventions. The name must be globally unique within your network.

For example:

iqn.2010-04.com.amazonaws.xxxxxx-1.ec2-xxx-xxx-xxx-xxx-xx.:storage.disk2.sys1.xyz

14 Record the IQN of the target device.

You need the IQN later to connect the target device to the Windows server.

15 Exit the SSH session.

16 Continue with Section A.11, "Configuring the iSCSI Initiator Software on a Windows Server," on page 209.

A.11 Configuring the iSCSI Initiator Software on a Windows Server

1 On a Windows Server 2008 server, open a Web browser and go to the Microsoft Downloads Center (http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en), then download and install the Microsoft iSCSI Software Initiator Version 2.08.

2 Launch the iSCSI Initiator.

3 Open a command prompt console with administrator privileges. Select *Start > All Programs > Accessories*, right-click *Command Prompt*, then select *Run as Administrator*.

4 At the command prompt, use the iSCSICLI command to add a target device by entering:

`iscsicli QAddTarget iqn_target_device elastic_ip_address`

Parameter	Description
iqn_target_device	Use the IQN of the iSCSI target device that you set up in Section A.10, "Configuring the iSCSI Target Device," on page 208.
elastic_ip_address	Use the public Elastic IP address that you set up for the openSUSE Linux VM in Section A.5, "Setting Up an Elastic IP Address," on page 203.

You must use the command line method to set up the cloud-based iSCSI target device rather than the iSCSI Initiator GUI. This step is required because of the address translation that occurs between the public Elastic IP address and private IP address on the openSUSE Linux VM behind the Amazon AWS firewall. The *Discovery* option in the iSCSI Initiator GUI finds the Amazon AWS private IP address for the openSUSE Linux VM, and not the public IP address that you set up for it. If the private IP address is associated with the target device, you are unable to connect to the device across the public Internet.

5 Close the command prompt console.

6 In the iSCSI Initiator Properties window, click the *Targets* tab.

7 Select the IQN of the target device, then click *Connect*.

8 Select the check box next to *Add this connection to the Favorites List* to enable the automatic restart.

9 Click *Advanced*.

10 On the *General* tab of the Advanced Settings page, from the *Target portal IP* drop-down list, select the IP address you entered in Step 4, which is the Elastic IP address for the iSCSI Target server in the cloud.

11 Click *OK* to apply the changes.

12 Click *OK* to connect to the target device.

13 Click *OK* again to exit the iSCSI Initiator Properties page.

14 Continue with Section A.12, "Formatting the iSCSI Device as NTFS on the Windows Server," on page 210.

A.12 Formatting the iSCSI Device as NTFS on the Windows Server

1 On the Windows server, launch the iSCSI Initiator software.

2 In the iSCSI Initiator Properties page, click the *Volume and Devices* tab.

3 Click *Auto Configure*.

4 Click *OK* to apply the changes and exit.

5 Go to the Windows Disk Management to view the disk.

6 Select the disk and set it to *Online*.

7 Initialize the disk.

For information, see "Overview of Disk Management" (http://technet.microsoft.com/en-us/library/dd163558.aspx) in the *Microsoft TechNet Library.*

8 Create a volume on the disk and format it as NTFS.

For information, see "Partitions and Volumes" (http://technet.microsoft.com/en-us/library/dd163559.aspx) in the *Microsoft TechNet Library*.

The target device is ready to use on your local server. You can use the disk as if it is a local disk.

9 Continue with Section A.13, "Creating a Dynamic File Services Pair with the Cloud-Based iSCSI Device," on page 211.

A.13 Creating a Dynamic File Services Pair with the Cloud-Based iSCSI Device

You can use the volume for the secondary path in a Dynamic File Services pair. Because of potential latency issues with the public Internet, cloud-based devices should not be used as the primary location in a pair.

1 On a Windows server or workstation, launch the Dynamic File Services Management Console.

2 Connect to the Windows Server 2008 server where you attached the cloud-based iSCSI target device.

For information, see Section 7.3, "Connecting to a Server," on page 99.

3 Select the server, then create a pair as described in Section 8.2, "Creating a Pair," on page 109.

Specify the Primary Path as a location on a device running in the local network (non-cloud-based device). Specify the Secondary Path as a location on the cloud-based iSCSI target device that is attached to the Windows server.

4 Associate the pair with one or more existing policies by using the methods described in Section 9.5, "Associating or Disassociating Pairs and Policies," on page 135.

A.14 Additional Information

- Section A.14.1, "openSUSE 11 SP2 Linux," on page 211
- Section A.14.2, "Linux iSCSI Target Software Documentation," on page 211
- Section A.14.3, "PuTTY," on page 212
- Section A.14.4, "Microsoft iSCSI Software Initiator Version 2.08," on page 212
- Section A.14.5, "IETF RFC 3220: Internet Small Computer Systems Interface," on page 212
- Section A.14.6, "Amazon EC2 Cloud Services Costs," on page 212

A.14.1 openSUSE 11 SP2 Linux

Refer to the openSUSE Linux 11 SP2 documentation (http://www.novell.com/documentation/opensuse112/) for information about how to manage the Linux operating system.

A.14.2 Linux iSCSI Target Software Documentation

For information about using iSCSI Target software on openSUSE Linux, see "Mass Storage over IP Networks: iSCSI" (http://www.novell.com/documentation/sles11/stor_admin/data/cha_inst_system_iscsi.html) in the *SUSE Linux Enterprise Server 11 Storage Administration Guide* (http://www.novell.com/documentation/sles11/stor_admin/data/bookinfo.html).

A.14.3 PuTTY

To download PuTTY products, go to the PuTTY Download page (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).

For information about using PuTTY, see the *PuTTY User Manual* (http://the.earth.li/~sgtatham/putty/0.58/htmldoc/index.html).

A.14.4 Microsoft iSCSI Software Initiator Version 2.08

For information about the Microsoft iSCSI Software Initiator Version 2.08, see the Microsoft Downloads Center (http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en).

For information about using the Microsoft iSCSI Initiator software, see *Microsoft iSCSI Initiator Step-by-Step Guide* (http://technet.microsoft.com/en-us/library/ee338476(WS.10).aspx) in the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/default.aspx).

For information about using the iSCSI command line interface (`iSCSICLI.exe`) for the Microsoft iSCSI Initiator software, open a command prompt console on your Windows desktop, then enter

```
iscsicli.exe help
```

A.14.5 IETF RFC 3220: Internet Small Computer Systems Interface

For information about the iSCSI protocol, see the *IETF RFC 3220: Internet Small Computer Systems Interface* (http://www.ietf.org/rfc/rfc3720.txt).

A.14.6 Amazon EC2 Cloud Services Costs

For current pricing for your cloud-based iSCSI Target server and storage device implementation, refer to the Amazon EC2 Web site (http://aws.amazon.com/ec2/#pricing).

Setting Up a Merged View for Collaboration Applications: Novell Teaming

B

Novell Dynamic File Services 1.6 can also be used with applications that store unstructured files to the file system. One example application environment is Novell Teaming. This section describes how to set up Dynamic File Services pairs and policies for Novell Teaming so that users see the merged view of files stored in an application environment.

Steps and requirements to use the merged view with Novell Dynamic File Services are:

- Section B.1, "Verify That the Application can support using a Microsoft network share to store files.," on page 213
- Section B.2, "Understand how the application stores, names, and versions files so useful policies can be created," on page 213
- Section B.3, "Create a Microsoft Share for the Application to use," on page 214
- Section B.4, "Configure the application to use the Microsoft Networking Share," on page 214
- Section B.5, "Install Dynamic File Services on the Windows Server where the Share will be for the primary path," on page 214
- Section B.6, "Create a Pair," on page 215
- Section B.7, "Create a Policy," on page 215

B.1 Verify That the Application can support using a Microsoft network share to store files.

Novell Teaming supports Microsoft network shares on the same Windows Sever that the product is installed on. To enable the application to use a share, you must edit the `ssf-ext.properties` file.

B.2 Understand how the application stores, names, and versions files so useful policies can be created

The more you understand about how an application stores files, the more opportunities you can create for integrating the application with Dynamic File Services.

This example focuses on one way that Novell Teaming stores photos. When you upload a photo to Teaming, it creates a thumbnail file for the photo in the `cachefilestore` subfolder structure and places the photo image in the `filerepository` subfolder structure. Because photos can be large, we want to set up a pair and policy so that photos are moved to a secondary storage location.

1 Create a pair where the primary path is on the `filerepository` folder.

B.3 Create a Microsoft Share for the Application to use

By default, Novell Teaming creates a folder called `C:\Novell\Teaming` to store files. This is where you should create the network share for Teaming to use.

1 Use the Microsoft Network Sharing feature to create a share to be used by Novell Teaming.

For this example, the share is called `NovellTeaming` and the Share path should be on the `C:\Novell` path.

B.4 Configure the application to use the Microsoft Networking Share

1 Stop the Novell Teaming application.

2 Modify the `C:\Program Files\Novell\Teaming\apache-tomcat-6.0.18\webapps\ssf\WEB-INF\classes\config\ssf-ext.properties` file as follows:

```
##data.root.dir=C:/Novell/Teaming
##data.simplefilerepository.root.dir=C:/Novell/Teaming
##data.simplefilerepository.root.dir=C:/Novell/Teaming
##data.jackrabbitrepository.root.dir=C:/Novell/Teaming
##data.extension.root.dir=C:/Novell/Teaming
##data.archivestore.root.dir=C:/Novell/Teaming
##data.luceneindex.root.dir=C:/Novell/Teaming
##cache.file.store.dir=C:/Novell/Teaming/cachefilestore
##temp.dir=C:/Novell/Teaming/temp
##filtering.failed.dir=C:/Novell/Teaming/filteringfailed
##fi.work.dir=C:/Novell/Teaming/fi/work

data.root.dir=//<ServerIP>/NovellTeaming/teaming
data.simplefilerepository.root.dir=//<ServerIP>/NovellTeaming/teaming
data.jackrabbitrepository.root.dir=//<ServerIP>/NovellTeaming/teaming
data.extension.root.dir=//<ServerIP>/NovellTeaming/teaming
data.archivestore.root.dir=//<ServerIP>/NovellTeaming/teaming
data.luceneindex.root.dir=//<ServerIP>/NovellTeaming/teaming
cache.file.store.dir=//<ServerIP>/NovellTeaming/teaming/cachefilestore
temp.dir=//<ServerIP>/NovellTeaming/teaming/temp
filtering.failed.dir=//<ServerIP>/NovellTeaming/teaming/filteringfailed
fi.work.dir=//<ServerIP>/NovellTeaming/teaming/fi/work
```

3 Restart the Novell Teaming application.

B.5 Install Dynamic File Services on the Windows Server where the Share will be for the primary path

1 Install Dynamic File Services on the Windows Server that is running Teaming where you have created the share.

B.6 Create a Pair

1 Create another Microsoft Network Share at `C:\Novell\Teaming\filerepository` and call it `filerepository`.

2 Add Novell Dynamic File Services pair with `C:\Novell\Teaming\filerepository` as the primary path and set the secondary path where desired.

B.7 Create a Policy

1 Create a policy to move all JPG files.

2 After the policy is executed, the JPG files are moved to the secondary path.

Now when the Teaming Application using the `NovellTeaming` share and reads files from `filerepository`, the Teaming application gets a merged view and has no idea that the files at two different storage locations.

Management Tools Quick Reference

C

This section provides a quick reference of where to find the various features for the Novell Dynamic File Services (DynamicFS) tools, including the Management Console, Service Controller, Repair Tool GUI, and Uninstall Wizard.

- Section C.1, "Server Properties," on page 217
- Section C.2, "Pair Properties," on page 218
- Section C.3, "Policy Properties," on page 219
- Section C.4, "Pair Statistics," on page 220
- Section C.5, "Server Wizard," on page 222
- Section C.6, "Setup Wizard," on page 222
- Section C.7, "Pair Wizard," on page 224
- Section C.8, "Policy Wizard," on page 224
- Section C.9, "Toolbar Menus," on page 226
- Section C.10, "Right-Click Menus," on page 227
- Section C.11, "Service Controller," on page 228
- Section C.12, "Repair Tool," on page 229
- Section C.13, "Uninstall Wizard," on page 229

C.1 Server Properties

- General
    - System
        - Operating system
        - Server time zone
    - Computer
        - Processor
        - RAM
    - Domain
    - Version
- Disk details
    - Disks on the computer that are seen as native drives
    - Capacity (GB)
    - Free space (GB)
    - Free space (%)
    - Type

- File system
- Used space
- Free space
- Graphical display of capacity
- History
  - Graphical display of the disk capacity over time
  - Roll over observed values to see the date and value information
  - Right-click to save or print the graphical display
- Log files
  - DswMcpCore.log
  - DswStandardPolicy.log
  - install.log
- Logging options
  - DswMcpCore.config.xml
    - Log level
  - DswStandardPolicy.config.xml
    - Log level

C.2 Pair Properties

- General
  - Primary
    - Type
    - Primary path
    - Share name(s)
  - Secondary
    - Type
    - Secondary path
- Associations
  - View associated policies for the pair.
  - Add policy associations for the pair.
  - Remove policy associations for the pair.
- Include/Exclude
  - Restriction options: None, Exclude, or None.
  - Add/Remove directories to be included or to be excluded.
- Pair history
  - Schedule when to run the pair history scan.
    - Frequency (Hourly, Daily (default), Weekly)
    - At (time of day)

C.3 Policy Properties

- General
    - Policy name
    - Direction
        - Primary to secondary
        - Secondary to primary
    - Frequency
        - Scheduled/Not Scheduled
        - Frequency and run time
            - Hourly
            - Daily
                - Start
                - Duration
            - Weekly
                - Day
                - Start
                - Duration
            - Monthly
                - Day
                - Start
                - Duration
            - Yearly
                - Month
                - Day
                - Start
                - Duration
        - Schedule description
    - Filter options
        - File size
            - Greater than (>) or Less than (<)
            - Value
            - Bytes, Kilobytes, Megabytes, or Gigabytes
        - Last accessed
            - Greater than (>) or Less than (<)
            - Value
            - Days, Weeks, Months, or Years

- Last modified
  - Greater than (>) or Less than (<)
  - Value
  - Days, Weeks, Months, or Years
- File patterns
  - Comma-delimited list of patterns
  - *.* (Move all files)
- File types
  - application
  - audio
  - compressed
  - image
  - message
  - model
  - system
  - text
  - video
- Description
- Associations
  - View associated pairs for the policy.
  - Add pair associations for the policy.
  - Remove pair associations for the policy.

C.4 Pair Statistics

- General
  - Pair status
    - Current status
    - Last run task
    - Start time
    - Elapsed time
    - Files scanned
    - Files moved
    - Total size moved
  - Policies associated to pair
    - Policy name
    - Status
    - Last run
    - Elapsed time

- Pair execution history
  - History of Bytes Moved (Recent history of policy executions on the pair)
    - Primary to secondary - graphical display
      - Run history list for a selected run of a policy on the primary path
        - File name
        - Extension
        - Size
    - Secondary to primary - graphical display
      - Run history for a selected run of a policy on the secondary path
        - File name
        - Extension
        - Size
    - Date and time of the selected policy run
  - Primary to secondary
    - Total files moved
    - Size of files moved (KB)
    - Total files failed to move
    - Policies executed
  - Secondary to primary
    - Total files moved
    - Size of files moved (KB)
    - Total files failed to move
    - Policies executed
- Pair history
  - History of Bytes on Primary and Secondary
  - Graphical display of bytes stored on the primary path
    - Summary inventory
      - Total size (default)
      - Number of files
      - Graph options
        - Accessed
        - Creation
        - Modified
        - File Size
        - Extension (default)
  - Graphical display of bytes stored on the secondary path
    - Summary inventory
      - Total size (default)

- Number of files
- Graph options
  - Accessed
  - Creation
  - Modified
  - File Size
  - Extension (default)
- Actions menu
  - Execute now
  - Preview now
  - Stop running process
  - Add policy association
  - Remove policy association
- View menu
  - Refresh (F5)
  - Preview results

C.5 Server Wizard

- IP/DNS
- Port
- Username
- Password

C.6 Setup Wizard

- Pair paths
  - Primary path
  - Secondary path
- Pair name
- Policy rules
  - Direction
    - Primary to Secondary
    - Secondary to Primary
  - Filter options
    - File size
      - Greater than (>) or Less than (<)
      - Value
      - Units: Bytes, Kilobytes, Megabytes, or Gigabytes

- Last accessed
  - Greater than (>) or Less than (<)
  - Value
  - Units: Days, Weeks, Months, or Years
- Last modified
  - Greater than (>) or Less than (<)
  - Value
  - Units: Days, Weeks, Months, or Years
- File patterns
  - Comma delimited list of patterns with no spaces before or after commas.
  - *.* (Move all files)
- File types
  - application
  - audio
  - compressed
  - image
  - message
  - model
  - system
  - text
  - video
- Policy schedule
  - Scheduled / Not scheduled
  - Frequency and when
    - Hourly
    - Daily
      - Start: Time of day in 15-minute increments. Default is 12:00 a.m.
      - Duration: Until complete (default), or specify the period of time as 1, 2, 3, 4, 5, 6, 8, 10, 12, 14, 16, 18, 20, 22, or 24 hours
    - Weekly (default)
      - Day: Sunday (default), Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
      - Start: Time of day in 15-minute increments. Default is 12:00 a.m.
      - Duration: Until complete (default), or specify the period of time as 1, 2, 3, 4, 5, 6, 8, 10, 12, 14, 16, 18, 20, 22, or 24 hours
    - Monthly
      - Day: Day of the month (1 through 31, with a default of 15)

- Start: Time of day in 15-minute increments. Default is 12:00 a.m.
- Duration: Until complete (default), or specify the period of time as 1, 2, 3, 4, 5, 6, 8, 10, 12, 14, 16, 18, 20, 22, or 24 hours
  - Yearly
    - Month: Month in the Gregorian calendar year
    - Day: Day of the month (1 through 31, with a default of 15)
    - Start: Time of day in 15-minute increments. Default is 12:00 a.m.
    - Duration: Until complete (default), or specify the period of time as 1, 2, 3, 4, 5, 6, 8, 10, 12, 14, 16, 18, 20, 22, or 24 hours
- Policy name and description
- Policy summary

C.7 Pair Wizard

- Pair paths
  - Primary path
  - Secondary path
- Pair name
- Policy to pair association

C.8 Policy Wizard

- Policy rules
  - Direction
    - Primary to Secondary
    - Secondary to Primary
  - Filter options
    - File size
      - Greater than (>) or Less than (<)
      - Value
      - Units: Bytes, Kilobytes, Megabytes, or Gigabytes
    - Last accessed
      - Greater than (>) or Less than (<)
      - Value
      - Units: Days, Weeks, Months, or Years
    - Last modified
      - Greater than (>) or Less than (<)
      - Period
      - Units: Days, Weeks, Months, or Years

- File patterns
  - Comma delimited list of patterns with no spaces before or after commas.
  - *.* (Move all files)
- File types
  - application
  - audio
  - compressed
  - image
  - message
  - model
  - system
  - text
  - video
- Policy schedule
  - Scheduled / Not scheduled
  - Frequency and when
    - Hourly
    - Daily
      - Start: Time of day in 15-minute increments. Default is 12:00 a.m.
      - Duration: Until complete (default), or specify the period of time as 1, 2, 3, 4, 5, 6, 8, 10, 12, 14, 16, 18, 20, 22, or 24 hours
    - Weekly (default)
      - Day: Sunday (default), Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
      - Start: Time of day in 15-minute increments. Default is 12:00 a.m.
      - Duration: Until complete (default), or specify the period of time as 1, 2, 3, 4, 5, 6, 8, 10, 12, 14, 16, 18, 20, 22, or 24 hours
    - Monthly
      - Day: Day of the month (1 through 31, with a default of 15)
      - Start: Time of day in 15-minute increments. Default is 12:00 a.m.
      - Duration: Until complete (default), or specify the period of time as 1, 2, 3, 4, 5, 6, 8, 10, 12, 14, 16, 18, 20, 22, or 24 hours
    - Yearly
      - Month: Month in the Gregorian calendar year
      - Day: Day of the month (1 through 31, with a default of 15)
      - Start: Time of day in 15-minute increments. Default is 12:00 a.m.
      - Duration: Until complete (default), or specify the period of time as 1, 2, 3, 4, 5, 6, 8, 10, 12, 14, 16, 18, 20, 22, or 24 hours
- Policy name and description

- Pair to policy associations
- Summary

C.9 Toolbar Menus

- File
  - New
    - Server
    - Pair
    - Policy
  - Import/Export
    - Import policy
    - Export policy
    - Import server list
    - Export server list
  - Exit
- View
  - Refresh (refreshes the screen display)
- Actions
  - Unlink
  - Execute now
  - Preview now
  - Stop running process
  - Statistics
  - Properties
- Help
  - Help Topics
  - Administration Guide
  - About Novell Dynamic File Services
    - Company
    - Company link
    - Product
    - Build number
    - Installation folder
    - Language
    - Product version
    - Copyright

C.10 Right-Click Menus

C.10.1 Server Folder

- Server Wizard

C.10.2 Server

- Disconnect / Connect
- Setup Wizard
- Properties

C.10.3 Pair Folder

- Pair Wizard

C.10.4 Pair

- Unlink
- Manual move
- Execute now
    - Policy list (if multiple policies)
- Preview now
    - Policy list (if multiple policies)
- Stop running process
- Statistics
- Properties

C.10.5 Policy Folder

- Policy Wizard
- Import policy

C.10.6 Policy

- Export

- Delete
- Execute now
  - Pair list (if multiple pairs)
- Properties

C.11 Service Controller

- Management Console
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
- Repair Tool

  See .
- Windows Firewall Access
  - On/Off
- Service Port Access
  - Use the default (8999)
  - Use this port
    - Port number
- Certificate Configuration
  - Create a new self-signed certificate
  - Use your own certificate from the Local Computer Personal Store
    - Certificate thumbprint
- Merged View Access
  - On/Off
- Service enabled and Stop service
- Service disabled and Start service
- About
  - Company
  - Company link
  - Product
  - Build number

- Installation folder
- Language
- Product version
- Copyright

C.12 Repair Tool

- Repair type
  - Repair
  - Report
- Repair option
  - Full
  - Pairs
  - Policies

C.13 Uninstall Wizard

- Modify
- Repair
- Remove

Keyboard Shortcuts

D

If your mouse is unavailable or if you prefer to use your keyboard, you can use keyboard shortcuts to navigate within the Novell Dynamic File Services (DynamicFS) Management Console and the Repair tool.

D.1 Using Keyboard Shortcuts

For keyboard shortcuts in which you press two or more keys simultaneously, the keys to press are separated by a plus sign (+). For keyboard shortcuts in which you press one key immediately followed by another key, the keys to press are separated by a greater-than symbol (>).

NOTE: The keyboard shortcuts that are described in this section refer to the U.S. keyboard layout. Keys on other layouts might not correspond exactly to the keys on a U.S. keyboard.

D.2 Quick Reference for Keyboard Shortcuts

To do this	Press
Cancel changes.	Esc
Close a dialog box or wizard without saving changes.	Alt+F4
Close a selected drop-down list.	
Display a selected drop-down list.	Alt+Down-arrow
Display *Help*.	F1
Display the *Actions* menu in the toolbar.	Alt+A
Display the *File* menu in the toolbar.	Alt+F
Display the *Help* menu in the toolbar.	Alt+H
Finished; apply the changes and close the wizard.	Alt+F
Go back to the previous pane in a wizard.	Alt+B
Go to the next pane in a wizard.	Alt+N
Apply the changes and close the wizard (when there is no *Next* button).	
Jump to the beginning of a list.	Ctrl+Home
Jump to the end of a list.	Ctrl+End
Move between options in an open menu, drop-down list, or between options in a group of options.	Arrow keys

To do this	Press
Move down one topic in a displayed menu.	Down-arrow
Move down to the next option in a radio-button selection.	
Move to the next option or option group in a pane.	Tab
Move to the previous option or option group in a pane	Shift+Tab
Move up one topic in a displayed menu.	Up-arrow
Move up to the previous option in a radio-button selection.	
Select (check) or deselect (clear) a check box.	Spacebar
Perform the action assigned to the selected button.	
Refresh the display in Statistics dialog boxes.	F5
Run the selected command or action.	Enter
Scroll through a displayed list.	Up-arrow or Down-arrow
Select an option.	Alt+ the letter underlined in an option
Switch to the next tab in the dialog box.	Ctrl+Tab
Switch to the previous tab in the dialog box.	Ctrl+Shift+Tab
Underscore the keyboard shortcut options for items in the toolbar.	Alt

D.3 Navigating with Keyboard Shortcuts

D.3.1 Toolbars

Pressing Alt underlines a character in each toolbar option to open the option's menu. For example, pressing Alt+F opens the *File* menu in the toolbar. In an open menu, use the Up-arrow and Down-arrow keys to select an item from the menu, then press Enter to execute the action.

D.3.2 Wizards

In the Dynamic File Services wizards, use the following keyboard navigation methods:

- Press the Tab key to navigate to the different fields and buttons on each page in the wizard.
- For a check box, press the spacebar like a toggle switch to select or deselect the option.
- For a radio button, press the Up-arrow or Down-arrow key to select a different radio button, then press Tab to continue to the next option.
- For a drop-down list, press Alt+Down-arrow key to open a drop-down box, use the Up-arrow or Down-arrow key to select an item in the list, then press Enter to select it.

- In a data field, type the information, then tab to the next field.

- When you are done on a page, tab to the appropriate button (such as *Next*, *OK*, *Apply*, or *Finish*) then press Enter.

- Press Esc to exit the wizard without applying unsaved changes. You can also tab to the *Cancel* button and press Enter to close without saving.

D.3.3 Dialog Boxes

To open the Pair Statistics dialog box, use the Tab key to navigate to the pair, then press Enter.

To open the Pair Properties dialog box, use the Tab key to navigate to the pair, press Alt+A to open the *Actions* menu, use the Down-arrow key to navigate to *Properties*, then press Enter to choose the option.

To open the Policy Properties dialog box, use the Tab key to navigate to the policy, press Alt+A to open the *Actions* menu, use the Down-arrow key to navigate to *Properties*, then press Enter to choose the option.

In a dialog box, press Ctrl+Tab to navigate between the page tabs, and press the Tab key to navigate within a page.

Email Subject and Body Format for Event Notifications

E
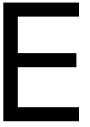
This section provides example notification messages for the Email add-on to the Novell Dynamic File Services Notification Services.

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

Event: Pair Created

```
Subject: NDFS Notification - Server Name: Pair Created
Body:
Date/Time: 10 January 2010 15:32
Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Description: Description of My Pair. (If No description This line will be
removed.)
```

Event: Pair Unlinked

```
Subject: NDFS Notification – Server Name: Pair Unlinked
Body:
Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Description: Description of My Pair. (If No description This line will be
removed.)
```

Event: Policy Created

```
Subject: NDFS Notification - Server Name: Policy Created
Body:
Date/Time: 10 January 2010 15:32
Policy Name:  My Policy
Policy Direction: Primary to Secondary or Secondary to Primary
Policy Type: Standard or Retention
Identity: Domain Name\User Name
Description: Description of My Policy. (If No description This line will
be removed.)
```

Event: Policy Modified

```
Subject: NDFS Notification - Server Name: Policy Modified
Body:
Date/Time: 10 January 2010 15:32
Policy Name:  My Policy
Policy Direction: Primary to Secondary or Secondary to Primary
Policy Type: Standard or Retention
Identity: Domain Name\User Name
Description: Description of My Policy. (If No description This line will
be removed.)
```

Event: Policy Scheduled to Run on Pair

```
Subject: NDFS Notification - Server Name: Policy Scheduled to Run on Pair
Body:
Date/Time: 10 January 2010 15:32
Policy Name:  My Policy
Policy Direction: Primary to Secondary or Secondary to Primary
Policy Type: Standard or Retention
Identity: Domain Name\User Name
Description: Description of My Policy. (If No description This line will
be removed.)

Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Description: Description of My Pair. If No description This line will be
removed.
```

Event: Policy Delete

```
Subject: NDFS Notification - Server Name: Policy Delete
Body:
Date/Time: 10 January 2010 15:32
Policy Name:  My Policy
Policy Direction: Primary to Secondary or Secondary to Primary
Policy Type: Standard or Retention
Identity: Domain Name\User Name
Description: Description of My Policy. (If No description This line will
be removed.)
```

Event: Policy Associated to Pair

```
Subject: NDFS Notification - Server Name: Policy Associated to Pair
Body:
Date/Time: 10 January 2010 15:32
Policy Name:  My Policy
Policy Direction: Primary to Secondary or Secondary to Primary
Policy Type: Standard or Retention
Description: Description of My Policy. (If No description This line will
be removed.)

Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Description: Description of My Pair. If No description This line will be
removed.
```

Event: Policy Disassociated with Pair

```
Subject: NDFS Notification - Server Name: Policy Disassociated with Pair
Body:
Date/Time: 10 January 2010 15:32
Policy Name:  My Policy
Policy Direction: Primary to Secondary or Secondary to Primary
Policy Type: Standard or Retention
Description: Description of My Policy. (If No description This line will
be removed.)

Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Description: Description of My Pair. (If No description This line will be
removed.)
```

Event: Added Exclude/Include Folders to Pair

```
Subject: NDFS Notification - Server Name: Added Exclude/Include Folders to
Pair
Body:
Date/Time: 10 January 2010 15:32
Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Current Include List or Exclude List:
myfolder\exclude\1;myfolder\excluded\2
```

Event: Removed Exclude/Include Folders to Pair

```
Subject: NDFS Notification - Server Name: Removed Exclude/Include Folders
to Pair
Body:
Date/Time: 10 January 2010 15:32
Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Current Include List or Exclude List:
myfolder\exclude\1;myfolder\excluded\2
```

Event: Policy Execute Now on Pair

```
Subject: NDFS Notification - Server Name: Policy Execute Now on Pair
Body:
Date/Time: 10 January 2010 15:32
Policy Name:  My Policy
Policy Direction: Primary to Secondary or Secondary to Primary
Policy Type: Standard or Retention
Description: Description of My Policy. (If No description This line will
be removed.)

Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Description: Description of My Pair. (If No description This line will be
removed.)
```

Event: Policy Preview Now on Pair

```
Subject: NDFS Notification - Server Name: Policy Preview Now on Pair
Body:
Date/Time: 10 January 2010 15:32
Policy Name:  My Policy
Policy Direction: Primary to Secondary or Secondary to Primary
Policy Type: Standard or Retention
Description: Description of My Policy. (If No description This line will
be removed.)

Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Description: Description of My Pair. (If No description This line will be
removed.)
```

Event: Policy Ran on Pair

```
Subject: NDFS Notification - Server Name: Policy Ran on Pair
Body:
Date/Time: 10 January 2010 15:32
Policy Name:  My Policy
Policy Direction: Primary to Secondary or Secondary to Primary
Policy Type: Standard or Retention
Description: Description of My Policy. (If No description This line will
be removed.)

Note: You get a event for each policy executed even when multiple are on a
pair and have the same run time.

Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Description: Description of My Pair. (If No description This line will be
removed.)
```

Event: Manual Move on Pair

```
Subject: NDFS Notification - Server Name: Manual Move on Pair
Body:
Date/Time: 10 January 2010 15:32
Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Description: Description of My Pair. (If No description This line will be
removed.)
```

Event: Stop Running Processes on Pair

```
Subject: NDFS Notification - Server Name: Stop Running Processes on Pair
Body:
Date/Time: 10 January 2010 15:32
Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Description: Description of My Pair. (If No description This line will be
removed.)
```

Event: Log Level Change on Pair

```
Subject: NDFS Notification - Server Name: Log Level Change on Pair
Body:
Date/Time: 10 January 2010 15:32
Pair name:  My Pair
Primary Path:  C:\primary
Secondary Path: C:\Secondary
Identity: Domain Name\User Name
Current Log Level  on DswMcpCore: Debug
Current log level on DswEnforcer: Debug
```