Installation and Administration Guide

Novell®
Dynamic File Services

January 14, 2010

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

G Silent Install Options for Dynamic File Services   201

H Using the Uninstall Tool to Modify, Repair, or Remove Dynamic File Services 203

I Using the Uninstall Tool to Modify, Repair, or Remove Dynamic File Services in a Windows Cluster   207

J Dynamic File Services Components   211

About This Guide

This guide describes how to install, configure, and manage Novell® Dynamic File Services (DynamicFS) pairs and policies in your Windows* storage environment.

Audience

This guide is designed to help storage solutions administrators:

- Make planning decisions for implementing pairs and policies as part of your overall storage solution strategy.

- Configure and manage the DynamicFS 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 anyone who is responsible for the security of the system.

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 Installation and Administration Guide*, visit the Dynamic File Services Documentation Web site (http://www.novell.com/documentation/dynamic_file_services/).

Additional Documentation

Additional documentation is available on the Dynamic File Services Documentation Web site (http://www.novell.com/documentation/dynamic_file_services/):

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol ($^{®}$, ^{TM}, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

Overview of Dynamic File Services

<div align="right">1</div>

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 the same or different storage devices on a server. DynamicFS transparently provides a merged view of the file tree to users 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. You specify policies that classify the files to be moved based on frequency of use, file extension, and file size. Policy enforcement is automated with scheduled and on-demand policy enforcement.

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 mission-critical data on high-performance storage devices, and move seldom-used less-essential data to lower-performance devices. Backup can be performed separately on the two paths, which allows for different backup schedules.

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 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.

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 and without affecting user access to the data they use most often.

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 measures for the underlying file systems control 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 DynamicFS 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.

Move data seamlessly between the two paths

 ◆ Define policies that control what data is 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.

 ◆ Apply a policy to multiple pairs.

 ◆ Apply multiple policies to a pair.

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.

 ◆ 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.

 ◆ 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.

 ◆ Schedule a window of time when you want a policy to run by specifying the start time and duration of the run.

 ◆ Schedule a policy to run hourly, daily, weekly, or monthly.

 ◆ Start and stop policies manually. Scheduled and unscheduled policies can be run manually for one or more of their associated pairs.

1.1 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.

 ◆ Section 1.1.1, "Storage Nears Its Capacity," on page 17
 ◆ Section 1.1.2, "Storage for Seldom-Used Files," on page 17

1.1.1 Storage Nears Its Capacity

Abraham works for a large university system with thousands of students each semester. Students have a home directory to use as a workspace for their personal files and homework.

The Data

The home directory workspaces contain many media files for music and pictures.

The DynamicFS Solution

Abraham creates a DynamicFS pair where the primary location is a folder that contains all user home directories. He uses an empty drive as the secondary location in the pair. He creates a policy that moves media files from the primary to secondary every night between 2:00 a.m. to 4:00 a.m.

This helps free the needed space on the primary drive while allowing users to transparently access their media files on either drive. Users are not aware of the physical location of their files.

1.1.2 Storage for Seldom-Used 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.

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.

Current and active patient records from all specialty clinics and hospital units must be available on demand.

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. The historic 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 DynamicFS Solution

Joe creates a different DynamicFS pair for each of the pre-1975 specialty clinics. A policy for each pair is tailored to move the largest image files daily between 7:00 p.m. and midnight. After the large files are migrated, Joe modifies the policy to move other file types and sizes.

This 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.

1.2 Key Components of Dynamic File Services

Novell Dynamic File Services includes multiple components to manage pairs and policies. Table 1-1 describes the DynamicFS components that run automatically after the install.

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

DynamicFS Components	Description
DynamicFS 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 DynamicFS Service is the engine for all of the DynamicFS components. On a server, the DynamicFS Service automatically starts and runs in the background.
	You can verify that the service is running by looking for the `DswService.exe` process in the Task Manager.
Service Controller	The DynamicFS Service Controller allows the Administrator user and members of the Dynamic File Services group to enable, disable, or configure the DynamicFS Service. You can also launch the DynamicFS Management Console and Repair tool.
	The DynamicFS Service Controller icon is displayed in the notification area of the server desktop. It starts automatically when the Administrator user or a member of the Dynamic File Services group logs in to the server desktop. The application is `DswServiceController.exe`.
Management Console	The DynamicFS 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 DynamicFS pairs and policies.
	The DynamicFS Management Console icon is placed on the desktop, in the *Control Panel*, and in the *Start* menu in *DynamicFS > DynamicFS Management Console*. These icons are shortcuts that open the `DswMgmtConsole.exe` application.
Filter Driver	The DynamicFS Filter Driver is a Windows* File System filter driver that is managed by the DynamicFS Service and runs whenever the DynamicFS 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 the DynamicFS pair.
	The DynamicFS Filter Driver is installed in the `C:\Windows\System32\Drivers` folder and is named `dswflt.sys`.

Table 1-2 describes other DynamicFS applications run when they are called or are scheduled to run.

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

DynamicFS Components	Description
Certificate Configuration	The DynamicFS 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 your own SSL certificate. For information, see Section 6.7.3, "Configuring a Non-Self-Signed Certificate for Dynamic File Services," on page 71.
	Access this utility through the *Service Controller* menu. The application is `DswCert.exe`.
CLI	The DynamicFS 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 Appendix A, "Dynamic File Services Commands for Pair and Policy Management," on page 141.
	The application is `DswCLI.exe`.
Configuration Dump	The DynamicFS Configuration Dump utility aggregates information about the current DynamicFS server settings for pairs, policies, and logs, and puts it an output file in XML format. This tool is available to help with troubleshooting when working with Novell Support.
	For information, see Appendix D, "Dynamic File Services Configuration Dump Utility," on page 185.
	The application is `DswDump.exe`.
Enforcer	The DynamicFS Enforcer runs selected policies for a pair when you select *Execute Now* or when the policy is scheduled to run.
	The DynamicFS Service controls when the enforcer runs. The application is `DswEnforcer.exe`.
File System Inventory	The DynamicFS 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 metadata information 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 8.7, "Scheduling the Pair History Scan," on page 90.
	The DynamicFS Service controls when the File System Inventory runs. The application is `DswInventory.exe`.

DynamicFS Components	Description
Repair tool	The DynamicFS 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 it was taken. Thus, 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 DynamicFS Repair tool from the *Service Controller* menu. The application is `DswRepair.exe`.
Synchronize Pair tool	The DynamicFS Synchronize Pair utility is used to detect duplicate files in the DynamicFS 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. The application is `DswSyncPair.exe`.

Getting Started with Dynamic File Services

2

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.

2.1 Installing and Setting Up Dynamic File Services

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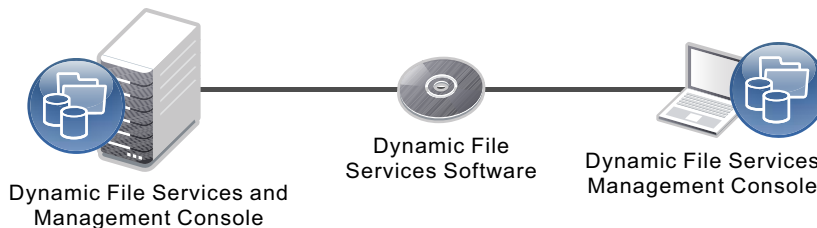
The DynamicFS Service controls the pairs and policies that you create on a server. After the install and on server reboots, the DynamicFS Service automatically starts and runs in the background. Each server's pairs and policies are unique on the server, and their related configuration files are stored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

The Dynamic File Services group is a local server-based group that is created when the DynamicFS 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 the Administrator user (or a user with Administrator 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 DynamicFS 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 DynamicFS Service and manage the its settings, such as the Service Port Access, the Windows Firewall Access, and the Certificate Configuration. You can also use it to open the Management Console or open the Repair tool.

2.2 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 DynamicFS *Windows Firewall Access* option must be enabled on the target server so that an exception in the Windows Firewall is allowed for the configured DynamicFS Service port. Remote management communications are secured with SSL.

Dynamic File Services
Management Console

IP or DNS: localhost
Username: Administrator
Password: password
Port: 8999

Dynamic File Services

Local
Management

Remote
Management

Dynamic File Services
Management Console

IP or DNS: server1.example.com
Username: Administrator
Password: password
Port: 8999

Dynamic File Services
Server
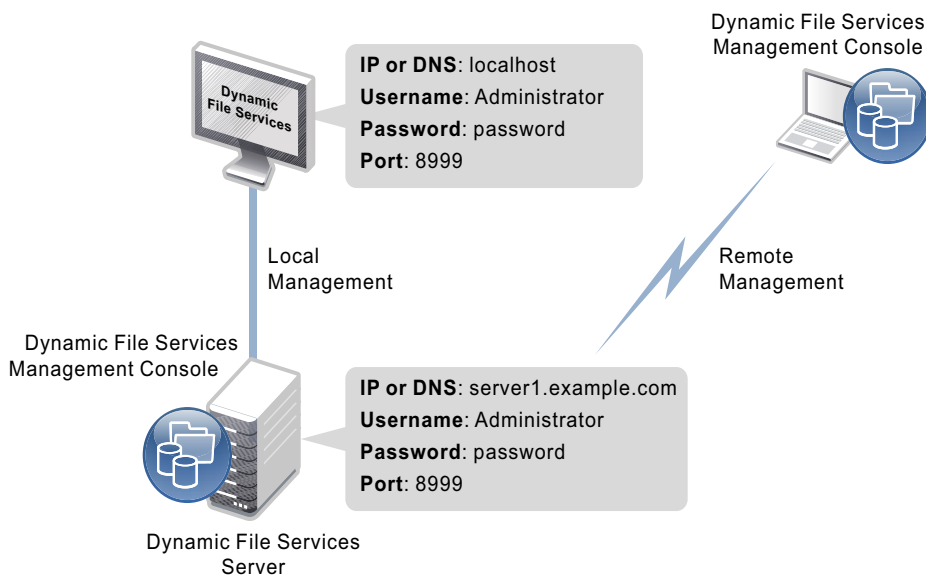
2.3 Creating a Dynamic File Services Pair

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. Paths can contain files or be empty. Pair names must be unique on the server.

Create a DynamicFS 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 a policy, then it automatically associates them. 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 file tree 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 share on the secondary path.
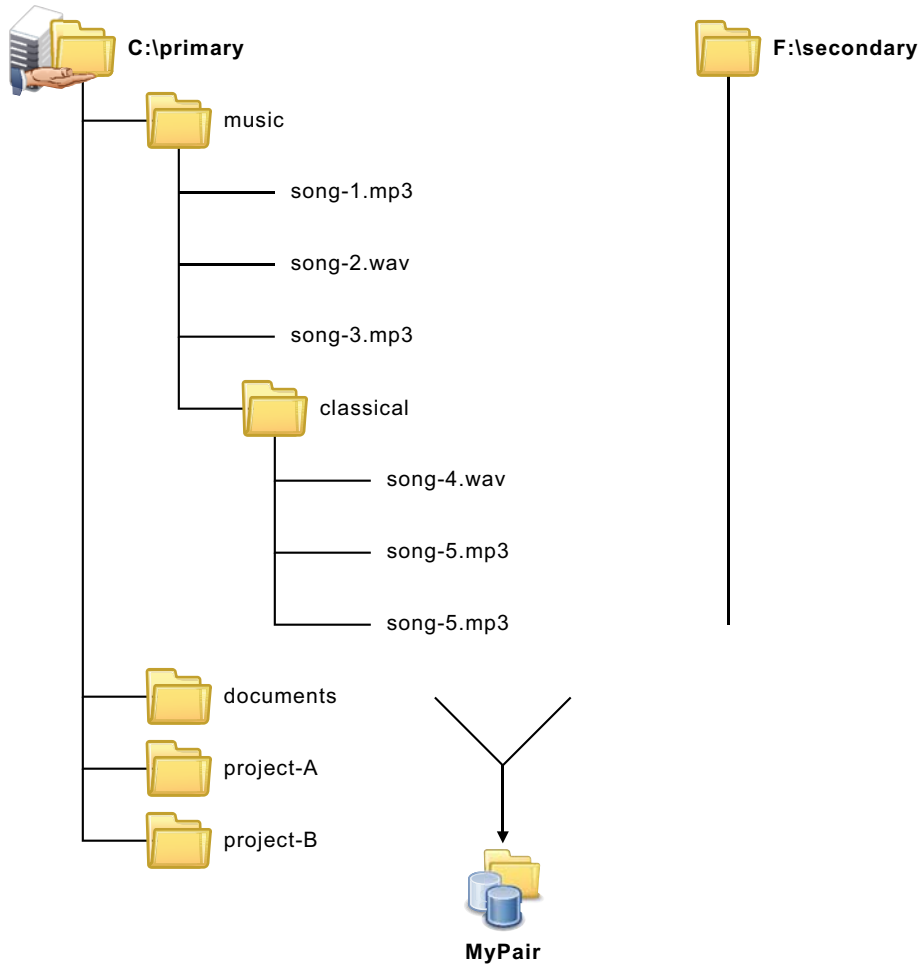
Primary Path: Path on a local drive.

Secondary Path: Path on the same or different local drive.
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.

2.4 Creating a Dynamic File Services Policy

A Dynamic File Services 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 DynamicFS 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 extension

A policy can have no schedule or be scheduled to run hourly, daily, weekly, or monthly. 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 a policy, then automatically associates the them. 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 criteria for moving files. Filters set in the same policy are "AND" operations. Files are moved only if they meet all of the criteria in the policy.

IMPORTANT: Filters set in separate policies that are run on the same pair are "OR" operations. Files are moved if they meet the criteria in any one of the policies.

Schedule: Set when to run the policy.

Policy Name: Give the policy a unique name.

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

2.5 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 associatione 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 pair or policy and modifying its associations.

MyPair   **MyPolicy**

2.6 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.

Assign one or more policies
to a given pair.

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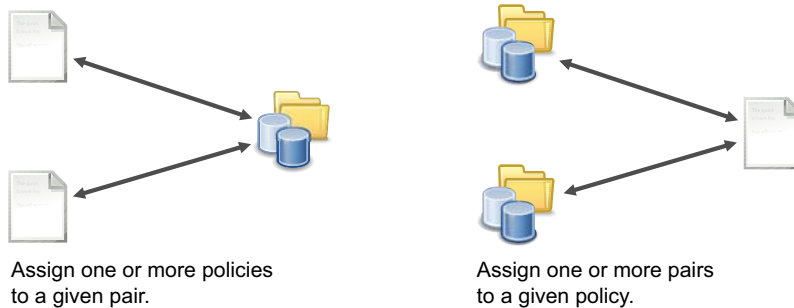
Use any of the following methods to create additional pairs and policies and associate them:

 ◆ **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.

2.7 Enforcing Policies

In a policy run, a Dynamic File Services 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.
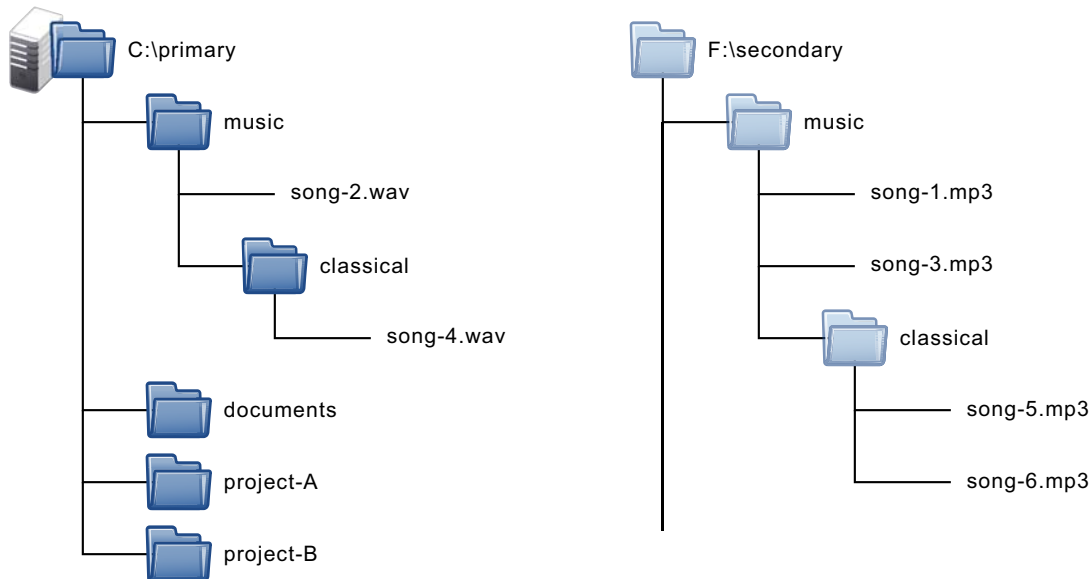
2.8 Viewing the Merged File Tree for a Pair

Users access the primary path on the Dynamic File Services pair via a network share (*servername**sharename*) to get a merged file tree 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 file tree 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.
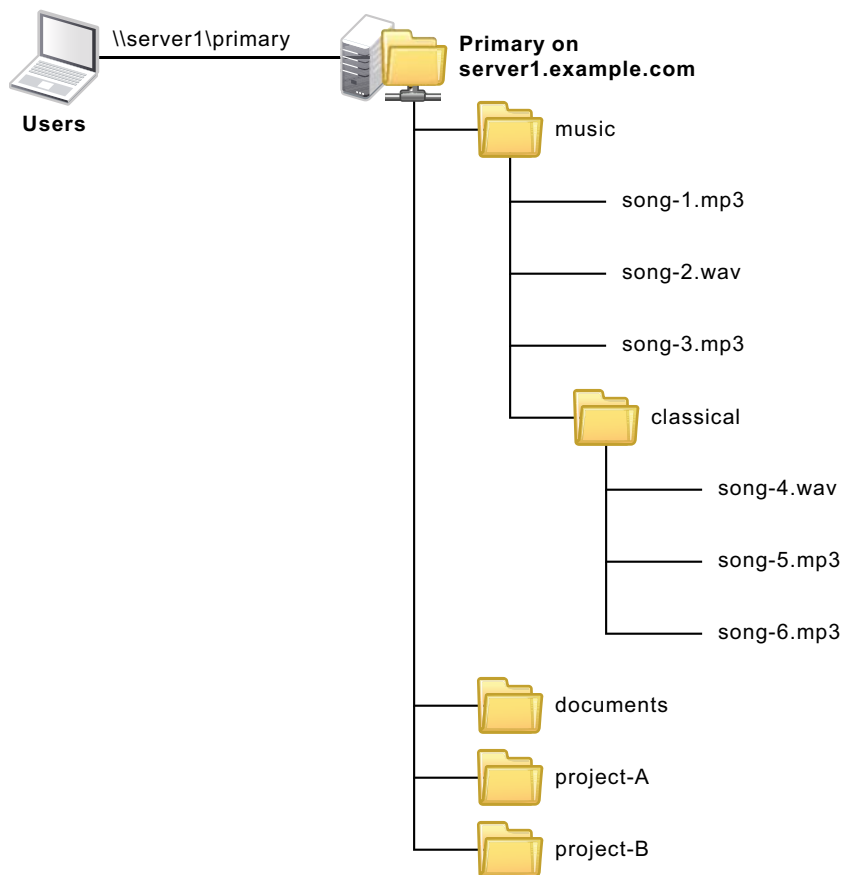
2.9 Backing Up Files in the Pair

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.
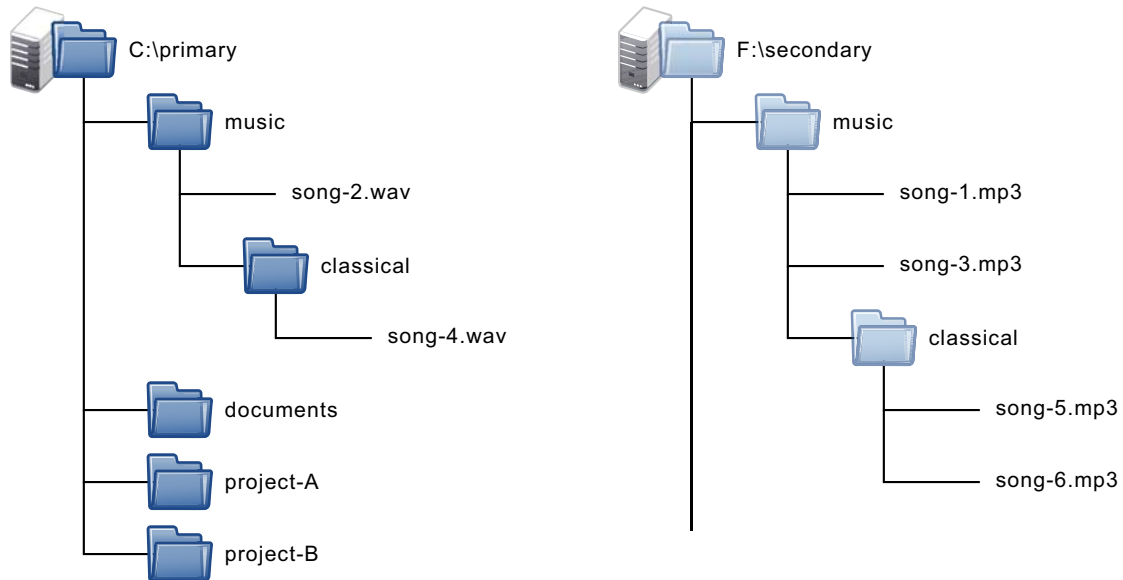
Planning for Dynamic File Services Pairs and Policies

3

Novell® Dynamic File Services (DynamicFS) pairs and policies are easy to set up and manage, but 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 of DynamicFS in your Windows environment.

IMPORTANT: For information about supported configurations, see Section 4.1, "Planning the Installation," on page 39.

- Section 3.1, "Dynamic File Services Group," on page 29
- Section 3.2, "Server-Centric Pair and Policy Configuration," on page 30
- Section 3.3, "Dynamic File Services Pairs," on page 30
- Section 3.4, "Merged File View for Users," on page 30
- Section 3.5, "Naming Conventions for Pairs and Policies," on page 31
- Section 3.6, "File and Folder Attributes and ACL Permissions," on page 31
- Section 3.7, "Duplicate Folders," on page 32
- Section 3.8, "Duplicate Files," on page 32
- Section 3.9, "System Files," on page 33
- Section 3.10, "Policy Schedules," on page 33
- Section 3.11, "Time Displays," on page 34
- Section 3.12, "Event Logging," on page 34
- Section 3.13, "Using Antivirus Software with Dynamic File Services Pairs," on page 34
- Section 3.14, "Using Backup Software with Dynamic File Services Pairs," on page 34
- Section 3.15, "Using Compression with Dynamic File Services Pairs," on page 35
- Section 3.16, "Using Disk Quotas with Dynamic File Services Pairs," on page 35
- Section 3.17, "Using Encryption with Dynamic File Services Pairs," on page 35
- Section 3.18, "Using Windows Distributed File System with Dynamic File Services Pairs," on page 36

3.1 Dynamic File Services Group

The Dynamic File Services group is created automatically during the installation of the Dynamic File Services Service. The Administrator user account is automatically allowed to administer DynamicFS, but the username is not added by default to the Dynamic File Services group. If you want a different user to administer the DynamicFS Service on that computer, the user's username must be added to the Dynamic File Services group.

For information, see Section 6.1, "Adding or Removing Members in the Dynamic File Services Group," on page 61.

3.2 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` directory 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 Dynamic File Services Service login can validate administrator user identity in Workgroup and Active Directory* Domain environments.

3.3 Dynamic File Services Pairs

Dynamic File Services pairs consist of a primary location and a secondary location that DynamicFS manages as a unit. DynamicFS 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 criteria:

- Drives must be mounted and appear as native local drives.
- The 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.
- DynamicFS pairs cannot be nested. The primary location and the secondary location cannot contain folders or reside in folders that are already in use for another pair.

3.4 Merged File View for Users

Dynamic File Services leverages Microsoft* Network Sharing to provide the merged file tree 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 DynamicFS 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 3.6, "File and Folder Attributes and ACL Permissions," on page 31.

- 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.

3.5 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.

3.6 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 who accesses the data via the merged file tree view.

After creating a DynamicFS 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 file tree 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 file tree 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 file tree 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 file tree 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 8.8, "Reporting Conflicts for Attributes and ACL Permissions," on page 90.

3.7 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 file tree 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.

DynamicFS automatically synchronizes the metadata information (such as ACLs and attributes) from the primary location instance of the folder to its secondary instance. DynamicFS does this automatically when the folders are accessed via the merged file tree 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 3.6, "File and Folder Attributes and ACL Permissions," on page 31.

The attributes and ACL settings for the two folder instances can become out of synchronization if you access a folder directly instead of via the merged file tree view and modify its metadata. 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 8.8, "Reporting Conflicts for Attributes and ACL Permissions," on page 90.

3.8 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 file tree 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.

Duplicate files can occur when restoring 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.

Duplicate files can also occur if you access a file directly instead of via the merged file tree view. You should always use the merged file tree view when creating, modifying, or deleting files in a pair.

Duplicate files have the same name and are located in matching subdirectories in both the primary and secondary storage locations. If a copy of a file exists in the primary and secondary locations, only the file 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 attempts to move a duplicate file, the move fails, and the error is reported in the policy move log in the *Statistics > Policy execution history*.

For information about detecting and reporting duplicate files, see Section 8.9, "Reporting Conflicts for Duplicate Files," on page 91.

3.9 System Files

The Dynamic File Services policy enforcer component 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.

3.10 Policy Schedules

Dynamic File Services 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 set within an individual policy are enforced as an AND condition.

Only one DynamicFS 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 8.7, "Scheduling the Pair History Scan," on page 90.

DynamicFS 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 as described above.

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 DynamicFS enforcer 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 105.

3.11 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.

3.12 Event Logging

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

3.13 Using Antivirus Software with Dynamic File Services 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 file tree view.
- Run your antivirus software separately on each drive, or run it separately on the primary and secondary path.

3.14 Using Backup Software with Dynamic File Services 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.

3.15 Using Compression with Dynamic File Services 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.

3.16 Using Disk Quotas with Dynamic File Services 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.

3.17 Using Encryption with Dynamic File Services 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 DynamicFS policy, the encryption key changes and the data is no longer accessible to the user. The data is effectively lost.

- Section 3.17.1, "Windows File and Folder Encryption," on page 36
- Section 3.17.2, "Hardware-Level Disk Encryption," on page 36

3.17.1 Windows File and Folder Encryption

DynamicFS does not support using file or folder encryption for DynamicFS pairs.

To prevent possible data loss, make sure your DynamicFS 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.

3.17.2 Hardware-Level Disk Encryption

DynamicFS 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.

3.18 Using Windows Distributed File System with Dynamic File Services Pairs

Dynamic File Services supports using Windows Distributed File System (DFS) links to point to the network share on the primary folder in a DynamicFS pair. That is, the network share on the primary path of the DynamicFS 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 DynamicFS 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 DynamicFS pairs and DFS 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 DynamicFS 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.

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

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).

3.18.1 Example: Dynamic File Services and Windows Distributed File System on Different Servers

Figure 3-1 illustrates a configuration where the Windows Distributed File System Server is a different server than the targets of the DFS links. DynamicFS is installed on the servers where you create the DynamicFS pairs, but it is not installed on the DFS Server. DFS links point to the network shares on the primary paths of the DynamicFS pairs.

Figure 3-1   *Using Windows DynamicFS and DFS on Different Servers*
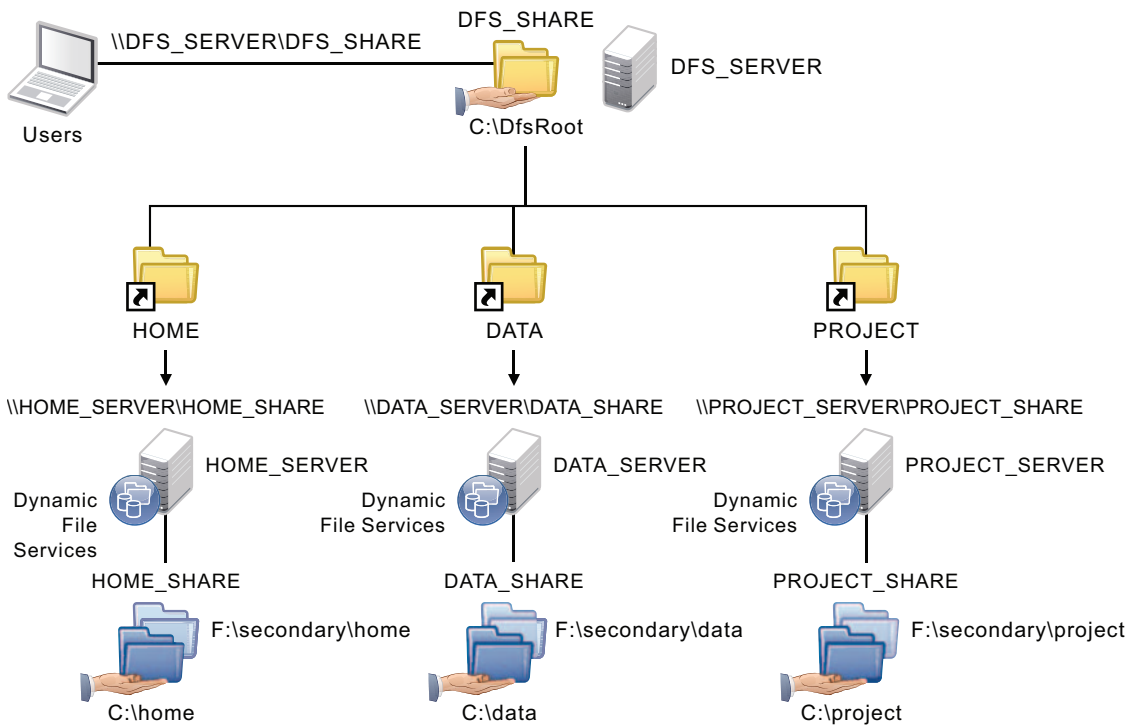
3.18.2 Example: Dynamic File Services and Windows Distributed File System on the Same Server

Figure 3-2 illustrates a configuration where the Windows Distributed File System Server is on the same server as the targets of the DFS links. In this case, DynamicFS is installed on the DFS Server. DFS links point to the network shares on the primary paths of the DynamicFS pairs. The DFS Namespace folder (or DFS Root folder) is not configured as a DynamicFS pair, and it is not nested with any of the primary paths and secondary paths that are used in the DynamicFS pairs.

Figure 3-2 *Using DynamicFS and DFS on the Same Server*
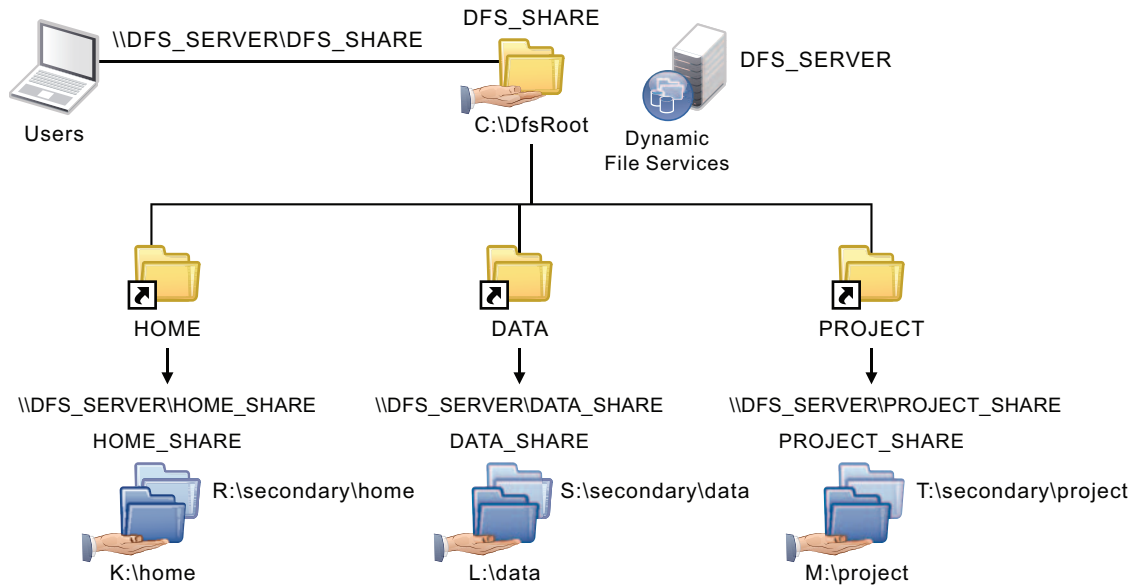
Installing and Setting Up Dynamic File Services

4

This section explains how to install and set up Novell® Dynamic File Services (DynamicFS).

4.1 Planning the Installation

This section identifies the supported configurations and key issues to consider when planning to install Novell Dynamic File Services.

IMPORTANT: For general planning information, see Chapter 3, "Planning for Dynamic File Services Pairs and Policies," on page 29.

For Windows clusters, also see Section 5.1, "Planning the Installation in a Windows Cluster," on page 49.

4.1.1 Supported Platforms

◆ "Windows Servers" on page 40
◆ "Windows Workstations" on page 40

Windows Servers

You can install the Service and Management components of Dynamic File Services on your Windows servers. DynamicFS supports both 32-bit and 64-bit architectures for the following Microsoft Windows Server* operating systems with the latest service packs and patches applied:

◆ Windows Server 2008 R2
◆ Windows Server 2008 Service Pack 2 or later
◆ Windows Server 2003 Service Pack 2 or later

Windows Workstations

You can install the Dynamic File Services Management component on a Windows workstation in order to manage the DynamicFS Service running on your servers. DynamicFS supports both 32-bit and 64-bit architectures for the following Windows client operating systems with the latest service packs and patches applied:

◆ Windows 7
◆ Windows Vista* Service Pack 1 or later
◆ Windows XP Service Pack 3 or later

It is not supported to install the Dynamic File Services Service component on Windows workstations in a production environment. However, you can install the Service component on a workstation for testing purposes. For information about configuration requirements on Windows XP, see "Disabling Simple File Sharing on Windows XP" (http://www.novell.com/documentation/dynamic_file_services/dynamic_readme/data/dynamic_readme.html#bltz17z) in the *Dynamic File Services: Readme* (http://www.novell.com/documentation/dynamic_file_services/dynamic_readme/data/dynamic_readme.html).

4.1.2 Supported Devices

The storage devices where you want to create the Dynamic File Services pair must be attached to the server. This includes Fibre Channel, iSCSI, and direct-attached storage devices (internal or external). DynamicFS does not support using CDs, DVDs, or floppy drives in a pair.

Only devices that the system considers to be native storage devices can be used. This means no flash drives or mapped drives.

The drives used in a DynamicFS 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.

4.1.3 Supported File Systems

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

4.1.4 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.

4.1.5 Software Requirements

The following software should be installed and working properly before installing Dynamic File Services:

◆ Microsoft .NET 3.5 Service Pack 1

If .NET is not already installed on the computer, the Dynamic File Services InstallShield* Wizard automatically attempts to install the following Microsoft .NET 3.5 SP1 download:

```
http://download.microsoft.com/download/0/6/1/061f001c-8752-4600-a198-
53214c69b51f/dotnetfx35setup.exe
```

An Internet connection is required. The download time varies based on your connection speed. A reboot might be required on some platforms.

If the InstallShield Wizard is unable to install .NET, the wizard halts the installation and returns an error to install .NET 3.5 SP1. Manually install .NET, then start the InstallShield Wizard to install Dynamic File Services.

◆ Microsoft Network Sharing
◆ Microsoft Event Logger

4.1.6 Security Considerations

Use the guidelines in this section to configure the initial security settings for Dynamic File Services during the install.

◆ "Dynamic File Services Self-Signed SSL Certificate" on page 41
◆ "Dynamic File Services Service Port" on page 42
◆ "Windows Firewall Access" on page 42
◆ "Dynamic File Services Group" on page 42
◆ "Windows User Access Control" on page 42
◆ "Network Connections" on page 42
◆ "Network Shares" on page 43

Dynamic File Services Self-Signed SSL Certificate

During the installation, Dynamic File Services creates and configures a self-signed certificate (*servername*-DynamicFileServicesSSLCertificate) for the SSL communications to use.

After the install, you can continue to use the self-signed certificate, or configure DynamicFS to use your own non-self-signed certificate. For information, see Section 6.7.3, "Configuring a Non-Self-Signed Certificate for Dynamic File Services," on page 71.

Dynamic File Services Service Port

During the install, you can use the *Custom* install option to modify the port to use for remote management of the DynamicFS Service. By default, DynamicFS uses port 8999.

You can modify the port during or after the install. For information, see Section 6.5, "Configuring the Dynamic File Services Service Port," on page 66.

Windows Firewall Access

During the install, you can use the *Custom* install option to enable an exception in the Windows Firewall for the configured Dynamic File Services Service port (default 8999). The firewall exception is enabled by default. Disabling the firewall exception effectively disables the remote management capability for the DynamicFS Service.

You can also enable and disable the firewall exception after the install. For information, see Section 6.6, "Enabling or Disabling a Firewall Exception for the Dynamic File Services Service Port," on page 67.

Dynamic File Services Group

During the install, a new group called *Dynamic File Services* is created on machines where you install the Dynamic File Services Service. The Dynamic File Services group is a local group, not a domain group. Initially, there are no members assigned in the Dynamic File Services group. Only the Administrator user account on the machine and the users you assign to be members of the Dynamic File Services group are allowed to manage DynamicFS.

IMPORTANT: The Administrator user is the only user account in the Administrators group that is allowed to manage DynamicFS without first being added as a member of the Dynamic File Services group. You can add the Administrator user account to the Dynamic File Services group.

After the install, you set up DynamicFS administrators by adding them as members of the Dynamic File Services group. It is not necessary for the Dynamic File Services group members to also be members in the Administrators group. You must be logged in as a user with Administrators group privileges in order to add members to the Dynamic File Services group.

When using 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.

Windows User Access Control

Windows User Access Control is available on some Windows platforms. If it is enabled, Windows User Access Control typically prompts you for permission to run an application when the application starts. If you are prompted for permission, type the password or provide confirmation.

Network Connections

You can run the DynamicFS 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 the pairs on a server, 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.

Network Shares

To give users a merged file tree view of the files in the two locations, create a network share on the primary folder of the DynamicFS pair. Users map a drive on their computers to the network share.

For secure access and authentication, users should access the data in the pair via merged file tree view. You can create additional network shares above or below the share on the primary path.

If users directly access the primary path or secondary path, conflicts can arise with duplicate files or with access rights and attributes being out of synchronization between primary and secondary folders. The DynamicFS Synchronize Pair utility can be used to report conflicts if this situation arises.

Conflicts can also be caused if users access data on the secondary location via shares on the secondary location instead of through the merged file tree view. To prevent potential conflicts, make sure to remove network shares for the secondary path. In addition, shares must not be nested above or below or 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 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.

4.1.7 Destination Folder for the Dynamic File Services Software

The default destination folder for the software is `C:\Program Files\Dynamic File Services`. You can configure a different location during the install by using the *Custom* install option.

4.1.8 Installation Files

Novell Dynamic File Services is available in the Novell File Management Suite. On the Novell Downloads page (http://www.novell.com/documentation/downloads), search for the Novell File Management Suite, then download the Dynamic File Services software. Choose the install file based on the processer architecture of your computer:

Architecture	Install File
32-bit	`DswSetup-x86.exe`
64-bit	`DswSetup-x64.exe`

4.1.9 Silent Install Options

DynamicFS supports the InstallShield silent install options. For information, see Appendix G, "Silent Install Options for Dynamic File Services," on page 201.

4.1.10 Cluster Install

DynamicFS can be used in a Windows cluster environment, but it is not cluster aware. For information, see Chapter 5, "Installing, Setting Up, and Using Dynamic File Services in a Windows Cluster," on page 49.

4.2 Installing Dynamic File Services with the InstallShield GUI

Install Dynamic File Services on the server where you want to create pairs and policies, and on any computer from which you want to remotely manage DynamicFS servers.

1 Log in as the Administrator user, or as a user in the Windows Administrators group.

2 Download the 32-bit (x86) or 64-bit (x64) architecture version of the `DswSetup-*.exe` file to a folder on the server or the client computer where you want to install it.

3 Double-click the file to start the InstallShield Wizard, then follow the on-screen instructions to install the DynamicFS software:

Wizard Page	Action
Welcome	Click *Next*.
License Agreement	Read and accept the agreement, then click *Next*.
Setup Type	Select one of the following setup options: **Complete:** Select *Complete* to accept the default setup, then click *Next* to continue to the Ready to Install the Program page. **Custom:** Select *Custom*, then click *Next* to continue to the Installation Details page where you can view and modify the setup options.
Installation Details (Custom install only)	Modify the following options if desired, then click *Next* to continue to the Select Features page: **Allow an exception for the DynamicFS Service port in the firewall:** Select this option to enable the remote management of the DynamicFS Service. It is enabled by default. **Service port:** Specify the port number (default 8999) to use for the DynamicFS Service remote management communications. **Destination folder:** Click *Browse* to locate and select the destination folder where you want to install the DynamicFS software, then click *OK*. The default destination folder is `C:\Program Files\Dynamic File Services`.
Select Features (Custom install only)	Specify which DynamicFS components to install on this computer, then click *Next* to continue to the Ready to Install the Program page. **Management:** The management tools are automatically selected for install on both servers and clients. This option cannot be deselected. **Service:** Select the DynamicFS Service for server installations where you want to use pairs and policies.
Ready to Install the Program	Click *Install* to begin the installation.
InstallShield Wizard Complete	Specify whether to open the Readme and DynamicFS Management Console now, then click *Finish* to exit the wizard.

4 (Optional) Verify the installation setup by inspecting the various DynamicFS components that are described in Table 1-1, "Dynamic File Services Components That Run Automatically," on page 18.

5 Continue with Section 6.1, "Adding or Removing Members in the Dynamic File Services Group," on page 61.

4.3 Configuring Administrators for the Dynamic File Services Group

Dynamic File Services administrators are users you assign as members of the Dynamic File Services group. The Administrator user is the only user account in the Administrator group that can manage DynamicFS without explicitly being added to the Dynamic File Services group. For information, see "Configuring Administrators for the Dynamic File Services Group" on page 45.

During the install of the DynamicFS Service, the Dynamic File Services group is automatically added as a local group on the computer. However, no users are added to the group during the install. To enable users (in addition to the Administrator user) to be DynamicFS administrators, you must add them to the Dynamic File Services group. The Administrator user or any user with Administrator privileges can add usernames as members of the Dynamic File Services group.

1 After the install, log in as the Administrator user or as a user with Administrator privileges.

2 Open the *Windows Computer Management* dialog box.

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

4 Click *Add*, then type the usernames in the *Enter the object names to select* field of the users you want to manage DynamicFS on that server.

For information about requirements for DynamicFS administrator users, see "Dynamic File Services Group" on page 42.

5 Click *OK* to save and apply your changes, then click *OK* to close the *Properties* dialog box.

6 Continue with Section 4.4, "Configuring Network Shares," on page 45.

4.4 Configuring Network Shares

Use the Windows Network Sharing feature to set up a network share for each of the folders that you plan to use as the primary location in Dynamic File Services pairs. After you set up a pair, users map to the network share on its primary location to get a merged view of the data on the primary and secondary locations.

Continue with Section 4.5, "Connecting to a Server," on page 45.

4.5 Connecting to a Server

Use the Dynamic File Services Management Console to connect to the server you want to manage.

1 Open the DynamicFS Management Console, then open the Server Wizard.

When no pairs or policies are defined on the computer where you are running the Management Console, a Server Wizard opens automatically to help you set up a connection to the server you want to manage.

2 Provide the following information:

- IP address or DNS name of the DynamicFS server you want to manage.

  If you are managing the server locally (that is, you are logged in to the server), you can use `localhost` or the loopback IP address (`127.0.0.1`) to manage the server without enabling an exception in the firewall for the DynamicFS Service port.

- The DynamicFS Service port number (default 8999).

- The username and password credentials for a user that you added to the Dynamic File Services group (or for the Administrator user) on the target DynamicFS server.

3 Click *Connect*.

If you are connecting to a remote server, you are prompted to accept the DynamicFS SSL Certificate. For information, see Section 7.2, "Accepting a Dynamic File Services Certificate," on page 77.

The server folder is created and appears in the left panel.

4 Continue with Section 4.6, "Creating the First Pair and Policy," on page 46.

4.6 Creating the First Pair and Policy

In the Dynamic File Services Management Console, use the Setup Wizard to create a pair and a policy. The pair and policy are automatically associated.

If no pairs or policies have been defined for the specified DynamicFS server, the Setup Wizard opens automatically to help you to create a DynamicFS pair, to create a policy for the pair, and to associate the policy to the pair.

For information, see the following sections:

1. Section 8.2, "Creating a Pair," on page 84
2. Section 9.2, "Creating a Policy," on page 97
3. Section 8.3, "Giving Users Access to Files on a Pair," on page 88

Continue with Section 4.7, "Creating More Pairs and Policies," on page 46.

4.7 Creating More Pairs and Policies

Use any of the following methods to create additional Dynamic File Services pairs and policies:

- **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*.

For information, see the following sections*:*

- Section 8.2, "Creating a Pair," on page 84
- Section 9.2, "Creating a Policy," on page 97

Continue with Section 4.8, "Running Policies," on page 47.

4.8 Running Policies

The policies for a Dynamic File Services pair run at their next scheduled time, but you can run a policy at any time by right-clicking a pair and selecting the *Execute Now* option.

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.

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.

Continue with Section 4.9, "Accessing Data on a Pair," on page 47.

4.9 Accessing Data on a Pair

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

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.

4.10 Additional Information

See the following resources for additional information about installing, modifying, and uninstalling Dynamic File Services:

- Appendix G, "Silent Install Options for Dynamic File Services," on page 201
- Appendix 5, "Installing, Setting Up, and Using Dynamic File Services in a Windows Cluster," on page 49
- Appendix H, "Using the Uninstall Tool to Modify, Repair, or Remove Dynamic File Services," on page 203
- Appendix I, "Using the Uninstall Tool to Modify, Repair, or Remove Dynamic File Services in a Windows Cluster," on page 207

4.11 What's Next

- Section 7.1, "Setting Up a Server in the Management Console," on page 75
- Section 8.2, "Creating a Pair," on page 84
- Section 9.2, "Creating a Policy," on page 97

Installing, Setting Up, and Using Dynamic File Services in a Windows Cluster

5

Novell® Dynamic File Services (DynamicFS) supports using pairs and policies in a Windows failover cluster. However, DynamicFS is not cluster aware.

This section provides general guidelines for installing, setting up, and using DynamicFS on servers in a Windows cluster.

IMPORTANT: The Windows cluster configuration, management, terminology, and tools can vary depending on the version of Windows Server you are running and on how you set up your cluster and cluster resources. Adjust the instructions in this section as needed for your cluster environment.

For all issues related to Windows cluster configuration and management, see the official Microsoft documentation for your Windows Server operating system in the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/default.aspx).

5.1 Planning the Installation in a Windows Cluster

Make sure that your system meets the following requirements for Dynamic File Services:

- Chapter 3, "Planning for Dynamic File Services Pairs and Policies," on page 29
- Section 4.1, "Planning the Installation," on page 39

Consider the additional requirements in this section when installing and setting up DynamicFS in a Windows cluster.

5.1.1 Windows Cluster

The operating system used in the Windows cluster must be one of the supported Windows Server operating systems listed in Section 4.1.1, "Supported Platforms," on page 40.

IMPORTANT: For information about Windows cluster requirements, refer to the official Microsoft documentation in the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/default.aspx).

5.1.2 Shared Disks

Your Windows cluster must provide shared disks to use for DynamicFS as follows:

- The DynamicFS software and related database and log files must be stored in a folder on a shared disk.
- The primary path and secondary path in a DynamicFS pair must reside on shared drives.
- Each of the shared disks that are used with DynamicFS must be configured so that the disk is assigned the same drive letter on each server in the cluster.
- All shared disks that are used with DynamicFS must be configured in the cluster to fail over in conjunction with the DynamicFS Service.

5.1.3 Destination Folder for Installation

DynamicFS must be installed on each node of the cluster in turn. The destination folder for each installation uses the same path on a shared disk.

5.1.4 Dynamic File Services Group

The Dynamic File Services group must be configured separately on each node in the cluster. The Dynamic File Services group is a local group on each node in the cluster, and is not an Active Directory domain group. Make sure that the users in the Dynamic File Services group have privileges on each of the servers in the cluster.

5.1.5 Dynamic File Services SSL Certificates

When you install DynamicFS on a cluster node, a self-signed certificate is created for the DynamicFS Service on that node. You do not associate the certificate with the DynamicFS Service cluster resource. That is, each node of the cluster has a different self-signed certificate.

When the Management Console connects to a DynamicFS Service cluster resource for remote management, DynamicFS uses the certificate that is configured on the active node in the cluster. You are prompted to accept the certificate for the active server if you have not previously logged in to the DynamicFS Service on that server.

5.1.6 Cluster-Managed Network Shares

Use the Windows cluster administration tool to configure cluster-managed network shares on the primary path of a DynamicFS pair. This allows users to connect to a single share and see the merged file-tree view regardless of the node where the shared primary path currently resides. Workstations must be in the same Active Directory domain to access the cluster-managed network shares.

5.1.7 Dynamic File Services Service

- The DynamicFS Service and other components run only on the active node in a cluster.
- Instead of using the DynamicFS Service Controller menu to start or stop the service, use the Windows cluster administration tool to take the DynamicFS Service cluster resource offline and to bring it online.

5.1.8 Dynamic File Services Service Cluster Resource

The DynamicFS Service cluster resource should include all of the resources that are needed for DynamicFS to run in a cluster, such as:

- A unique IP address for the cluster resource
- The DynamicFS Service application (`DswService.exe`)
- The shared disk resource that contains the `Dynamic File Services` folder, which contains the DynamicFS pair and policies databases, logs, and program files
- A cluster managed share for the `Dynamic File Services` folder
- The domain-level share (such as SHARENET)
- The shared disk resources that contain the primary paths or secondary paths that will be used in pairs
- The cluster-managed network shares that you create for the primary paths in DynamicFS pairs

Do not add the Dynamic File Services Service Controller and other DynamicFS executable files to the cluster resource.

- The Dynamic File Services Service Controller starts automatically at the beginning of each session when you log in to the active node of the cluster as user in the Dynamic File Services group (or as the Administrator user on that node).
- Other DynamicFS executable files are automatically called from the DynamicFS Service.
- DynamicFS commands can be started manually on the active node by users in the Dynamic File Services group (or as the Administrator user on that node).

5.1.9 Dynamic File Services Service Dependencies

Specify dependencies for the DynamicFS Service so that it is not started until the related resources are started and available. DynamicFS requires that the cluster group IP address, cluster disk drives, and shares are mounted and available when the DynamicFS Service begins.

5.2 Installing and Setting Up Dynamic File Services in a Cluster

You must install Dynamic File Services on each node in turn in order to lay down the information that is stored locally on each server. Specify the same path for the destination folder on a shared drive when you install on each node.

IMPORTANT: The Windows cluster configuration, management, terminology, and tools can vary depending on the version of Windows Server you are running and on how you set up your cluster and cluster resources. Adjust the instructions in this section as needed for your cluster environment.

For all issues related to Windows cluster configuration and management, see the official Microsoft documentation for your Windows Server operating system in the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/default.aspx).

The following installation description assumes a two-node failover cluster with servers named Node1 and Node2. Modify the procedure as necessary if you have more nodes.

5.2.1 Installing and Setting Up Dynamic File Services on Node1

Use the following procedure to install and set up DynamicFS on the currently active node (Node1).

1 Log in to Node1 as the Administrator user (or as a user with Administrator privileges).

2 Use the Windows cluster administration tool to create a cluster disk resource for the drive where you want to install the DynamicFS software, such as `S:\`.

3 Install DynamicFS by using the *Custom* option, and specify the *Destination folder* as a path on the shared drive. You can also specify the port and firewall settings.

   For example, specify the *Destination folder* as `S:\Dynamic File Services`.

   For detailed instructions, see Section 4.2, "Installing Dynamic File Services with the InstallShield GUI," on page 44.

4 Set up the DynamicFS administrator users for Node1 by adding their usernames as members of the Dynamic File Services group.

   For information, see Section 6.1, "Adding or Removing Members in the Dynamic File Services Group," on page 61.

   IMPORTANT: You later assign the same users to the Dynamic File Services group on each node.

   ---

5 Stop the DynamicFS Service and Service Controller:

   5a Log in as the Administrator user or as a user with Administrator privileges in the Dynamic File Services group.

5b Right-click the *Dynamic File Services Service Controller* icon in the notification area, then select *Stop service* to disable the DynamicFS Service.

5c Right-click the *Dynamic File Services Service Controller* icon in the notification area and verify that the DynamicFS Service status is *Service Disabled*.

5d Right-click the *Dynamic File Services Service Controller* icon in the notification area, then select *Exit*.

6 Delete the `Dynamic File Services` folder in the custom install path on the shared drive, but do not delete the DynamicFS system settings, and do not uninstall DynamicFS.

7 Continue with

5.2.2 Moving the Shared Drive from Node1 to Node2

1 On Node1, use the Windows cluster administration tool to move the shared drive from Node1 to Node2.

2 Make sure that the same drive letter is used to mount the shared disk on Node2 that was used for Node1, such as `S:\`.

3 Continue with

5.2.3 Installing and Setting Up Dynamic File Services on Node2

Use the following procedure to install DynamicFS on the currently active node (Node2).

1 Log in to Node2 as the Administrator user (or as a user with Administrator privileges).

2 Install DynamicFS by using the *Custom* option, and specify the *Destination folder* as a path on the shared drive. Specify the same settings for the port and firewall that you used on Node1.

For example, specify the *Destination folder* as `S:\Dynamic File Services`.

For detailed instructions, see

3 Set up the DynamicFS administrator users for Node1 by adding their usernames as members of the Dynamic File Services group.

For information, see

IMPORTANT: Assign the same users to the Dynamic File Services group that you used on Node1.

---

4 (Optional) On Node2, use the Windows cluster administration tool to move the shared drive from Node2 to Node1.

5 Continue with

5.2.4 Configuring a Cluster Resource for the Dynamic File Services Service

Configure cluster resources for the DynamicFS Service and the shared disks that you want to use for pairs and policies. Use the guidelines in Section 5.1, "Planning the Installation in a Windows Cluster," on page 49. When the cluster setup is complete, continue with Section 5.2.5, "Creating Pairs and Policies in a Cluster," on page 57.

IMPORTANT: It is beyond the scope of this guide to provide detailed instructions about Windows cluster resources configuration, management, and best practices. To illustrate the process, this section provides one possible scenario. It also lists some helpful links to clustering topics in the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/default.aspx).

- ◆ "Example: Setting Up a Cluster Resource for Dynamic File Services in a Windows 2003 Cluster" on page 54
- ◆ "Windows Cluster References" on page 56

Example: Setting Up a Cluster Resource for Dynamic File Services in a Windows 2003 Cluster

This section provides one example of how to set up a DynamicFS cluster resource in a two-node Windows Server 2003 failover cluster.

- ◆ "Example Cluster Configuration" on page 54
- ◆ "Configuring the Dynamic File Services Service for Clustering" on page 55

Example Cluster Configuration

The example cluster configuration uses the following setup for a Windows Server 2003 cluster.

Component	Sample Value
First node in the Windows cluster	Node1
Second node in the Windows cluster	Node2
Domain share	`SHARENET`
Cluster drive resource for DynamicFS program files, databases, and log files	`S:\`
Install destination path	`S:\Dynamic File Services`
Share for the `S:\Dynamic File Services` path	`DYNAMICFS_SHARE` `\\SHARENET\DYNAMICFS_SHARE`
Cluster drive resource for a primary path The same drive is used for the `Dynamic File Services` folder.	`S:\`
Cluster drive resource for a secondary path	`T:\`
Primary path for `DATA_PAIR`	`S:\DATA`

Component	Sample Value
Secondary path for `DATA_PAIR`	`T:\Secondary\DATA`
Share for `S:\DATA`, which will be used as the primary path for `DATA_PAIR`	`DATA_SHARE` `\\SHARENET\DATA_SHARE`
Cluster drive resource for a primary path	`K:\`
Cluster drive resource for a secondary path	`M:\`
Primary path for `PROJECTS_PAIR`	`K:\PROJECTS`
Secondary path for `PROJECTS_PAIR`	`M:\Secondary\PROJECTS`
Share for `K:\PROJECTS`, which will used as the primary path for `PROJECTS_PAIR`	`PROJECTS_SHARE` `\\SHARENET\PROJECTS_SHARE`

Configuring the Dynamic File Services Service for Clustering

1 Use the Windows Cluster Administrator tool to create cluster-managed network shares for the domain, the `Dynamic File Services` folder, and the folders that you plan to use as primary paths in DynamicFS pairs.

For example, in our scenario, we set up the following shares:

Component	Sample Value
Domain share	`SHARENET`
Share for the `S:\Dynamic File Services` path	`DYNAMICFS_SHARE`
Share for `S:\DATA`, which will be used as the primary path for `DATA_PAIR`	`DATA_SHARE`
Share for `K:\PROJECTS`, which will used as the primary path for `PROJECTS_PAIR`	`PROJECTS_SHARE`

2 Use the Windows Cluster Administrator tool to create a `DynamicFS Group` cluster resource where you will later add all of the resources needed to run and use DynamicFS.

3 Use the Windows Cluster Administrator tool to add the following resources in the `DynamicFS Group` cluster resource:

Resource Type	Description
IP Address	A unique IP address for the `DynamicFS Group` cluster resource
Generic Service	The Dynamic File Services Service application (`DswService.exe`)
Physical Disk	The shared disk that contains the `Dynamic File Services` folder where you installed DynamicFS
File Share	A cluster share for the `Dynamic File Services` folder
Domain Share	The domain-level cluster share (such as SHARENET)

Resource Type	Description
Physical Disk	The shared disks that contain the primary paths or secondary paths that will be used in pairs
File Share	The shares that you create for the primary path in each of the DynamicFS pairs

For example, the setup might look like this in the Windows Cluster Administrator tool:
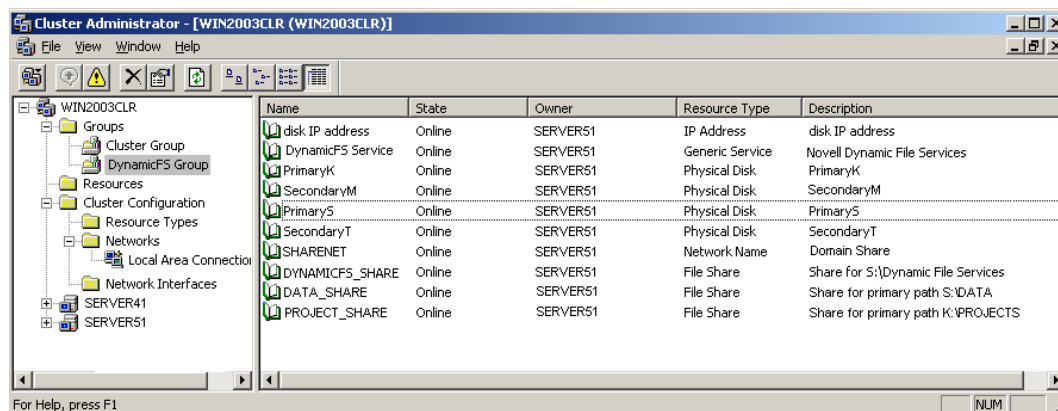
4 Use the Windows Cluster Administrator tool to specify dependencies for the DynamicFS Service cluster resource:

   4a In the `DynamicFS Group` cluster resource, take the DynamicFS Service resource offline.

   4b Open the Properties page for the DynamicFS Service cluster resource, then select the *Dependencies* tab.

   4c Specify the other resources in the `DynamicFS Group` as dependencies for the DynamicFS Service resource.

   The DynamicFS Service resource is not started until all of the other resources in the `DynamicFS Group` are started and are online.

   4d Click *OK* or *Apply* to save your changes.

   4e In the `DynamicFS Group` cluster resource, bring the DynamicFS Service resource online.

5 Use the *Move Group* feature of the Windows Cluster Administrator tool to verify that the `DynamicFS Group` can move between the two nodes, and that the DynamicFS Service starts up automatically after the other resources in the group are available.

Windows Cluster References

The Microsoft references listed in this section might be helpful in using the Windows cluster administration tool to set up the DynamicFS Service resource:

Windows Server 2008 Cluster

- *Failover Clusters* (http://technet.microsoft.com/en-us/library/dd197477(WS.10).aspx)

- *Configure a Service or Application for High Availability* (http://technet.microsoft.com/en-us/library/dd197590(WS.10).aspx)
- *Add a Resource to a Clustered Service or Application* (http://technet.microsoft.com/en-us/library/dd197494(WS.10).aspx)
- *Create a Shared Folder in a Clustered File Server* (http://technet.microsoft.com/en-us/library/dd197480(WS.10).aspx)
- *Verify the Configuration and Failover of a Clustered Service or Application* (http://technet.microsoft.com/en-us/library/dd197543(WS.10).aspx)
- *<Resource> Properties: Dependencies Tab* (http://technet.microsoft.com/en-us/library/cc772430.aspx)
- *Managing a Failover Cluster* (http://technet.microsoft.com/en-us/library/cc731618.aspx)

Windows Server 2003 Cluster

- *Windows Clustering* (http://technet.microsoft.com/en-us/library/cc757731%28WS.10%29.aspx)
- *Checklist: Creating a New Group* (http://technet.microsoft.com/en-us/library/cc780721(WS.10).aspx)
- *Checklist: Creating a New Resource* (http://technet.microsoft.com/en-us/library/cc757479(WS.10).aspx)
- *Checklist: Installing Server Cluster Resources* (http://technet.microsoft.com/en-us/library/cc736636(WS.10).aspx)
- *Setting Resource Properties* (http://technet.microsoft.com/en-us/library/cc783522(WS.10).aspx)
- *Manage Server Cluster Groups* (http://technet.microsoft.com/en-us/library/cc780778(WS.10).aspx)
- *Manage Resources* (http://technet.microsoft.com/en-us/library/cc787285(WS.10).aspx)

5.2.5 Creating Pairs and Policies in a Cluster

After the DynamicFS Service has been set up as a cluster resource, use the Management Console to connect to its cluster resource IP address to create 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.

For information about creating DynamicFS pairs and policies, see:

- Chapter 8, "Creating and Managing Dynamic File Services Pairs," on page 83
- Chapter 9, "Creating and Managing Dynamic File Services Policies," on page 93

5.3 Using Dynamic File Services in a Windows Cluster

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

This section describes known issues for using DynamicFS in an Windows cluster.

5.3.1 Dynamic File Services Management Console

When you use the Management Console to manage the DynamicFS 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 you create 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.

5.3.2 Dynamic File Services Service Controller

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

5.3.3 Dynamic File Services Service and Executable Files

The DynamicFS Service is started automatically by the Windows cluster management tool when it brings the DynamicFS Service cluster resource online. The DynamicFS 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, not the DynamicFS Service controller.

Other DynamicFS executable files are called from the DynamicFS 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.

5.3.4 Dynamic File Services Enforcer 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, ensure that the node's registry contains the right install location.

5.3.5 Moving the Dynamic File Services Service Cluster Resource Between Nodes

Before initiating a non-failover move of the DynamicFS Service cluster resource from the active node to a failover node, make sure that there are no policy runs in progress. You should not issue a cluster move while a policy run is in progress.

If a policy is running 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 DynamicFS Service are unavailable, and users cannot access the files.

If the active node crashes when a policy run is in progress, the DynamicFS Service also crashes. The DynamicFS Service cluster resource immediately goes offline and fails over to the failover node. The following issues must be addressed after the DynamicFS 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 copy of the file that was being moved by a policy is only a sparse file in the target location.

  To resolve this problem:

  1. Run the Pair Synchronization utility on each pair to check for duplicate files in the pairs where the policy was running. For information, see Section 8.9, "Reporting Conflicts for Duplicate Files," on page 91.
  2. For each reported duplicate file conflict, delete the copy of the file in the target location of the policy move.
  3. After all duplicate file conflicts have been resolved, you can start the policy run manually, or let the policy run at its next scheduled time.

5.4 Additional Information

- Chapter 4, "Installing and Setting Up Dynamic File Services," on page 39
- Appendix G, "Silent Install Options for Dynamic File Services," on page 201
- Appendix H, "Using the Uninstall Tool to Modify, Repair, or Remove Dynamic File Services," on page 203
- Appendix I, "Using the Uninstall Tool to Modify, Repair, or Remove Dynamic File Services in a Windows Cluster," on page 207

Configuring and Managing the Dynamic File Services Service

6

This section describes how to configure and manage the Novell® Dynamic File Services (DynamicFS) Service.

6.1 Adding or Removing Members in the Dynamic File Services Group

Dynamic File Services administrators are users who are assigned as members of the Dynamic File Services group. The Administrator user account is automatically allowed to administer DynamicFS, but the Administrator username is not added by default to the Dynamic File Services group. (It is not necessary to explicitly add the Administrator username to the group, but you can add it.) Before a different user can administer the DynamicFS Service, the user's username must be added to the Dynamic File Services group on that computer. The Administrator user or any user with Administrator privileges can add or remove usernames as members of the Dynamic File Services group.

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

2 Open the *Windows Computer Management* dialog box.

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

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

- **Add a member:** Click *Add*, then use the *Enter the object names to select* field to specify the users you want to manage DynamicFS on that server.
- **Remove a member:** Select a username from the list, then click *Remove*.

5 Click *OK* to save and apply your changes, then click *OK* to close the *Properties* dialog box.

6.2 Starting and Stopping the Dynamic File Services Service

The Dynamic File Services Service is the engine that manages the various components. It starts automatically after the install and on system boot, and it runs in the background. You can also start and stop the DynamicFS Service without rebooting by using the Dynamic File Services Service Controller.

IMPORTANT: The DynamicFS Service must be installed and running on the server in order to connect to the server from the Management Console, commands, or utilities.

- Section 6.2.1, "Viewing the Status of the Dynamic File Services Service," on page 62
- Section 6.2.2, "Starting the Dynamic File Services Service," on page 62
- Section 6.2.3, "Stopping the Dynamic File Services Service," on page 62

6.2.1 Viewing the Status of the Dynamic File Services Service

1 Log in to the DynamicFS server as the Administrator user or as a user that is a member of the Dynamic File Services group.

2 In the desktop notification area, right-click the *Dynamic File Services Service Controller* icon to display the menu.

3 View the status of the DynamicFS 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 disabled* and *Start service*

6.2.2 Starting the Dynamic File Services Service

1 Log in to the DynamicFS server as the Administrator user or as a user that is a member of the Dynamic File Services group.

2 Right-click the *Dynamic File Services 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 *Dynamic File Services Service Controller* icon in the notification area. In the pop-up menu, the options are now *Service enabled* and *Stop service*.

6.2.3 Stopping the Dynamic File Services Service

The DynamicFS Service must not be stopped while scanning or moving files. Before you attempt to stop the DynamicFS Service, wait until all DynamicFS policies on the server are in the *Idle* state, or manually stop any policy runs that are in progress by using the *Actions > Stop running process* option from the pair's Statistics dialog box.

1 Log in to the server as the Administrator user or as a user that is a member of the Dynamic File Services group.

2 Verify that all policies on the server are in the *Idle* state.

    2a Open the DynamicFS Management Console.

    2b Under the server, select its *Policies* folder to view a list of policies and their current status.

    2c Make sure all policies are in the *Idle* state.

    2d If necessary, wait until policy runs are completed, or manually stop the policy runs by using the *Actions > Stop running process* option from the pair's Statistics dialog box.

3 Right-click the *Dynamic File Services Service Controller* icon in the notification area, then select *Stop service*.

4 (Optional) Verify that the service has stopped by right-clicking the *Dynamic File Services Service Controller* icon in the notification area. In the pop-up menu, the options are now *Service disabled* and *Start service*.

6.3 Accessing the Dynamic File Services Service Controller

The Dynamic File Services Service Controller runs by default when the Administrator user (or a member of the Dynamic File Services Administrator Group) logs in to a server where the Dynamic File Services Service is running. The DynamicFS Service Controller icon is displayed in the desktop notification area.

Use the Service Controller menu to access the following management tools and information:

- Management Console
- Repair Tool
- Windows Firewall Access
- Service Port Access
- Certificate Configuration
- About

You can also use the Service Controller menu to view the current Service status or to start or stop the Service. For information, see Section 6.2, "Starting and Stopping the Dynamic File Services Service," on page 62.

For information about accessing, starting, or stopping the Service Controller, see the following sections:

- Section 6.3.1, "Accessing the Dynamic File Services Service Service Controller Menu," on page 64
- Section 6.3.2, "Automatically Starting the Dynamic File Services Service Controller," on page 64
- Section 6.3.3, "Manually Starting the Dynamic File Services Service Controller," on page 64
- Section 6.3.4, "Stopping the Dynamic File Services Service Controller," on page 65

6.3.1 Accessing the Dynamic File Services Service Service Controller Menu

The DynamicFS Service Controller icon is displayed in the desktop notification area (the lower right corner of the computer screen).

1 Right-click the Dynamic File Services Service Controller icon to view the menu.
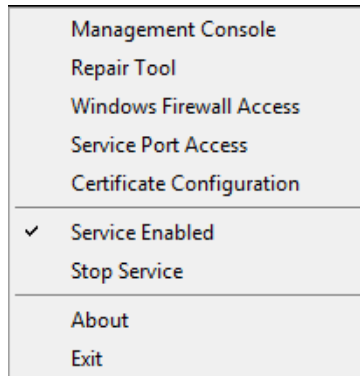
6.3.2 Automatically Starting the Dynamic File Services Service Controller

The Dynamic File Services Service Controller starts automatically when the Administrator user or a member of the Dynamic File Services Administrator Group logs in to the desktop of a computer where the DynamicFS Service is installed and running.

6.3.3 Manually Starting the Dynamic File Services Service Controller

If the Dynamic File Services Service Controller is not running (its icon is not displayed in the notification area), you can start it manually.

1 Log in to the DynamicFS server as the Administrator user or as a user who is a member of the Dynamic File Services group.

If the DynamicFS Service is running, the Service Controller starts automatically and the icon appears in the notification area. If it does not start, continue with Step 2.

2 Start the DynamicFS Service:

2a If necessary, log out, then log in as the Administrator user or as a user with Administrator privileges who is a member of the Dynamic File Services group.

2b In the Windows Computer Management tool, verify that the DynamicFS Service is stopped.

2c Select the DynamicFS Service, then click *Actions > Start* to restart the service.

You can also start the service by double-clicking the `DswService.exe` file in the folder where you installed the DynamicFS software.

2d If you are prompted for credentials by the Windows User Access Control, provide the username and password of the Administrator user or a user with Administrator privileges in the Dynamic File Services group.

3 Start the Dynamic File Services Service Controller:

    3a Start the controller by double-clicking the `DswServiceController.exe` file in the folder where you installed the DynamicFS software.

    3b If you are prompted for credentials by the Windows User Access Control, provide the username and password of the Administrator user or a user with Administrator privileges in the Dynamic File Services group.

6.3.4 Stopping the Dynamic File Services Service Controller

Dynamic File Services Service runs independently of the Dynamic File Services 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 of the Dynamic File Services Service at that time.

1 Right-click the *Dynamic File Services Service Controller* icon in the Windows notification area.

2 Select *Exit*.

6.4 Accessing the Dynamic File Services Management Console

The Dynamic File Services Management Console is a GUI-based management tool that allows you to configure and manage DynamicFS pairs and policies on servers in the same local area network.

You can manage DynamicFS pairs and policies on multiple servers by using the Management Console on any server or workstation where the Management Console is installed. Each server's pairs and policies are unique to that server, and the related configuration files are stored locally on that server. The pair and policy configuration files are stored by default in the `C:\Program Files\Dynamic File Services` directory (or the directory where you installed DynamicFS) on the server being managed. This directory also contains the history and statistics information about policy runs for the server being managed.

When you installed DynamicFS, a *Management Console* icon was placed on the desktop and in the *Start* menu under *Dynamic File Services > Dynamic File Services Management Console*.

1 Log in to the server as the Administrator user or as a user that is a member of the Dynamic File Services group.

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

    ◆ Double-click the *Dynamic File Services Management Console* icon on the desktop.

    ◆ In the *Start* menu, select *All Programs > Dynamic File Services > Dynamic File Services Management Console*.

    ◆ Right-click the *Dynamic File Services Service Controller* icon in the notification area of the desktop, then select *Management Console*.

The Management Console provides four configuration wizards:

Wizard	Description	For Information
Server Wizard	Use to set up the login identity and credentials of a DynamicFS server that you want to manage.	Section 7.1, "Setting Up a Server in the Management Console," on page 75
Setup Wizard	Use to create a pair, a policy, and associate them at create time.	Section 8.2.3, "Using the Setup Wizard to Create a Pair," on page 87
Pair Wizard	Use to configure a pair on a specified server, and associate it with none, one, or multiple policies.	Section 8.2.2, "Using the Pair Wizard to Create a Pair," on page 85
Policy Wizard	Use to configure a policy on a specified server, and associate it with none, one, or multiple pairs.	Section 9.2, "Creating a Policy," on page 97

6.5 Configuring the Dynamic File Services Service Port

The Dynamic File Services Service uses port 8999 by default for remote communications between the Management Console (or DynamicFS commands) being run on one computer and the DynamicFS 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. If a remote connection is in progress when the port is changed, the remote Management Console session must disconnect from the server, then reconnect with the new port.

1 Log in to the server as the Administrator user or as a user that is a member of the Dynamic File Services group.

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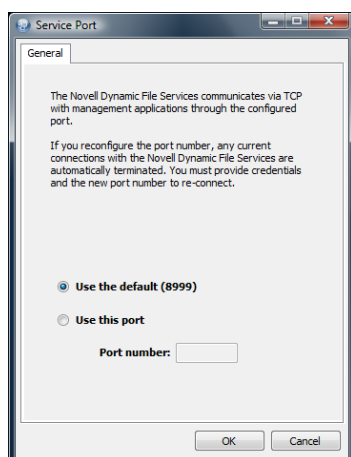
3 Select *Use the default port*, or specify the port number you want to use.

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

5 If necessary, reconnect to continue any in-progress management sessions, and use the new configured port number when logging in.

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

6.6 Enabling or Disabling a Firewall Exception for the Dynamic File Services Service Port

To manage Dynamic File Services pairs and policies on a server from a different computer, you must configure the server to allow DynamicFS communications through its Windows Firewall.

The Windows Firewall allows you to specify exceptions for programs that you want 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 Services Service Controller > Windows Firewall Access* option to control whether a DynamicFS exception is allowed in the firewall.

When you disable the *Windows Firewall Access* option, DynamicFS automatically removes any firewall exceptions from the *Windows Firewall > Exceptions* list that it created for the configured DynamicFS 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.

When you enable the *Windows Firewall Access* option, DynamicFS automatically adds an exception for the configured DynamicFS 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 the DynamicFS Service from another computer through the firewall on the configured service port. You must specify the configured port when connecting to the server.

By default, DynamicFS 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 DynamicFS exception, then selecting *Change Scope*. Alternative manual settings are *My network (subnet) only* and *Custom list*.

IMPORTANT: On Windows Server 2008, DynamicFS creates a firewall exception for the network profiles *Domain* and *Private*. Therefore, 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*.

When *Windows Firewall Access* is enabled, DynamicFS uses TCP communications over the configured port number. If you modify the configured DynamicFS port, DynamicFS automatically updates the firewall exception settings to use the new port. For information about changing the port to use, see Section 6.5, "Configuring the Dynamic File Services Service Port," on page 66.

To enable or disable the firewall exception for the DynamicFS Service port:

1 Log in to the DynamicFS server as the Administrator user or as a user that is a member of the Dynamic File Services group.

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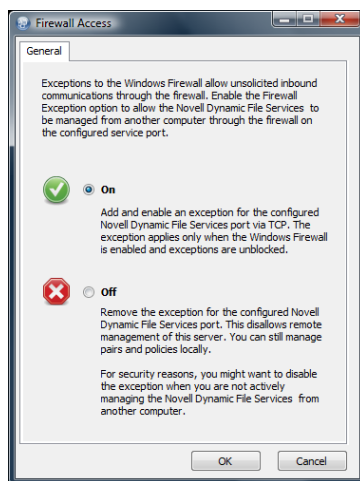
3 In the *Firewall Access* dialog box, select one of the following:

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

   ◆ **Off (not recommended):** Removes the exception for the configured DynamicFS Service port. This disallows remote management of this server. You can still manage pairs and policies locally.

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

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

6.7 Managing a Dynamic File Services SSL Certificate

A Dynamic File Services certificate is required to support SSL sessions between a DynamicFS server and a remote computer running the DynamicFS Management Console. During remote management sessions, the certificate helps assure the client that the server is the intended target. A

self-signed certificate is created automatically during the install. The certificate is automatically bound to the configured DynamicFS Service port (default 8999). The DynamicFS SSL connection uses standard RSA SHA-1 encryption with a 2048-bit key size.

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 Services Service port.
- 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 DynamicFS Service whether a non-self-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 DynamicFS 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 DynamicFS Service port.
DswSSLEnabled	Indicates to the DynamicFS Service whether SSL is enabled or disabled for the configured DynamicFS Service port. Valid values are 0 (disabled) or 1 (enabled). The default value is 1.

This setup is required in order for successful authentication to occur when connecting from the client to the server.

You can also use the *Dynamic File Services Certificate Configuration* option to create a new self-signed SSL certificate, or to specify your own SSL certificate that has been added to the local computer personal store.

6.7.1 Viewing the Dynamic File Services Self-Signed Certificate

You can view the Dynamic File Services self-signed SSL certificate (*servername*-DynamicFileServicesSSLCertificate) after DynamicFS has been installed by using the Certificates snap-in for the Microsoft Management Console (MMC).

1 Log in to Windows 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 certificates you want to manage, then click *Finish* or *Close*.

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

     The `Certificates` directory 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 the *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.

6.7.2 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 if the current certificate is expiring.

1 Log in to the DynamicFS server as the Administrator user (or as a user with Administrator privileges who is also a member of the Dynamic File Services group).

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

For information, see .

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

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

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

A message pops up to confirm whether the configuration succeeded or failed.

6 Click *OK* to dismiss the confirmation message.

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

8 (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:

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.

6.7.3 Configuring a Non-Self-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 certificate authority. Use this option if your enterprise security policy requires this level of security.

Additional steps are required when using a non-self-signed certificate. You must first generate a certificate signing request, import the certificate from the certificate authority into the Local Computer Personal store, then assign the certificate to DynamicFS.

After you have obtained the certificate from the certificate 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 who is also a member of the Dynamic File Services group).

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

For information, see .

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

4 Open the Certificate Configuration dialog box by right-clicking the *Dynamic File Services 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, then click *OK*.

A message pops up to confirm whether the configuration succeeded or failed.

6 Click *OK* to dismiss the confirmation message.

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

8 (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:

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.

6.7.4 Unbinding a Non-Self-Signed Certificate from Dynamic File Services

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

1 Log in to the DynamicFS server as the Administrator user (or as a user with Administrator privileges who is also a member of the Dynamic File Services group).

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

For information, see .

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

4 Open the DynamicFS Certificate Configuration dialog box by right-clicking the *Dynamic File Services 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*, then click *OK*.

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

A message pops up to confirm whether the configuration succeeded or failed.

6 Click *OK* to dismiss the confirmation message.

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

8 (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:

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.

6.7.5 Handling Expiring Certificates

A DynamicFS self-signed SSL certificate is valid for five years from its creation date. As the date of expiration for a configured SSL certificate nears, DynamicFS provides a notification message as you log in to the server from the DynamicFS Management Console. To replace the expiring certificate, use the DynamicFS *Certificate Configuration* option to create a new self-signed certificate, or to set up your own replacement certificate.

6.8 What's Next

  ◆ Configure and log in to a DynamicFS server. For information, see Chapter 7, "Managing Dynamic File Services Servers," on page 75.

  ◆ Configure DynamicFS pairs on the server. For information, see Chapter 8, "Creating and Managing Dynamic File Services Pairs," on page 83.

  ◆ Configure DynamicFS policies to run on the pair. For information, see Chapter 9, "Creating and Managing Dynamic File Services Policies," on page 93.

  ◆ Monitor the health and history of server disks that are used in pairs, the pairs, and the policies. For information, see Chapter 10, "Monitoring Dynamic File Services Pairs and Policies," on page 119.

Managing Dynamic File Services Servers

7

The Novell® Dynamic File Services (DynamicFS) servers can be managed locally or remotely by using the DynamicFS 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 DynamicFS Service is installed. The console can be running on the same computer or a different computer. For information about how to open the console, see Section 6.4, "Accessing the Dynamic File Services Management Console," on page 65.

The list of configured servers is stored in the `Local Application Data` folder for the currently logged-in user on the computer where the Management Console is running.

On Windows XP and Windows Server 2003 computers, the location is:

`C:\Documents and Settings\`*`username`*`\Local Settings\Application Data\Dynamic File Services\DswUIServers.xml`

On Windows Vista, Windows 7, and Windows Server 2008 computers, the location is:

`C:\Users\`*`username`*`\AppData\Local\Dynamic File Services\DswUIServers.xml`

If different administrator users log in to the same computer to use the Management Console, each user configures a list of servers to manage. You can use the import and export features of the Management Console to share a single server list. For information, see Section 7.6, "Exporting and Importing a Dynamic File Services Server List," on page 81.

7.1.1 Prerequisites for Connecting to the Dynamic File Services Server

The DynamicFS Service must be installed and running on the server in order to connect to it. For information, see Section 6.2, "Starting and Stopping the Dynamic File Services Service," on page 62.

In order to connect to a DynamicFS server that you want to manage, you must be able to provide the following information:

*   **Administrator User or a Member of the Dynamic File Services Group:** You must log in 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 6.1, "Adding or Removing Members in the Dynamic File Services Group," on page 61.

*   **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 destination server. The default is port 8999.

    For information about modifying the configured port, see Section 6.5, "Configuring the Dynamic File Services Service Port," on page 66.

    For remote management, the configured DynamicFS Service port must have an exception for it enabled in the Windows Firewall on the destination server. For information, see Section 6.6, "Enabling or Disabling a Firewall Exception for the Dynamic File Services Service Port," on page 67.

7.1.2 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 Log in to a server or client where the Management Console is installed as the Administrator user or as a user that is a member of the Dynamic File Services group on that machine, then access the Dynamic File Services Management Console.

2 In the Management Console, select *Servers* in the left panel, then click *Actions > Server Wizard*.
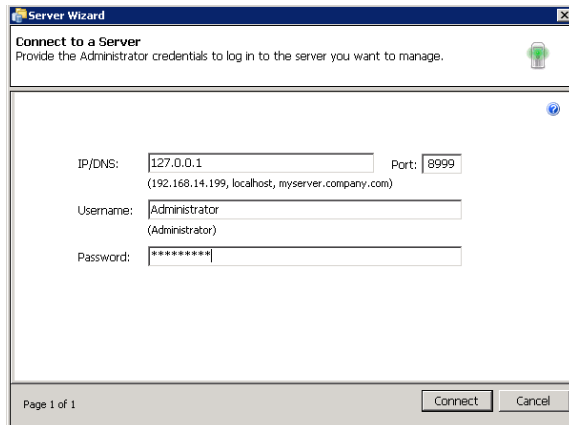
3 In the Server Wizard, provide the credentials of a user in the Dynamic File Services group (or the credentials of the Administrator user) on the Dynamic File Services server that you want to manage.

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 DynamicFS pair. The IPv4 format is supported for the IP address. DNS names are case sensitive.
Username	Type the username of a user with Dynamic File Services group privileges (or the Administrator user) on the destination 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 DynamicFS Service port is 8999.

4 Click *Connect* to connect to the server.

5 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 .

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 who manages DynamicFS on the target server is prompted to accept the certificate when connecting for the first time to the server.

7.2.1 Importing a Certificate to the Default Location

By default, the SSL certificate is imported to the Current User Personal Computer Store.

1 In the *DynamicFS 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 *DynamicFS 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 *DynamicFS 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* dialog box, 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 *DynamicFS Certificate Validation* dialog box.

7.3 Connecting to a Dynamic File Services Server

After you set up a Dynamic File Services server to be managed, you can connect to it by using the Management Console whenever you want to manage pairs or policies for the server.

1 Log in as the Administrator user or as a user that is a member of the Dynamic File Services group, then access the DynamicFS Management Console.

2 In the Management Console, select the server you want to manage.

3 Use either of the following methods to connect to the server:

- Right-click the server and select *Connect*.

- Select the server then select *Actions > Connect*.

4 If the configured DynamicFS Service port has changed on the server, specify the configured port.

5 Specify the username and password of a user in the Dynamic File Services group (or the credentials of the Administrator user) on the server, then click *OK*.

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

7.4 Disconnecting from a Dynamic File Services Server

You can disconnect the Dynamic File Services Management Console from the target servers when you are not actively monitoring or managing the DynamicFS Service on those servers. You might also need to disconnect from the server in order to reconnect to it if the connection is broken for other reasons, such as if the service is disabled or the port is reconfigured on the target server.

1 Log in as the Administrator user or as a user that is a member of the Dynamic File Services group, then right-click the *Dynamic File Services Service Controller* icon and select *Management Console*.

2 In the Management Console, select the server you want to manage.

3 Use either of the following methods to disconnect from the server:

- Right-click the server and select *Disconnect*.

- Select the server, then select *Actions > Disconnect*.

When the server is disconnected, the *DynamicFS Server* icon is dimmed.

7.5 Viewing Server Properties

1 In the Dynamic File Services Management Console, connect to the server you want to manage.

2 Right-click the server, then select *Properties*.

3 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.

Property	Description
Computer	Server processor and RAM on the server.
Version	The release version of Dynamic File Services.
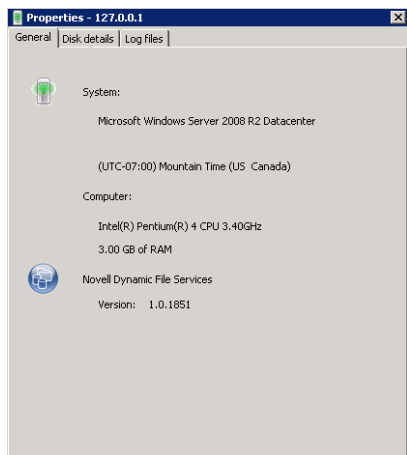
4 Select the Disk Details tab to view a list of disks on the server and the Used Space, Free Space, and Capacity of each disk.
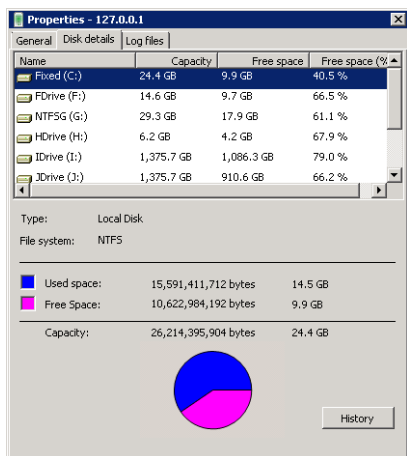
5 Select the Log Files tab to view log information for the Dynamic File Services Service component (`DswMpcCore.log`) or the Enforcer component (`DswEnforcer.log`).
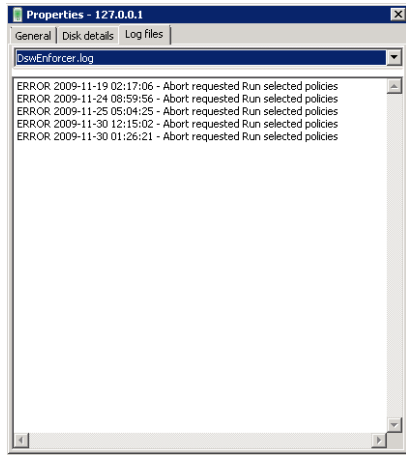
7.6 Exporting and Importing a Dynamic File Services Server List

Dynamic File Services allows you to export and import the server configuration to make it easier to set up management on multiple computers. You set up multiple servers in the Management Console on one computer, then export the list of configured servers in an `.xml` file (default name of `DswServersList.xml`). You can import a server list on another computer to automatically set up the servers for management.

- Section 7.6.1, "Exporting a Server List," on page 81
- Section 7.6.2, "Importing a Server List," on page 81

7.6.1 Exporting a Server List

1 Open the Management Console.

2 In the left panel, select the *Servers* container.

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

4 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.

5 Continue with Section 9.11.2, "Importing a Policy," on page 109.

7.6.2 Importing a Server List

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

2 Open the Management Console.

3 In the left panel, 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.

7.7 What's Next

- Configure DynamicFS pairs on the server. For information, see Chapter 8, "Creating and Managing Dynamic File Services Pairs," on page 83.

- Configure DynamicFS policies to run on the pair. For information, see Chapter 9, "Creating and Managing Dynamic File Services Policies," on page 93.

- Monitor the health and history of server disks that are used in pairs, the pairs, and the policies. For information, see Chapter 10, "Monitoring Dynamic File Services Pairs and Policies," on page 119.

Creating and Managing Dynamic File Services Pairs

8

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

8.1 Understanding Dynamic File Services Pairs

A Dynamic File Services pair consists of two separate and independent paths in the file system on an individual server. 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 primary path typically resides on higher performance storage hardware where the best performance can be provided for the most important and most used files. The other path is referred to as the secondary location.

DynamicFS policies allow you optimize the use of your storage by automatically moving data to storage that is best optimized for the data type or frequency of use. You can create one or more policies for a pair to move data between the primary path and secondary path according to your storage needs.

In order to allow users to access the DynamicFS pair and see a merged view of the data, you must use the Microsoft Network Share tool to create a share on the folder that you want to use as the primary path. Users should not have permission to directly access the data as local users of the primary path or secondary path.

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*
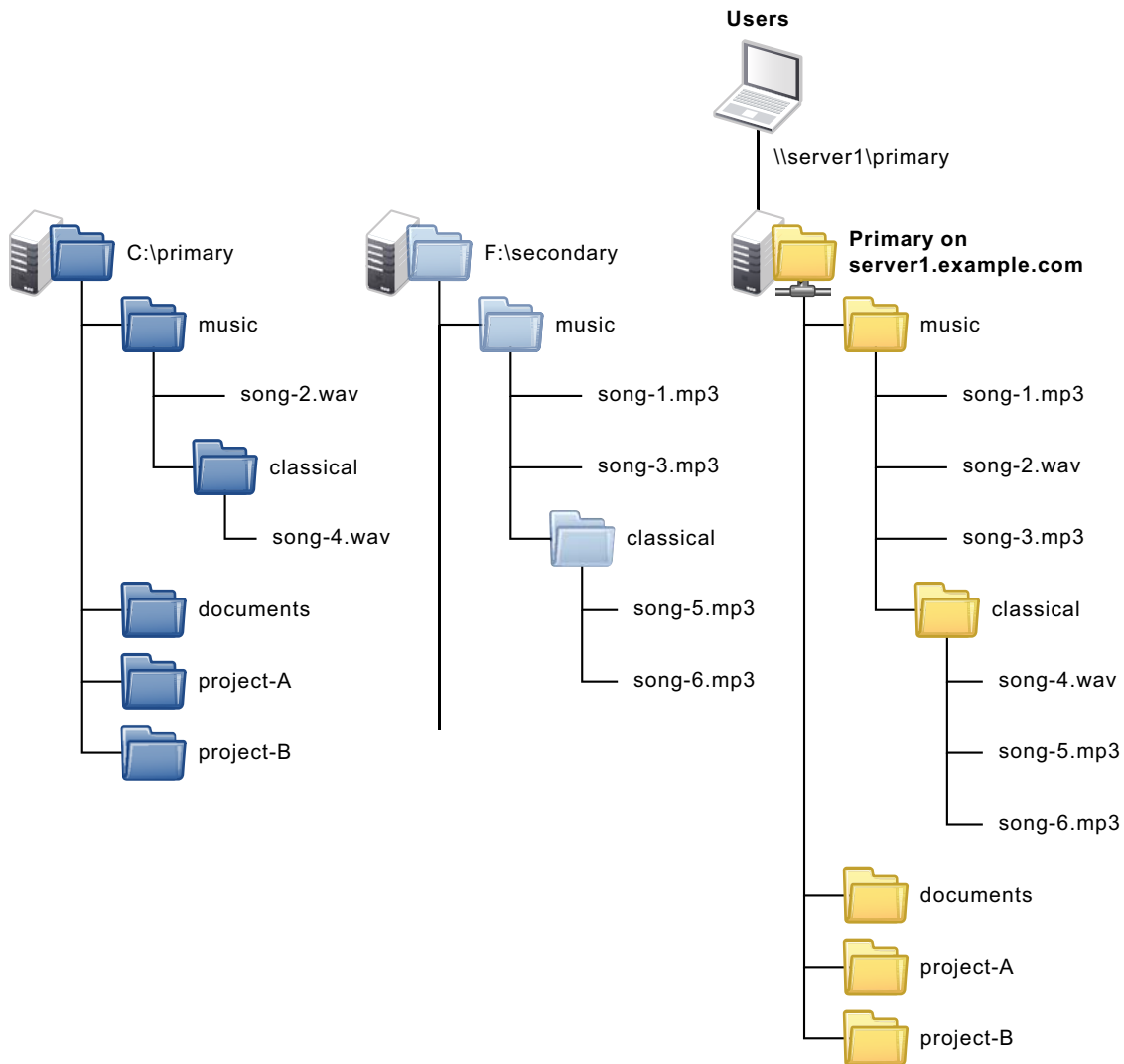
8.2 Creating a Pair

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: The pair must be associated with at least one policy before data can be moved between the primary and secondary areas.

Before you begin, make sure your system meets the requirements in "Prerequisites for Creating a Pair" on page 85. Gather the information you need about the paths that you want to use as the primary path and secondary path.

◆ Section 8.2.1, "Prerequisites for Creating a Pair," on page 85

◆ Section 8.2.2, "Using the Pair Wizard to Create a Pair," on page 85

◆ Section 8.2.3, "Using the Setup Wizard to Create a Pair," on page 87

8.2.1 Prerequisites for Creating a Pair

Before you create a DynamicFS pair, make sure your system meets the following requirements:

◆ The devices must be attached to the server where you want to create the pair. This includes Fibre Channel, iSCSI, and direct attached storage devices.

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

Usually, the secondary path is empty. Both paths can contain data, but if there are duplicate files, only the copy 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 again to users.

No data is moved between the two locations until you set up DynamicFS policies to do so.

◆ All user access to the pair must be through this network share on the primary path. You can add shares above or below the network share on the primary path.

Network shares should not be used for the secondary path. Do not nest shares above or below the secondary path.

8.2.2 Using the Pair Wizard to Create a Pair

The Pair Wizard sets up the DynamicFS pair and allows you to associate it with none, one, or multiple existing properties.

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

2 Use one of the following methods to access the Pair Wizard:

◆ Select *Pairs*, then select *Actions > Pair Wizard*.

◆ Right-click *Pairs*, then select *Pair Wizard*.

3 On the Pair Paths page, browse to select the primary and secondary storage areas on the selected DynamicFS server that you want to use for the new pair, then click *Next* to continue.

Paths used in the pair cannot be nested in this pair or other pairs.
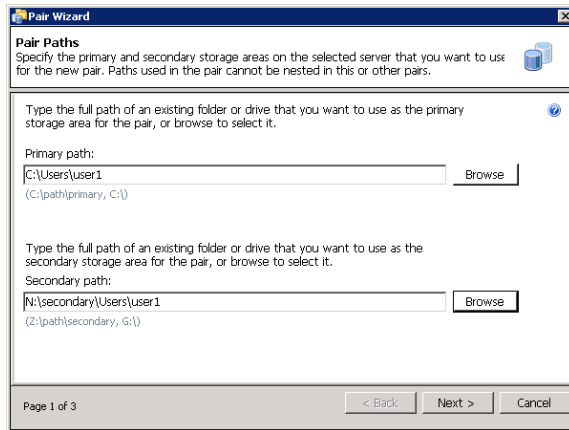
4 If the primary path you specified does not have a network share set up for it, a message pops up to remind you that you must create the share later to give users a merged file tree view of the pair. Click *OK* to dismiss the message.

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

For information, see Section 3.5, "Naming Conventions for Pairs and Policies," on page 31.
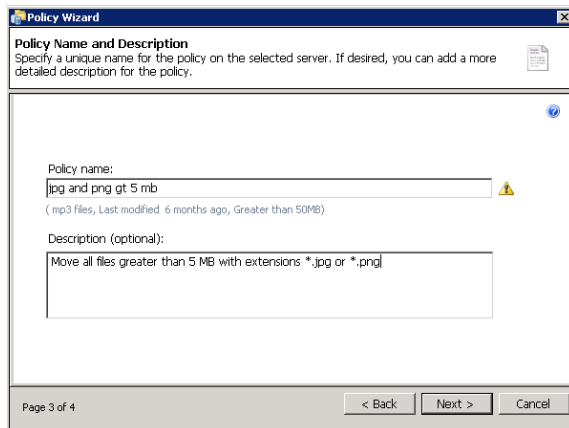
6 On the Pair to Policy Association page, select none, one, or multiple policies to associate with the new pair.
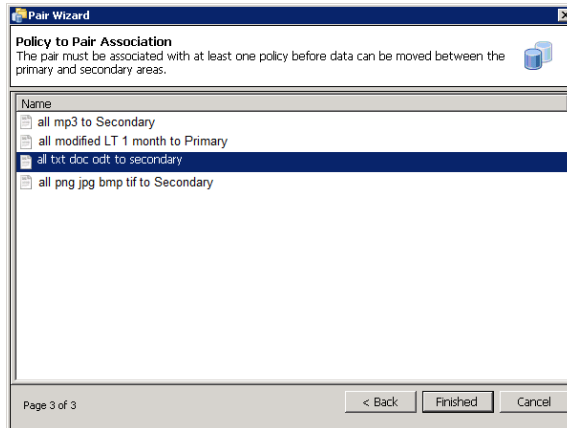
7 Click *Finished* to create the pair.

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

8 (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 Pair," on page 103.

◆ **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 Policy," on page 103.

8.2.3 Using the Setup Wizard to Create a Pair

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

2 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.

3 On the Pair Paths page, browse to select the primary and secondary storage areas on the selected DynamicFS server that you want to use for the new pair, then click *Next* to continue.

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

4 If the primary path you specified does not have a network share set up for it, a message pops up to remind you that you must create the share later to give users a merged file tree view of the pair. Click *OK* to dismiss the message.

5 On the Pair Name page, specify a unique name (up to 32 characters) for the pair on the selected server, then click *Next* to continue.

For information, see Section 3.5, "Naming Conventions for Pairs and Policies," on page 31.

6 On the Create Policy page, create a policy for the pair.

For information about completing the policy fields, see Section 9.2, "Creating a Policy," on page 97.

7 Click *Finish* to create the pair, create the policy, and associate the pair and the policy.

The pair appears in the *Pairs* folders for the server.

The policy appears in the *Policies* folder 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.

8 (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 Pair," on page 103.

- ◆ **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 Policy," on page 103.

8.3 Giving Users Access to Files on a Pair

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 file tree view of the files stored on the pair.

- ◆ A network share is needed on the primary path in order to provide a merged file tree 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.

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 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 Select the *Pairs* folder for the server, then view the list of pairs that are defined.

The *Pairs* list reports the following information for each pair:

- ◆ *Pair name*
- ◆ *Status* (*Idle*, *Running*)

- *Primary Path*
- *Secondary Path*

Click a column heading to sort the list by that parameter.

8.5 Viewing Properties for a Pair

You can view the settings for an existing Dynamic File Services pair in the Pair Properties dialog box.

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 *General* tab in the Pair Properties dialog box reports the following information:

- *Pair name*
- *Primary*
  - *Type* (the device type)
  - *Primary path*
  - *Share name*
- *Secondary*
  - *Type* (the device type)
  - *Secondary path*

The *Associations* tab lists the policies that are currently associated with the pair. For information, see Section 9.5, "Associating or Disassociating Pairs and Policies," on page 102.

The *Include/Exclude* tab identifies any directories in the pair that are either included or excluded from policy runs. For information, see Section 8.6, "Including or Excluding Folders from a Pair's Policy Runs," on page 89.

The *Pair history* tab shows the frequency and time that the pair history scan is run. For information, see Section 8.7, "Scheduling the Pair History Scan," on page 90.

8.6 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*.

8.7 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. By default, the history scan runs once daily at 4:00 a.m. You can configure the scan to run more or less often on a given pair by configuring the 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.

8.8 Reporting Conflicts for Attributes and ACL Permissions on Folders

You should use the merged file tree 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 3.7, "Duplicate Folders," on page 32.

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.

1 Log in to the DynamicFS server as the Administrator user (or as a user with Administrator privileges), then open a *Command Prompt* console.

It does not matter if the user is also a member of the Dynamic File Services group.

2 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.

For information about other options for the `DswSyncPair.exe` command, see Appendix C, "Dynamic File Services Synchronize Pair Utility," on page 181.

8.9 Reporting Conflicts for Duplicate Files

You should always use the merged file tree view when creating, modifying, or deleting files in a Dynamic File Services pair. DynamicFS manages the 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 DynamicFS handles them, see Section 3.8, "Duplicate Files," on page 32.

To identify duplicate file conflicts, you can run the DynamicFS Synchronize Pair tool (`DswSyncPair.exe`) to detect duplicate instances of a file that exist on the primary and secondary paths, and report them.

1 Log in to the DynamicFS server as the Administrator user (or as a user with Administrator privileges), then open a *Command Prompt* console.

It does not matter if the user is also a member of the Dynamic File Services group.

2 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.

For information about other options for the `DswSyncPair.exe` command, see Appendix C, "Dynamic File Services Synchronize Pair Utility," on page 181.

8.10 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*.

8.11 What's Next

- Configure DynamicFS policies to run on the pair. For information, see Chapter 9, "Creating and Managing Dynamic File Services Policies," on page 93.
- Monitor the health and history of server disks that are used in pairs, the pairs, and the policies. For information, see Chapter 10, "Monitoring Dynamic File Services Pairs and Policies," on page 119.

Creating and Managing Dynamic File Services 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. You can assign multiple policies to a pair. A policy can be assigned to multiple pairs.

9.1 Understanding Dynamic File Services Policies

Dynamic File Services policies define what data to move, the direction to move the data, and when to move it. 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 on 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 on 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. DynamicFS 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.

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.)

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, DynamicFS 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 policies are enforced, 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.)

When planning policies for a pair, consider the file types that occur in the pair and how the filter options are enforced. Makes sure that the policies assigned to a pair move files where you expect them to be moved, and 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.

It is important to monitor what files are moved during a policy run by viewing the policy execution history as described in Section 10.2, "Viewing the Policy Execution History for a Pair," on page 120. Use this information to refine the policies as needed to achieve your storage goals.

You must enable and configure at least one of the four filter options in each policy. For examples of how to create policy rules to achieve your storage goals, see Section 9.13, "Examples of Policy Rules," on page 110.

Table 9-2 *Policy Filter Options*

Option	Description
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 extensions	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 extensions. Separate multiple file extensions with a comma and no spaces.
	If you specify other filter options and do not enable *File extensions*, the specified filters to apply to files with any extension.
	The asterisk (*) wildcard character is used to indicate that files with any extension or filename should be moved. However, you cannot specify a filename or characters in a filename to further limit the move by filename.
	For example, you can use either of the following methods to specify extensions:
	`MP3,PNG,JPG`
	`*.mp3,*.png,*.jpg`
	The entries are case insensitive.
	To move all files with extensions, specify "`*.*`" in the *File extensions* field. If you specify other filter options, only files with extensions that also meet the other critera are moved.
	To move files with no extension, specify "`*.`" in the *File extensions* field. If you specify other filter options, only files with no extensions that also meet the other critera are moved.
	To move all files with and without extensions, specify the following in the *File extensions* field:
	`*.*,*.`

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 3.10, "Policy Schedules," on page 33.

If scheduling is enabled, you must specify one of the schedule options. The default is weekly on Sunday at 12:00 a.m.

Table 9-3 *Policy Schedule Options*

Option	Description
Scheduled	Select the *Scheduled* check box to enable the schedule.
	Deselect the Scheduled check box to disable the schedule. Unscheduled policies are not enforced unless you run them manually. You can associate scheduled and unscheduled policies with one or more pairs.
	A policy can be enforced hourly, daily, weekly, or monthly. Select one scheduling option, then specify when to run it.
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*.

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 9-4 *Policy Name and Description Options*

Option	Description
Policy Name	DynamicFS policy names can be up to 32 characters.
	For information about naming restrictions, see Section 3.5, "Naming Conventions for Pairs and Policies," on page 31.
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. A single pair can be associated with multiple policies. A single policy can be associated with multiple pairs.

9.1.6 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. You can use the *Preview Now* option to view the files that would be moved in a run without actually moving any files. You can also inspect the run history for a pair to examine lists that show what files were moved in the last several runs.

9.2 Creating a Policy

Two wizards are available for configuring Dynamic File Services 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 policy runs 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.

For information on the different fields in the policy, see Section 9.1, "Understanding Dynamic File Services Policies," on page 93.

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 84.

- **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 four 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 extensions	Select the check box, then create a rule that moves a file only if its filename uses one of the specified file extensions. Separate multiple file extensions with a comma and no spaces.

3c Click *Next* to continue.

4 On the Policy Schedule page, specify the schedule options:
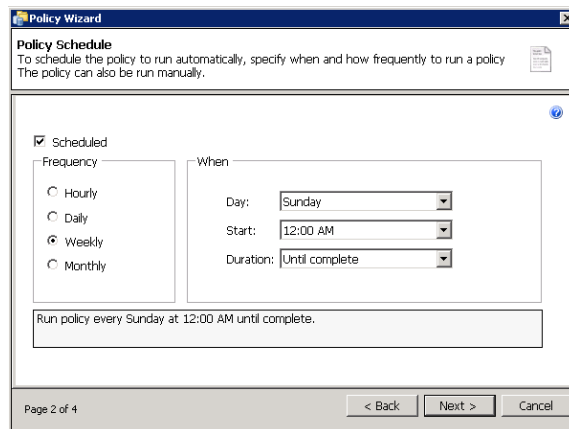
◆ **Not Scheduled:** Deselect *Scheduled* to disable scheduling, then click *Next* to continue.

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.

Option	Description
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.

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.
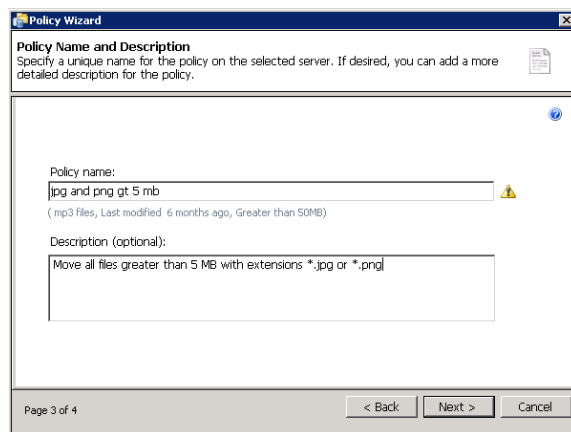
6 On the Pair to Policy Association page, select one or more pairs that you want to associate with this policy.
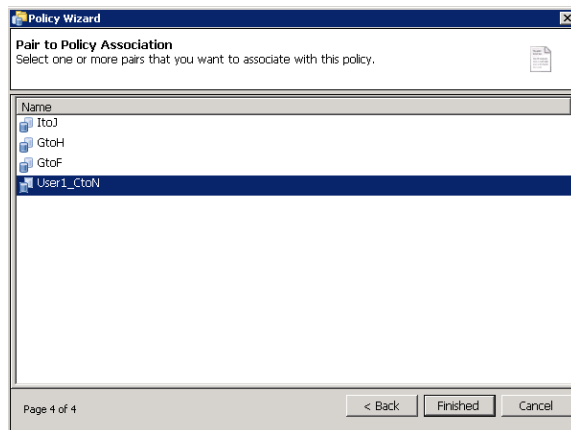
Policies must be associated with at least one pair to be able to run. Policies are enforced only for its associated pairs. If no pairs exist, you can use the Pair Wizard later to create a pair and associate it to the policy. For information about managing pair and policy associations, see Section 9.5, "Associating or Disassociating Pairs and Policies," on page 102.

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 102.

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 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*)

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 Dynamic File Services policy in its Policy Properties dialog box.

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 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*
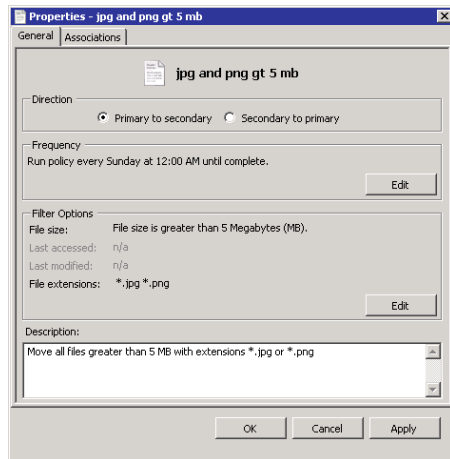
5 View the information on the *Associations* tab.

The *Associations* tab lists the pairs that are currently associated with the policy.
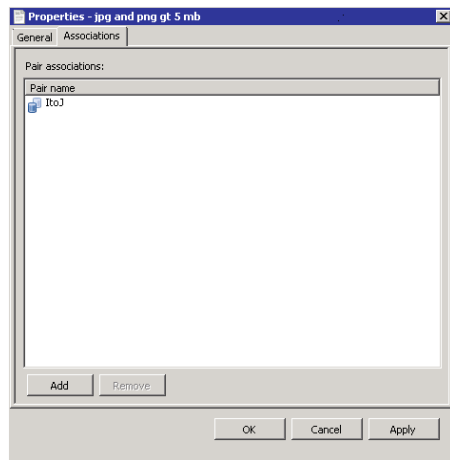
9.5 Associating or Disassociating Pairs and Policies

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.

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 DynamicFS 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 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 Properties dialog box.

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*.

4 Click the *Associations* tab to view a list of the policies that are currently associated with the pair.

9.5.3 Associating or Disassociating Pairs with 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, select the policy and open its Policy Properties page, then select the *Associations* tab.

3 To add pairs to a policy, click *Add*.

A list of all pairs that are defined on the server is displayed in the *Select pairs* dialog box.

4 Select one or more pairs that you want to add to the *Associations* list, then click *OK*.

5 To remove pairs from a policy, select one or more pairs in the *Associations* list that you want to remove, then click *Remove*.

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

The policy is enforced for the selected pairs at the policy's next scheduled run time. You can also run the policy for a pair manually by using the *Execute now* option.

9.5.4 Associating or Disassociating Policies with a Pair

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

2 Under the *Pairs* folder for the server, select the pair and open its Pair Properties page, then select the *Associations* tab.

3 To add policies to a pair, click *Add*.

A list of all policies that are defined on the server is displayed in the *Select policies* dialog box.

4 Select one or more policies that you want to add to the *Associations* list, then click *OK*.

5 To remove policies from a pair, select one or more policies in the *Associations* list that you want to remove, then click *Remove*.

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

The policies are enforced for the selected pair at the each policy's next scheduled run time. You can also run policies for a pair manually by using the *Execute now* option.

9.6 Modifying Policy Rules

Dynamic File Services 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 Dynamic File Services Policies," on page 93.

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 94.

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 extensions	Select the check box, then create a rule that moves a file only if its filename uses one of the specified file extensions. Separate multiple file extensions with a comma and no spaces.

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 105.

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.

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. Table 9-5 describes the behavior of DynamicFS when determining the next scheduled interval for the policy:

Table 9-5 *Determining the Next Scheduled Run Interval*

Run State	Hourly	Daily	Weekly	Monthly
The run is in progress.	The current run completes. The run is scheduled for the next hour.	The current run completes. The run is scheduled for tomorrow at the new time.	The current run completes. The next run is scheduled for the new time and day of the week.	The current run completes. The next run is scheduled for the new time and day of the month.
The run is completed for the current hour or day.	The run is scheduled for the next hour.	The run is scheduled for tomorrow at the new time.	The next run is scheduled for the new time and day of the week.	The next run is scheduled for the new time and day of the month.
The run has not started, and it is within 20 minutes after the scheduled start time.	The next run starts at the current hour if possible. If the pair is busy, the run is scheduled for the next hour.	The run starts as scheduled if possible. If the pair is busy, the run is scheduled for tomorrow at the new time.	The run starts as scheduled if possible. If the pair is busy, the next run is scheduled for the new time and day of the week.	The run starts as scheduled if possible. If the pair is busy, the next run is scheduled for the new time and day of the month.
The run has not started, and it is more than 20 minutes after the scheduled start time.	The run is scheduled for the next hour.	The next run is scheduled for tomorrow at the new time.	The next run is scheduled for the new time and day of the week.	The next run is scheduled for the new time and day of the month.

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.

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 95.

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.
Monthly	Select the *Monthly* check box, then specify the calendar day of the month, the start time, and duration to run the policy.

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 105.

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 107.

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 Policy," on page 103.

9.8 Starting a Policy Run

Dynamic File Services policies run according to the schedule that is configured for the policy. The policy applies to all pairs associated with the policy. You can also run the policy as needed by using the *Execute now* option.

For information about scheduling a policy to run, see Section 9.7, "Modifying Policy Schedules," on page 105.

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.

3 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.

4 Monitor the policy run by viewing the progress in the *Scan Progress* bar.

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 107
◆ Section 9.9.2, "Viewing the Last Run Preview," on page 108

9.9.1 Starting a Policy Preview

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

2 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.

3 When the preview run is completed, open the *Statistics* dialog box, then click *View > Preview results* to open the *Preview* dialog box.

4 In the *Preview* dialog box, 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.

9.9.2 Viewing the Last Run Preview

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 run preview.

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 Dynamic File Services 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 process from running this one time:

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 page and unschedule it. For information, see:

- Section 9.7.3, "Unscheduling a Policy for All Pairs," on page 106
- Section 9.7.4, "Disabling the Schedule for Selected Pairs," on page 107.

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 directory. You can also copy the exported `.xml` file to a different computer and import it there.

- Section 9.11.1, "Exporting a Policy," on page 108
- Section 9.11.2, "Importing a Policy," on page 109

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 Section 9.11.2, "Importing a Policy," on page 109.

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 Section 9.11.1, "Exporting a Policy," on page 108.

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 the Dynamic File Services 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 status of 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 108.

4 After the policy is in the *Idle* state, right-click the policy, then select *Delete*.

9.13 Examples of Policy Rules

The examples in this section can help you understand how to configure Dynamic File Services policy rules to achieve your desired outcome for moving data in a pair:

9.13.1 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 extensions are not considered.

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 extensions	Not selected.

9.13.2 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.

Option	Setting
Direction	Primary to secondary

Option	Setting
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 extensions	Select the check box, then specify `*.mp3` in the field.

9.13.3 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.

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 extensions	Select the check box, then specify `*.mp3` in the field.

9.13.4 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.

Option	Setting
Direction	Primary to secondary
File size	Not selected.

Option	Setting
Last accessed	Not selected.
Last modified	Not selected.
File extensions	Select the check box, then specify `*.*,*.` in the field to move all files with and without file extensions.

9.13.5 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 112
- ◆ "Move Files That Were Last Accessed Less than 1 Week Ago from Secondary to Primary" on page 113

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.

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 extensions	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.

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 extensions	Not selected.

9.13.6 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

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.

Option	Setting
Direction	Primary to secondary
File size	Not selected.

Option	Setting
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 extensions	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.

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 extensions	Not selected.

9.13.7 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 *.*,*. in the *File extensions* 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.

Option	Setting
Direction	Secondary to primary

Option	Setting
File size	Not selected.
Last accessed	Not selected.
Last modified	Not selected.
File extensions	Select the check box, then specify `*.*,*.` in the field.

9.13.8 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 four 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.

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 extensions	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.

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 extensions	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.

Option	Setting
Direction	Primary to secondary

Option	Setting
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 extensions	Not selected.

9.14 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 Chapter 10, "Monitoring Dynamic File Services Pairs and Policies," on page 119.

Monitoring Dynamic File Services Pairs and Policies

10

This section discusses how to monitor Novell® Dynamic File Services (DynamicFS) pairs and policies with the statistics and history features.

10.1 Viewing Pair Statistics

The Dynamic File Services Service scans pairs hourly and reports information about them, such as how many files and folders there are and the status of policies assigned to them.

In a pair's Statistics dialog box, the *Pair Status* area reports the following information:

Table 10-1 *Reported Information about the Pair Status*

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.
Files to be moved	Specifies the number of files that are pending being moved.
Total size to be moved	Specifies the combined size of the files that are pending being moved.

In a pair's Statistics dialog box, the *Policies associated to pair* area reports the following information about policies associated with this pair:

Table 10-2 *Reported Information about Policies Associated to a Pair*

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.

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.

If a scan is currently running, the *Current Status* bar shows activity for that policy run.

3 (Optional) Run one or more policies manually by selecting the policy, then right-clicking and selecting *Execute now*.

To select multiple policies, hold down the Shift key or Control key while selecting policies.

4 (Optional) Test a policy without executing it by selecting the policy, then right-clicking and selecting *Preview now*.

To select multiple policies, hold down the Shift key or Control key while selecting policies.

5 (Optional) Add a new policy association by selecting *Actions > Add policy association*.

6 (Optional) Remove a policy association by selecting the policy, then selecting *Actions > Remove policy association*.

10.2 Viewing the Policy Execution History for a Pair

The Policy Execution History provides information about the most-recent 16 runs of policies on the Dynamic File Services 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.

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 a given 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 and to view information about each one.
Policies executed	The *Policies executed* area lists the policies that were enforced in that run.

Statistic	Description
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.
Total files moved Total files failed to move	The *Total files moved* and *Total files failed to move* fields provide links that open the *Run History* dialog box, where you can view a list of the files in that category. It provides the file path, extension, and size information for each file. The list is paged to show 1000 files at a time. Use the left-arrow and right-arrow to move between pages. On each page, scroll down to see the 1000 filenames listed. Click the heading of a column to sort the list by filename, extension, or size. 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.

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 Under the *Pairs* folder, double-click the pair name to open the Statistics dialog box, then select the *Pair execution history* tab.
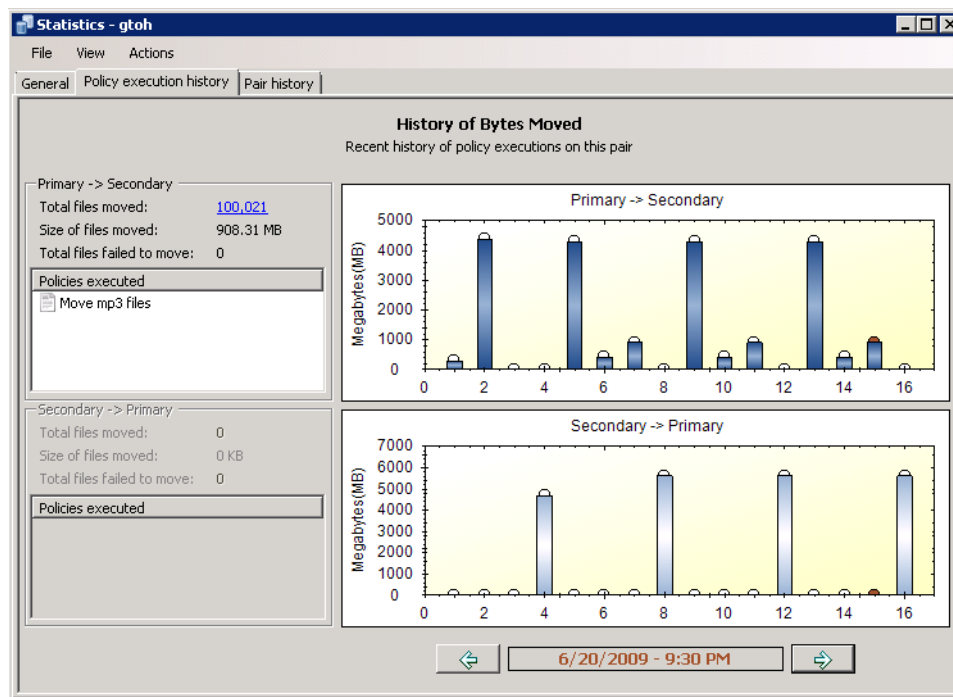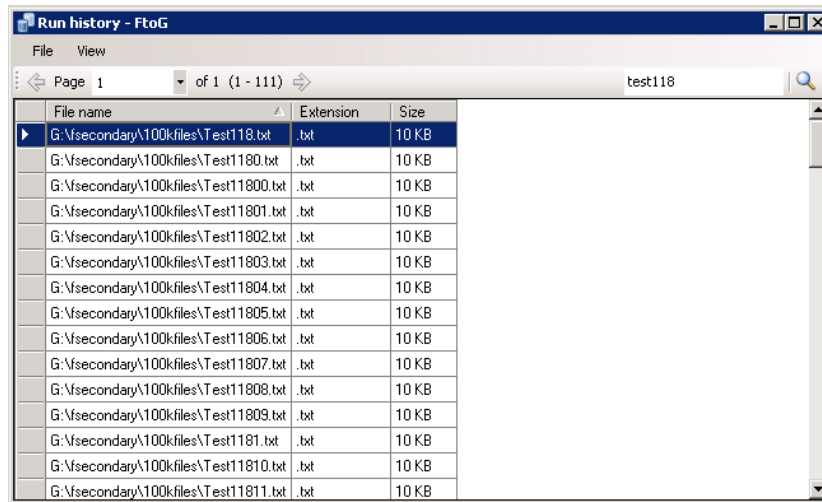
3 In the *Date and Time* area at the bottom of the dialog box, use the left-arrow and right-arrow to select the run you want to explore.

The selected run is highlighted with a red disk at the top of its bar in the graph.

4 View the summary on the left that shows the policies that were run and the number of files that were moved or not moved.

5 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.

The list has 1000 files listed per page. Use the scroll bar to scroll through the 1000 entries. Use the *Page* arrows to page through the list pages. Click the heading of a column to sort the list by filename, extension, or size. You can filter the results by typing a sequence of letters or numbers, then clicking the search icon.

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".

File name	Extension	Size
G:\fsecondary\100kfiles\Test118.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test1180.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11800.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11801.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11802.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11803.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11804.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11805.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11806.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11807.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11808.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11809.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test1181.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11810.txt	.txt	10 KB
G:\fsecondary\100kfiles\Test11811.txt	.txt	10 KB

Run history - FtoG — File   View — Page 1 ▼ of 1 (1 - 111) — test118

6 Click the link for *Total files failed to move* open the *Run History* dialog box where you can view a list of the files that should have moved in a particular direction, but did not move.

The list has 1000 files listed per page. Use the scroll bar to scroll through the 1000 entries. Use the *Page* arrows to page through the list pages. Click the heading of a column to sort the list by filename, extension, or size. You can filter the results by typing a sequence of letters or numbers, then clicking the search icon.

10.3 Viewing the Pair History

The Pair History shows the amount of space consumed over time on the devices in a Dynamic File Services pair by the files and folders in the primary and secondary location. 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 8.7, "Scheduling the Pair History Scan," on page 90.

For information about the storage status and history for the disks that are used in a pair, see Section 10.4, "Viewing Capacity and History for Server Disks," on page 123.

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.

3 Double-click the scan event for the primary (square) or the secondary (circle) 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, select *Total Size* to view the information organized by file size in the categories.

5 In a *Summary* dialog box, select *Number of Files* to view the information organized by number of files in the categories.

6 In a *Summary* dialog box, use the *Graph Option* drop-down box to graph the summary report by the following delimiters:

   - Accessed
   - Creation
   - Modified
   - File Size
   - Extension

7 To compare multiple scan events, double-click each event and view their *Summary* dialog boxes side-by-side.

10.4 Viewing Capacity and History for Server Disks

You can view the server capacity information about the disks on the 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 10.3, "Viewing the Pair History," on page 122) 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 120) to determine how much data is being moved by different policy runs on the pair.

10.4.1 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:

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 file system and capacity information.

5 Select a disk and click *History* to view information about how the total device capacity has changed over time.

10.4.2 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 DynamicFS 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.
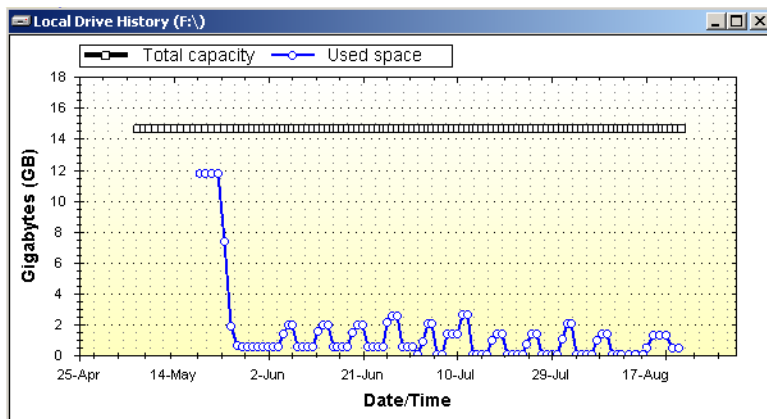
Initially, policies were run daily during non-peak traffic times on each pair to move files by type, size, or date last accessed or modified from the primary disk to a secondary disk (not pictured). Thereafter, the policy schedule was modified to run weekly during non-peak traffic times to move any new files that match the specified criteria from the primary disk to the secondary disk.

10.4.3 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 DynamicFS pairs. Initially, the disk contained little or no data. Over time, the disk capacity is being consumed by files that are moved by DynamicFS policies from primary paths on one or more other disks (not pictured) to their secondary paths on this disk.
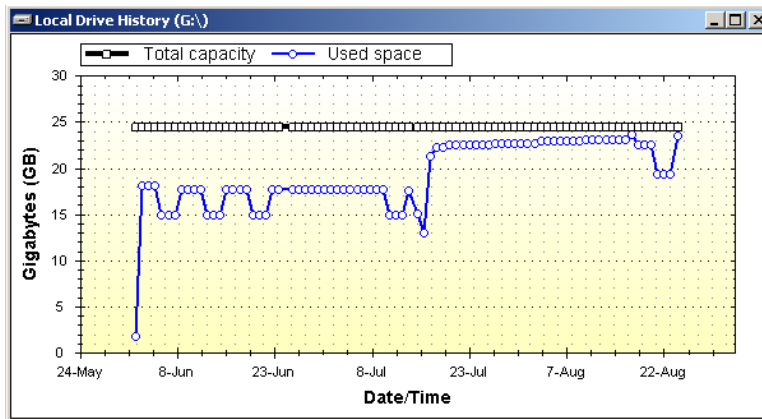
Because the disk capacity is near its maximum, you might need to take one or more of the following actions:

- 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 10.3, "Viewing the Pair History," on page 122) 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 120) 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.

10.5 Viewing Logged Events for the Service and Enforcer

Event logs for the Dynamic File Services Service and Enforcer components are available in the Management Console.

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 to view the following log files:

Log File	Description
DswMpcCore.log	Event log for the DynamicFS Service.
DswEnforcer.log	Event log for the DynamicFS Enforcer component that runs policies.

10.6 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/default.aspx) for documentation on viewing events with the Event Viewer snap-in for the Microsoft Management Console (MMC).

10.7 Auditing Management Events

Auditing the management events for the Dynamic File Services 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 DynamicFS management operations, such as create, delete, and modify (which includes association and disassociation of the policies with pairs).

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. No sensitive information is placed in the audit log. Both authorized and unauthorized attempts for management events are logged.

The audit log also reports when the DynamicFS Service is stopped and started.

The audit file is protected so that it cannot be deleted or accessed by unauthorized users.

The audit log and configuration files are by default located in the Dynamic File Services\audit folder where you installed DynamicFS:

```
C:\Program Files\Dynamic File Services\audit\DswAuditLog.xml
C:\Program Files\Dynamic File Services\audit\DswAuditCfg.xml
```

There is no special way to view this file. It is an XML file and most HTTP browsers can display XML in a readable form.

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 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.

Repairing the Dynamic File Services Pair and Policy Databases

11

Novell® Dynamic File Services (DynamicFS) provides a repair tool for repairing the pair and policy databases.

- Section 11.1, "Understanding Dynamic File Services Repair," on page 129
- Section 11.2, "Repairing a Pair or Policy Database," on page 130
- Section 11.3, "Dynamic File Services Pair and Policy Database Snapshots," on page 131

11.1 Understanding Dynamic File Services Repair

The Dynamic File Services pair and policy databases consist of the following files:

- DswPairDatabase.xml
- DswPolicyDatabase.xml

During the DynamicFS Service startup, the databases are opened and checked for errors. The repairs are made silently (no messages are generated). Two events trigger an entry in the Windows Event Logger:

- If non-fatal events are detected, DynamicFS starts the Repair tool and repairs them. If the Repair tool fails to open, an event is logged in the Windows event logger.
- If fatal errors are detected, DynamicFS uses the database snapshots to roll back to a previously known good version of the database. If the rollback fails, an event is logged in the Windows event logger.

The following sections identify the nature of errors and repair actions:

- Section 11.1.1, "Dynamic File Services Service Startup Errors," on page 129
- Section 11.1.2, "Fatal Errors for the Pair Database," on page 130

11.1.1 Dynamic File Services Service Startup Errors

If any of the following errors are detected, the databases are marked as needing repair. DynamicFS operations returns an error.

Pair Database

DswPairDatabase.xml is not valid XML. This is not repairable.

Any pair GUID is missing or damaged. This is repairable.

Any pair name is missing. This is repairable.

Any missing results directory in the XML. This is repairable.

Missing primary or secondary directory. This is not repairable.

Policy Database

`DswPolicyDatabase.xml` is not valid XML. This is not repairable.

Any policy GUID is missing or damaged. This is repairable.

Any policy name is missing or damaged. This is repairable.

Corresponding policy XML file is missing or has damaged XML. This is not repairable.

Policy XML Files

XML is damaged. This is not repairable.

Policy GUID is missing or damaged. This is repairable.

Policy name is missing or damaged. This is repairable.

Policy type is missing or damaged. This is repairable.

Policy direction is missing or damaged. This is not repairable.

Repair report mode: This mode generates a report of errors found. No attempt is made to fix anything.

11.1.2 Fatal Errors for the Pair Database

Fatal errors that cause the pair database to remain closed are:

- Damaged XML for the file `DswPairDatabase.xml`
- Missing the following tags or values for those tags:

  ```
  <guid>
  <name>
  <primary>
  <secondary>
  ```

11.2 Repairing a Pair or Policy Database

If you are unable to open a Dynamic File Services pair or policy, it might be because its definition has been corrupted. You can run the Repair tool to find out the possible errors. It repairs any errors that it can and reports the ones that it cannot fix.

1 Log in to the DynamicFS server as the Administrator user or as a user that is a member of the Dynamic File Services group.

2 On the server, start the Repair tool by right-clicking the *Dynamic File Services Service Controller* icon in the notification area and selecting *Repair Tool* from the menu.
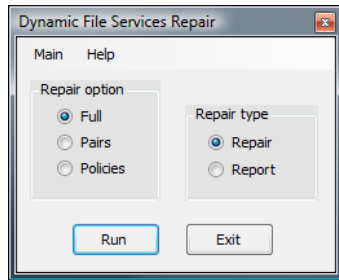
3 In the *Repair type* area, select one of the following options:

Repair: Repairs the problem pair or policy database errors that are repairable.

Report: Generates a report of the errors found. No attempt is made to fix anything.

4 In the *Repair option* area, select one of the following options:

Full: Checks both the pair and policy databases.

Pairs: Checks the pair databases.

Policies: Checks the policy databases.

5 Select *Run* to begin the report or repair process.

When the repair or report is completed, the Repair Results dialog box pops up.

6 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

- Pair database status and errors

- `CoreConfig.xml` file status and errors

7 (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 `DswRepair.log`.

8 When you are done, click *Close* to close the dialog box.

11.3 Dynamic File Services Pair and Policy Database Snapshots

Dynamic File Services automatically takes a snapshot of the pair database, policy database, and the individual policy files. The snapshots are taken between 11:30 p.m. and midnight daily. Each time a snapshot is taken, the database files are first verified to make sure they are valid database files. The files are stored in a directory named `Dynamic File Services SnapShot\`*day_of_the_week*`\`. Only one copy for each day of the week is kept at any given time. The copies are kept on a seven-day rotation. These snapshots are only used when the service starts and a fatal error is detected in either of the databases.

When a fatal error is detected, DynamicFS checks to see if there is a snapshot from the previous day. If the files for the previous day do not exist, each previous day's files are checked for valid databases. DynamicFS rolls back the databases to use the most recent valid version of the files. The `DswPairDatabase.xml`, `DswPolicyDatabase.xml`, and all of the policy files are copied to the correct location. If none of the snapshot daily directories contain valid database files, an event is logged in the event log, indicating that there were no snapshot files available to roll back.

The time value when the snapshot is taken is stored in the `coreconfig.xml` file. There is no interface to change the time when the snapshots are taken.

FAQs and Troubleshooting for Dynamic File Services

12

This section answers frequently asked questions about Novell® Dynamic File Services (DynamicFS). It also describes workarounds for any known issues.

12.1 Why can't I log in to the Dynamic File Services Service?

If you are having trouble logging in to the Dynamic File Services Service, 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 DynamicFS on the target server. See Section 6.1, "Adding or Removing Members in the Dynamic File Services Group," on page 61.

- **Service Port:** The port number (default 8999) must match the configured port on the target server. See Section 6.5, "Configuring the Dynamic File Services Service Port," on page 66.

- **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 DynamicFS Service port. See Section 6.6, "Enabling or Disabling a Firewall Exception for the Dynamic File Services Service Port," on page 67.

- **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 6.7, "Managing a Dynamic File Services SSL Certificate," on page 68.

12.2 Can I cancel a policy that is running?

You can stop a running policy by selecting the Dynamic File Services pair, then selecting *Actions > Stop running process*. This stops all policies currently running on the pair.

To ensure that a policy is not run again, go to the policy's Properties page and unschedule it. For information, see Section 10.2, "Viewing the Policy Execution History for a Pair," on page 120.

12.3 How do I configure a policy to not move files without disassociating it from the pair?

Go to the Dynamic File Services policy's Properties page and unschedule it. For information, see Section 9.7.3, "Unscheduling a Policy for All Pairs," on page 106.

12.4 How do I see what policies are running or what files have been moved?

Double-click the Dynamic File Services pair to open the Statistics page. For information, see Section 10.2, "Viewing the Policy Execution History for a Pair," on page 120.

12.5 The Dynamic File Services Service is not running

The Dynamic File Services Service must be running on the DynamicFS server before you can connect to it with the Management Console. The service starts automatically after the install and on reboot. You can verify that the service is running by using the *Dynamic File Services Service Controller* icon in the notification area or by looking for the `DswService.exe` process in the Task Manager or the Computer Management tool.

To start the service, see Section 6.2, "Starting and Stopping the Dynamic File Services Service," on page 62.

Security Considerations for Dynamic File Services

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.

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.

13.1.1 Service Authentication Credentials

To connect to a Dynamic File Services server, you must provide the login credentials (username and password) of a user who 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 Dynamic File Services group.

The DynamicFS administrator user identity can be validated in Workgroup and Active Directory Domain environments.

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 DynamicFS 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 non-self-signed certificate.

Self-Signed Certificates

By default, remote communications between the Management Console running on a client and the DynamicFS 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 DynamicFS 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 Services Service Controller. For information, see Section 6.7.2, "Creating a Dynamic File Services Self-Signed Certificate," on page 70.

Non-Self-Signed Certificates

Non-self-signed SSL certificates that you acquire through a certificate authority are also supported. Use this option if your enterprise security policy requires this level of security. You can set up a non-self-signed certificate by using the *Certificate Configuration* option in the Dynamic File Services Service Controller after the install. For information, see Section 6.7.3, "Configuring a Non-Self-Signed Certificate for Dynamic File Services," on page 71.

Self-Signed Certificates in a Cluster

When you install DynamicFS on a cluster node, a self-signed SSL certificate is created for the DynamicFS Service on that node. You do not associate the SSL certificate with the DynamicFS Service cluster resource because each node of the cluster has a different self-signed SSL certificate.

When the Management Console connects to a DynamicFS 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 who 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 DynamicFS Service. By default, DynamicFS uses port 8999. This port can be modified during or after the install. For information, see Section 6.5, "Configuring the Dynamic File Services Service Port," on page 66.

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 DynamicFS Service port (default 8999). The firewall exception is enabled by default. Disabling the firewall exception effectively disables the remote management capability for the DynamicFS Service. You can also enable and disable the firewall exception after the install. For information, see Section 6.6, "Enabling or Disabling a Firewall Exception for the Dynamic File Services Service Port," on page 67.

When the *Windows Firewall Access* option is enabled, DynamicFS automatically configures an exception for the configured DynamicFS 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 Administrator Group

During the install, a new administrator user group called *Dynamic File Services* is created on machines where you install the DynamicFS Service. 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.

IMPORTANT: The Administrator user account is automatically allowed to administer DynamicFS, but the Administrator username is not added by default to the Dynamic File Services group. (It is not necessary to explicitly add the Administrator username to the group, but it is okay to add it.) Before a different user can administer the DynamicFS Service, the user's username must be added to the Dynamic File Services group on that computer. The Administrator user or any user with Administrator privileges can add or remove usernames as members of the Dynamic File Services group.

After the install, you set up DynamicFS administrators by adding them as members of the Dynamic File Services group. It is not necessary for the Dynamic File Services group members to also be members in the Administrators group. You must be logged in as a user with Administrators group privileges in order to add members to the Dynamic File Services group.

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 DynamicFS 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 Access Control

Windows User Access Control is available on some Windows platforms. If it is enabled, Windows User Access 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 who is a member of the Dynamic File Services group.

13.1.8 Network Connections

You can run the DynamicFS Management Console on the same server where you are configuring DynamicFS 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

To give users a merged view of the data, create a single network share on the primary folder of the DynamicFS pair. 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 Auditing Management Events

Auditing of the management of the DynamicFS 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 DynamicFS Service, pairs and policies
DswAuditCfg.xml	Controls the logging behavior for the audit log

All DynamicFS 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. For more information, see Section 10.7, "Auditing Management Events," on page 126.

13.1.11 Event Logging

DynamicFS uses the Microsoft Event Viewer for logging the DynamicFS Service start/stop events and fatal errors such as application exceptions. See the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/default.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 DynamicFS 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
```

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` directory.

Table 13-1 *DynamicFS Log Files*

DynamicFS Component	Log File	Logging Control File
Enforcer	DswEnforcer.log	DswEnforcer.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).

Dynamic File Services Commands for Pair and Policy Management

A

This section describes the Novell® Dynamic File Services (DynamicFS) command line interface (CLI) utility for managing pairs and policies. A CLI provides needed capabilities for testing and for customers who are interested in developing command line scripts.

You can manage pairs and policies on a Windows server by using the DynamicFS CLI utility (`DswCli.exe`). On Windows servers, the DynamicFS CLI utility is found in the directory where you installed DynamicFS. By default, DynamicFS is installed in the `C:\Program Files\Dynamic File Services` directory.

The DynamicFS CLI utility provides only the basic functionality of the GUI interface. You can use it to do the following management tasks:

- Add and remove pairs.
- Add and remove policies.
- Associate and disassociate a pair with a policy.
- Run one or more policies for a pair.

Use the commands in this section to manage pairs and policies from the command line.

A.1 Command Line Syntax

The following notation is used in the Dynamic File Services command line syntax:

Notation	Description
Text without brackets or braces	Command, action, parameter, or option that you must type as shown.
<Italicized text inside angle brackets>	Variable that you must replace with a value.
Italicized text	Values in DynamicFS commands are read as character strings and should be surrounded by quotation marks.

Notation	Description
[Text inside square brackets]	Optional parameters or options.
{Text inside braces}	A set of mutually exclusive items separated by a vertical bar (|). Choose only one.

A.2 Help Command

`-help, -h`

Displays basic information about the syntax for Dynamic File Services CLI options, parameters, and actions. It also identifies the software version of DynamicFS that is running.

At the *Command Prompt* console, go to the `DynamicFS` directory, then enter one of the following:

```
DswCli.exe help
```

```
DswCli.exe -h
```

A.3 Authentication Options

You must specify the server name and login credentials for the server where you want to manage Dynamic File Services pairs and policies. This allows DynamicFS to connect to the server and execute the command.

IMPORTANT: Login credentials are not required if you run a DynamicFS command while you are logged in to the server you are managing as the Administrator user or a user in the Administrators group. Credentials are required if you are managing the server remotely from another computer, or if you are on the server you want to manage but are logged in as a user without Administrator privileges.

You can specify the server name and login credentials with each command, or you can set environment variables for the parameters while you are managing the server.

- Section A.3.1, "Setting Authentication Options in Commands," on page 142
- Section A.3.2, "Setting Authentication Options as Environment Variables," on page 144

A.3.1 Setting Authentication Options in Commands

You can specify the authentication options in each DynamicFS command for a server.

Syntax

```
DswCli.exe [-servername={"ip_address" | "DNS_name"}
[-username="admin_user_name" [-password="admin_user_password"]]
[-port="portnumber"]]  {-pair [pair_options] | -policy [policy_options]}
```

Specify the authentication parameters as needed in the pair or policy command.

Authentication Options

-servername

> Specify the IP address or DNS name of the server where you want to create or manage the DynamicFS pair. If you are issuing the DynamicFS commands locally on the DynamicFS server, you can also use the loopback address (127.0.0.1) instead of its assigned IP address, or you can use `localhost` as the server name instead of its full DNS name. The IPv4 format is supported for the IP address. DNS names are case sensitive.
>
> **Syntax**
>
> ```
> -servername={"ip_address" | "DNS_name"}
> ```
>
> **Examples**
>
> ```
> -servername="192.168.1.1"
> ```
> ```
> -servername="server1.site1.example.com"
> ```
> ```
> -servername="localhost"
> ```

-username, -u

> Specify the username of a user who is a member of the Dynamic File Services group (or as the Administrator user) for the DynamicFS server that you want to manage.
>
> **Syntax**
>
> ```
> -username="admin_user_name"
> ```
> ```
> -u="admin_user_name"
> ```
>
> **Examples**
>
> ```
> -username="Administrator"
> ```
> ```
> -u="Administrator"
> ```

-password, -p

> Specify the password for the user whose username you supplied.
>
> **Syntax**
>
> ```
> -password="admin_user_password"
> ```
> ```
> -p="admin_user_password"
> ```
>
> **Examples**
>
> ```
> -password="novell"
> ```
> ```
> -p="novell"
> ```

-port

> Instead of using the configured port number, use the supplied value.
>
> You need to specify this parameter only if you have set up the target server to use a port other than the default DynamicFS port (8999) for remote management communications.
>
> If this option is not used and the port is not configured as an environment variable, the default DynamicFS port is automatically used for DynamicFS communications.
>
> **Syntax**
>
> ```
> -port="portnumber"
> ```
>
> **Examples**
>
> ```
> -port="1234"
> ```

Authentication Examples

Using the IP Address of the DynamicFS Server

```
DswCli.exe -servername="192.168.1.1" -username="Administrator"
-password="novell" -pair
```

This command connects to the server via the IP address 192.168.1.1, logs in with the credentials of Administrator and novell, then lists all pairs on the specified server. You can also provide the credentials of a user who is a member of the Dynamic File Services group.

Using the DNS Address of the DynamicFS Server

```
DswCli.exe -servername="server1.site1.example.com" -u="Administrator"
-p="novell" -port="1234" -policy
```

This command connects to the server via the DNS name of server1.site1.example.com, logs in with the credentials of Administrator and novell, then lists all policies on the specified server. You can also provide the credentials of a user who is a member of the Dynamic File Services group. It specifies that the TCP connection should be made with port 1234 on the target server, because you have previously configured the DynamicFS Service port on that server to use port 1234.

A.3.2 Setting Authentication Options as Environment Variables

DynamicFS allows you to use the Windows `set` command in the *Command Prompt* console to specify environment variables for the authentication parameters (server name, username, password, and port) for the server that you want to manage with commands. The environment variables are set for only one server at a time. The environment variable settings persist until you issue the `set` command again with different values, or until you close the *Command Prompt* console.

If the environment variables are not set, you must provide the `-servername`, `-username`, and `-password` options for every command. You need to specify the port number for the DynamicFS Service port on the target server only if the server has been previously configured to use a port other than the default (8999). For example, you might need to provide the following authentication options for each command line you type:

```
DswCli.exe [-servername="servername" [-username="username"
[-password="password"]] [-port="portnumber"]] {-pair | -policy}
```

After the environment variables are set for a given server, the parameter values are automatically applied for every DynamicFS command where you do not provide authentication parameters. For example, the following commands apply only to the server that has been previously set up with the environment variables:

```
DswCli.exe -pair
DswCli.exe -policy
```

You can change the environment variables settings by issuing the `set` commands again with the new values.

If it is used without parameters, the `set` command displays the current environment variable settings.

IMPORTANT: You can remove the environment variable settings by closing the *Command Prompt* console.

The DynamicFS environment variables for the set command are:

Table A-1 *Syntax for the DynamicFS Environment Variables*

Environment Variable	Description

set DswParm1=*servername*	Specify the *servername* by providing the DNS address or the IP address of the server you want to manage.
	
	Examples
	
	The following command sets the environment variable for *servername* to 192.168.1.1:
	
	`set DswParm1=192.168.1.1`
	
	The following command displays the current setting for the DswParm1 environment variable:
	
	`set DswParm1`

set DswParm2=*username*	Specify the *username* of the user identity you want to use to manage the server. The user must be a member of the Dynamic File Services group (or the Administrator user) on the server.
	
	Examples
	
	The following command sets the environment variable for *username* to Administrator. You can also provide the credentials of a user who is a member of the Dynamic File Services group.
	
	`set DswParm2=Administrator`
	
	The following command displays the current setting for the DswParm2 environment variable:
	
	`set DswParm2`

set DswParm3=*password*	Specify the *password* of the user identity you specified with DswParm2.
	
	Examples
	
	The following command sets the environment variable for *password* to novell:
	
	`set DswParm3=novell`
	
	The following command displays the current setting for the DswParm3 environment variable:
	
	`set DswParm3`

Environment Variable	Description
set DswParm4=*portnumber*	Specify the *portnumber* to use for DynamicFS communications with the server you want to manage.
	You need to specify this parameter only if you have set up the target server to use a port other than the default DynamicFS port for remote management communications. The default port value is automatically assumed if this parameter is not otherwise specified.
	Examples
	The following command sets the environment variable for *portnumber* to 1234:
	`set DswParm4=1234`
	The following command displays the current setting for the DswParm4 environment variable:
	`set DswParm4`

To use environmental variables while executing DynamicFS commands:

1 On a Windows server or workstation where DynamicFS is installed, open the *Command Prompt* console.

2 At the command prompt, specify the server name and login credentials for the server that you want to manage by entering the following commands as needed:

```
set DswParm1=192.168.1.1

set DswParm2=Administrator

set DswParm3=password

set DswParm4=1234
```

Make sure to change the values to the credentials needed to log in to the server you want to manage.

3 At the command prompt, enter the `DswCli.exe` commands to manage pairs and policies on the specified server.

You can specify the commands without providing credentials.

4 Repeat Step 3 for all of the `DswCli.exe` commands you want to issue for that server.

5 When you are done, repeat Step 2 to Step 4 for each server you want to manage.

6 Close the *Command Prompt* console to remove the credentials as environmental variables.

A.4 Management Commands

You can use the management commands in this section to display information about the selected Dynamic File Services server. For information about authentication parameters, see Section A.3, "Authentication Options," on page 142.

DswCli.exe [*authentication_parameters*] -system

Displays system information for the specified server.

```
DswCli.exe [authentication_parameters] -localdrives
```

Displays local drive information for the specified server.

```
DswCli.exe [authentication_parameters] -shares
```

Displays network share information for the specified server.

A.5 Pair Commands

```
DswCli.exe -pair
```

The `-pair` option for `DswCli.exe` can be used to add and remove Dynamic File Services pairs on the server where the command is executed. You can also associate and disassociate DynamicFS policies with a pair.

IMPORTANT: After you create a pair, you must create a network share for the primary path in order to provide a merged view of the data for users. Use the Microsoft Network Sharing tool to create a network share. Users connect to the network share by mapping a local drive letter on their workstations to the network share. All user access takes place through the share.

Syntax

For information about how to provide the servername and login credentials that are needed to connect to the server that you want to manage, see Section A.3, "Authentication Options," on page 142.

For information about the policy command and parameters, see Section A.6, "Policy Commands," on page 152.

Add a Pair

```
DswCli.exe [authentication_parameters] -pair -add -name=<pairname>
-primaryPath=<path> -secondaryPath=<path> option
```

After you create a pair, you must associate it with one or more policies. For information about creating policies, see the -add action option for a policy command.

Delete a Pair

The delete option unlinks the two paths in a pair. The files are not deleted.

```
DswCli.exe [authentication_parameters] -pair -delete
-pairID=<pairname|GUID>
```

Associate a Pair with a Policy

```
DswCli.exe [authentication_parameters] -pair -associate
-pairID=<pairname|GUID> -policyID=<policyname|GUID>
```

Disassociate a Pair from a Policy

```
DswCli.exe [authentication_parameters] -pair -disassociate
-pairID=<pairname|GUID> -policyID=<policyname|GUID>
```

List All Pairs on a Server

```
DswCli.exe [authentication_parameters] -pair
```

List Details for a Pair

```
DswCli.exe [authentication_parameters] -pair -detail
-pairID=<pairname|GUID>
```

Run Policies for a Pair

```
DswCli.exe [authentication_parameters] -pair -run
-pairID=<pairname|GUID> [-policyIDlist]
```

Pair Parameters

`-pairID`

> Specify the pair identifier. You can provide the pair name, or provide the GUID of the pair.
>
> **Syntax**
>
> `-pairID=< "pairname" | "GUID" >`
>
> **Example**
>
> `-pairID="MyPair"`

Pair Actions

Add a Pair on a Server

`-add`

> The `-add` action creates the pair with the desired name and stores the configuration as an XML file in the `...\Dynamic File Services\Pairs` folder.
>
> If a pair name contains a space, you must delimit multiple entries with a comma when working from the command line interface.
>
> ---
>
> **IMPORTANT:** Before you issue a command to create a pair, make sure your system meets the requirements in Section 8.2.1, "Prerequisites for Creating a Pair," on page 85.
>
> ---
>
> You must specify a name for the pair, a primary path, and a secondary path. You can optionally specify a description of the pair.
>
> **Add Pair Parameters**
>
> **`-name`**
>
> > Specify the pair name. The name must be unique on the server you are managing.
> >
> > **Syntax**
> >
> > `-name="pairname"`
> >
> > **Example**
> >
> > `-name="MyPair"`
>
> **`-flags`**
>
> > Specify the flag to exclude or include the folders specified by the `-paths` option. A given pair can include folders or exclude folders, but you cannot do both.
> >
> > **Syntax**
> >
> > `-flags=<"exclude" | "include">`
> >
> > **Examples**
> >
> > `-flags="exclude" -paths="path1"`
> >
> > `-flags="include" -paths="path1,path2,path3"`
>
> **`-primaryPath`**
>
> > Specify the path of the primary location in the pair. The drive or path must already exist; the command does not create it for you.
> >
> > **Syntax**
> >
> > `-primaryPath="path"`

Examples

```
-primaryPath="C:\users"

-primaryPath="M:"

-primaryPath="K:\engineering\proj1"
```

-secondaryPath

Specify the path of the secondary location in the pair. The drive or path must already exist; the command does not create it for you.

Syntax

```
-secondaryPath="path"
```

Examples

```
-secondaryPath="L:\users\media"

-secondaryPath="N:\m_sh"

-secondaryPath="Z:\project1"
```

Add Pair Options

-description

Specify a textual description of the pair.

Syntax

```
-description="text"
```

Example

```
-description="Moves graphics files to the secondary location."
```

Add Pair Examples

Create a Pair

```
DswCli.exe -servername="localhost" -username="Administrator"
-password="novell" -pair -add -name="MyPair"
-primaryPath="e:\PrimaryPath"
-secondaryPath="f:\SecondaryPath"
```

This command uses the user credentials of the Administrator user to log you in to the server where you are running the command. You can also provide the credentials of a user who is a member of the Dynamic File Services group. It creates a DynamicFS pair named MyPair on the server. The pair's primary path is the e:\PrimaryPath directory. The pair's secondary path is the f:\SecondaryPath directory. No files are moved until you create a policy for the pair, and associate the policy to the pair.

Create a Pair with a Description

```
DswCli.exe -servername="localhost" -username="Administrator"
-password="novell" -pair -add -name="ProjectA"
-primaryPath="e:\PrimaryPath"
-secondaryPath="f:\SecondaryPath" -description="Project A
management files"
```

This command uses the user credentials of the Administrator user to log you in to the server where you are running the command. You can also provide the credentials of a user who is a member of the Dynamic File Services group. It creates a DynamicFS pair named ProjectA. It uses the optional description field

to provide more information about the pair. The pair's primary path is the `e:\PrimaryPath` directory. The pair's secondary path is the `f:\SecondaryPath` directory. No files are moved until you create a policy for the pair, and associate the policy to the pair.

Delete a Pair from a Server

`-delete`

The `-delete` action removes the specified pair from the DynamicFS database. All links between the two storage locations are removed. Data is not destroyed. The data is not moved; that is, the data remains in the location where it was stored when the delete command was executed. The associations between the pair and any policies are removed. After the pair is deleted, the users who are logged in to the network share on the primary location can see and access the data only on the primary location.

You must specify the pairID for the pair that you want to delete.

Syntax

```
DswCli.exe [authentication_parameters] -pair -delete
-pairID=<"pairname" | "GUID" >
```

Example

The following `-pair` command deletes the DynamicFS pair named MyPair on the specified server.

```
DswCli.exe -servername="localhost" -username="Administrator"
-password="novell" -pair -delete -pairID="MyPair"
```

Associate a Pair to a Policy

`-associate`

The `-associate` action links a specified pair to a specified policy. You must specify the pairID parameter for the pair that you want to associate.

Syntax

```
DswCli.exe [authentication_parameters] -pair -associate
-pairID=<"pairname" | "GUID" > -policyID=<"policyname" | "GUID">
```

Example

The following `-pair` command associates the DynamicFS pair named MyPair with the policy named MyPolicy on the specified server.

```
DswCli.exe -servername="localhost" -username="Administrator"
-password="novell" -pair -associate -pairID="MyPair"
-policyID="MyPolicy"
```

Disassociate a Pair to a Policy

`-disassociate`

The `-disassociate` action removes the association between a given pair and policy. You must specify the pairID parameter for the pair. You must specify the policyID parameter for the policy that you no longer want to run on the pair.

Syntax

```
DswCli.exe [authentication_parameters] -pair -disassociate
-pairID=<"pairname" | "GUID" > -policyID=<"policyname" | "GUID" >
```

Example

The following -pair command removes the association between the DynamicFS pair named MyPair and the policy named MyPolicy on the specified server.

```
DswCli.exe -servername=localhost -username=Administrator
-password=novell -pair -disassociate -pairID="MyPair"
-policyID="MyPolicy"
```

List All Pairs on a Server

(no action options)

When the -pair action option is used without any other parameters or options, all pairs on the server are listed.

Syntax

```
DswCli.exe [authentication_parameters] -pair
```

Example

The following -pair command displays a list of all pairs on the specified server.

```
DswCli.exe -servername="localhost" -username="Administrator"
-password="novell" -pair
```

List Details for a Pair

-detail

The -detail action provides a detail listing for a pair. You must specify the pairID parameter for the pair.

Syntax

```
DswCli.exe [authentication_parameters] -pair -detail
-pairID=<"pairname" | "GUID">
```

Example

The following -pair command lists details for the DynamicFS pair named MyPair on the specified server.

```
DswCli.exe -servername="localhost" -username="Administrator"
-password="novell" -pair -detail -pairID="MyPair"
```

Run Policies on a Pair

-run

The -run action causes all policies defined in the policy list to be executed. You must specify the pairID parameter for the pair. Use the policyIDlist parameter to list one or more policies to run. If the policy list is not specified, all policies are run that are associated with the specified pair.

Syntax

```
DswCli.exe [authentication_parameters] -pair -run
-pairID=<"pairname"|"GUID"> [-policyIDlist="policy1,policy2"]
```

Example

The following -pair command runs the DynamicFS policies named MyPolicy and MyPolicy100 for the pair named MyPair on the specified server.

```
DswCli.exe -servername="localhost" -username="Administrator"
-password="novell" -pair -run -pairID="MyPair"
-policyIDlist="MyPolicy,MyPolicy100"
```

A.6 Policy Commands

`DswCli.exe -policy`

The `-policy` option allows you to create and delete policies on a specified server. When it is used without other policy parameters, all policies on the server are listed from the Dynamic File Services data store.

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

For information about associating policies to pairs, see "-associate" on page 150 and "-disassociate" on page 150

For information about running policies on a pair, see "-run" on page 151.

Syntax

Add a Policy

```
DswCli.exe [authentication_parameters] -policy -add
-name=<policyname> options filterOptions frequencyOptions
```

After you add a policy, you must associate it with one or more pairs before you can run it on the pairs. For information, see the `-associate` action option for a pair command.

Delete a Policy

```
DswCli.exe [authentication_parameters] -policy -delete
-policyID=<"policyname"|"GUID">
```

List All Policies on a Server

```
DswCli.exe [authentication_parameters] -policy
```

List Details for a Policy

```
DswCli.exe [authentication_parameters] -policy -detail
-policyID=<"policyname"|"GUID">
```

Policy Parameters

`-policyID`

Specify the policy identifier. You can provide the policy name, or provide the GUID of the policy.

Syntax

```
-policyID=< "policyname" | "GUID" >
```

Examples

```
-policyID="MyPolicy"
```

```
-policyID="My JPG and BMP Policy"
```

```
-policyID="My Last Modified GT 6 Months Policy"
```

`-policyIDlist`

Specify a comma-separated list of policyID parameters. For each policy, you can provide the policy name, or provide the GUID of the policy.

If the policy list is not specified, all policies that are associated with the specified pair are run.

Syntax

```
-policyIDlist="<policyname|GUID>,<policyname|GUID>,..."
```

Example

```
-policyIDlist="MyPolicy,MyPolicy100"
```

Policy Actions

Add a Policy

`-add`

The `-add` action creates the policy with the specified name and stores the configuration as an XML file in the `...\Dynamic File Services\Policies` folder.

Add Policy Parameters

`-name="policyname"`

Specify a name for the policy.

Add Policy Options

Specify the following as options in combination with the `-add` action.

Options	Description
`-description="text"`	Specify a textual description of the policy. This option is optional.
`-primaryToSecondary`	Specifies the direction to move files. If a direction option is not specified, the default direction is primary to secondary. **Restriction:** This option cannot be used with the secondaryToPrimary option.
`-secondaryToPrimary`	Specifies the direction to move files. If a direction option is not specified, the default direction is primary to secondary. **Restriction:** This option cannot be used with the primaryToSecondary option.

Policy Filter Options

Specify the following as filter options in combination with the `-add` action. Filter options are applied in combination to determine which files you want to move. All of the specified filter options must be met in order for the file to be moved.

You can specify one or more filter options in the same policy. Only one filter option of each type can be used in the same policy.

Filters set in the same policy are enforced as AND conditions. A file must meet all filter conditions to be moved. For example, if you specify a filter with the file extension option for files ending in `*.jpg` and `*.gif`, then any file with either of the specified extensions is moved. If you specify a second filter with a file size option for files with a file size greater than 5 MB, only the `*.jpg` and `*.gif` files that have a file size greater than 5 MB are moved.

Filters set in different policies that run at the same time are enforced as OR conditions. A file that meets any one of the conditions is moved. In the example above, if each of the filters was set in a separate policy and both policies run at the same time, then a file is moved if it ends in `*.jpg`, if it ends in `*.gif`, or if it is greater than 5 MB.

Filter Options	Description

`-filesize="ccn[...]uu"`
 	
Where
 	
`cc` = `gt` or `lt` conditional
`n[...]` = any length numeric value
`uu` = units of size
 	
Valid `uu` values are:
 	
  `b` =bytes
  `kb` =kilobytes
  `mb` =megabytes
  `gb` =gigabytes
	Specify the file size of files to filter for movement.
	
	Examples:
	
	Move all files that are greater than 1 GB in size.
	
	 `-filesize="gt1gb"`
	
	Move all files that are less than 100 KB in size.
	
	 `-filesize="lt100kb"`

`-lastaccessed="ccn[...]u"`
 	
Where
 	
`cc` = `gt` or `lt` conditional
`n[...]` = any length numeric value
`u` = units of time
 	
Valid `u` values are:
 	
  `d` = days
  `w` = weeks
  `m` = months
  `y` = years
	Move files that meet the specified condition based on the last access time.
	
	Examples:
	
	Move all files that have an access time greater than 10 days old.
	
	 `-lastaccessed="gt10d"`
	
	Move all files that have an access time less than 5 weeks old.
	
	 `-lastaccessed="lt5w"`

`-lastmodified="ccn[...]u"`
 	
Where
 	
`cc` = `gt` or `lt` conditional
`n[...]` = any length numeric value
`u` = units of time
 	
Valid `u` values are:
 	
  `d` = days
  `w` = weeks
  `m` = months
  `y` = years
	Move files that meet the specified condition based on the last modified time.
	
	Examples:
	
	Move all files that have a modified time greater than 10 days old.
	
	 `-lastmodified="gt10d"`
	
	Move all files that have a modified time less than 5 weeks old.
	
	 `-lastmodified="lt5w"`

Filter Options	Description
`-fileextension="extensionlist"`	Move files that have the specified file extensions. An asterisk (*) can be used as a wildcard character. Separate multiple entries with a comma.
	Examples:
	Move all `.jpg` files and `.gif` files.
	`-fileextension="*.jpg,*.gif"`
	Move all `.txt` files.
	`-fileextension="*.txt"`

Policy Frequency Options

Specify one frequency option in combination with the -add action. The specified frequency option determines when the is enforced. The policy is enforced for all pairs associated with the policy.

Frequency Options	Description
`-manual`	Scan frequency is performed manually.
	Restrictions: This option cannot be combined with the following frequency options:

	`-hourly`
	`-daily`
	`-weekly`
	`-monthly`

`-hourly`	Scan frequency is performed hourly.
	Restrictions: This option cannot be combined with the following frequency options:

	`-manual`
	`-daily`
	`-weekly`
	`-monthly`

Frequency Options	Description

`-daily[="hh:mm[-hh:mm]"]`
 	
`hh:mm[-hh:mm]` specifies the scan start and stop time, respectively. Twenty-four-hour time is required with valid values of `00:00` to `23:59` (that is, midnight to 11:59 p.m.). The first two units specify hours from `00` to `23`. The second two units specify minutes from `00` to `59`.
	Scan frequency is performed daily.
	
	If the start and stop time are omitted, a default start time of 00:00 (midnight) is assumed and the scan runs to completion.
	
	If start time is provided and the stop time is omitted, the scan starts at the given time and runs to completion.
	
	Restrictions: This option cannot be combined with the following frequency options:
	
	`-manual`
	`-hourly`
	`-weekly`
	`-monthly`
	
	Example:
	
	The scan runs daily from 1:00 p.m. to 3:00 p.m.
	
	`-daily="13:00-15:00"`

Frequency Options	Description

`-weekly[="nn[@hh:mm[-hh:mm]]"]`
 	
Where
 	
`nn` specifies the day of the week. Valid values are:
 	
`00` = Sunday
`01` = Monday
`02` = Tuesday
`03` = Wednesday
`04` = Thursday
`05` = Friday
`06` = Saturday
 	
`@hh:mm[-hh:mm]` specifies the scan start and stop time, respectively. Twenty-four-hour time is required with valid values of `00:00` to `23:59` (that is, midnight to 11:59 p.m.). The first two units specify hours from `00` to `23`. The second two units specify minutes from `00` to `59`.
	Scan frequency is performed weekly.
	
	If the day of the week and the start and stop times are omitted, the scan starts on Sunday at 00:00 (12:00 midnight), and the scan runs to completion.
	
	If the start and stop time are omitted, a default start time of `00:00` (midnight) is assumed, and the scan runs to completion.
	
	If start time is provided and the stop time is omitted, the scan starts at the given time and runs to completion.
	
	Restrictions: This option cannot be combined with the following frequency options:
	
	  `-manual`
	  `-hourly`
	  `-daily`
	  `-monthly`
	
	Examples:
	
	The scan runs every Monday from 1:00 p.m. to completion
	
	 `-weekly="01@13:00"`
	
	The scan runs every Monday from 1:00 a.m. to 5:00 a.m.
	
	 `-weekly="01@01:00-05:00"`

Frequency Options	Description

`-monthly[="nn[@hh:mm-hh:mm]]"]`
 	
`nn` specifies the day of the month numerically. Valid values are from `1` to `31`.
 	
`@hh:mm[-hh:mm]` specifies the scan start and stop time, respectively. Twenty-four-hour time is required with valid values of `00:00` to `23:59` (that is, midnight to 11:59 p.m.). The first two units specify hours from `00` to `23`. The second two units specify minutes from `00` to `59`.
	Scan frequency is performed monthly.
	
	If the day of the month and the start and stop times are omitted, the scan starts on first day of the month at 00:00 (midnight) and runs to completion.
	
	If the start and stop time are omitted, a default start time of 00:00 is assumed and the scan runs to completion.
	
	If start time is provided and the stop time is omitted, the scan starts at the given time and runs to completion.
	
	Restrictions: This option cannot be combined with the following frequency options:
	
	   `-manual`
	   `-hourly`
	   `-daily`
	   `-weekly`
	
	Examples:
	
	The scan runs on the first day of the month from 1:00 p.m. to completion
	
	   `-monthly="1@13:00"`

Examples

Each of the following `-policy` commands creates a policy with a single filter specified. The direction option is not set in these policies, so data is moved in the default direction of primary to secondary. If no frequency is specified, the policy can be run manually.

-fileExtension Policy Filter

```
DswCli.exe -servername="localhost"
-username="Administrator" -password="novell" -policy -add
-name="My Pictures Policy"
-fileExtension="*.jpg,*.bmp,*.gif"
```

-fileSize Policy Filter

```
DswCli.exe -servername="localhost"
-username="Administrator" -password="novell" -policy -add
-name="My Size GT 1GB Policy" -fileSize="gt1gb"
```

-frequency Policy Filter

```
DswCli.exe -servername="localhost"
-username="Administrator" -password="novell" -policy -add
-name="My Weekly at 1300 Policy" -weekly="01@1300"
```

-lastAccessed Policy Filter

```
DswCli.exe -servername="localhost"
-username="Administrator" -password="novell" -policy -add
-name="My Last Accessed LT 5 Weeks Policy"
-lastAccessed="lt5w"
```

-lastModified Policy Filter

```
DswCli.exe -servername="localhost"
-username="Administrator" -password="novell" -policy -add
-name="My Last Modified GT 10 Days Policy"
-lastmodified="gt10d"
```

Delete a Policy

`-delete`

The `-delete` action removes the specified policy from the database. All links to any pairs are removed.

Syntax

```
DswCli.exe [authentication_parameters] -policy -delete
-policyID=<"policyname"|"GUID">
```

Example

The following `-policy` command deletes the DynamicFS policy named MyPolicy on the specified server.

```
DswCli.exe -servername="localhost" -username="Administrator"
-password="novell" -policy -delete -policyID="MyPolicy"
```

List All Policies on a Server

(no action options)

When the `-policy` action option is used without any other parameters or options, all policies on the server are listed.

Syntax

```
DswCli.exe [authentication_parameters] -policy
```

Example

The following `-policy` command displays a list of all policies on the specified server.

```
DswCli.exe -servername="localhost" -username="Administrator"
-password="novell" -policy
```

List Details for a Policy

`-detail`

The `-detail` action provides a detail listing of the requested policy. You must specify the policyID parameter for the policy.

Syntax

```
DswCli.exe [authentication_parameters] -policy -detail -policyID=<
"policyname" | "GUID" >
```

Example

The following -policy command lists details for the DynamicFS policy named MyPolicy on the specified server.

```
DswCli.exe -servername="localhost" -username="Administrator"
-password="novell" -policy -detail -policyID="MyPolicy"
```

A.7 Common Parameters

The following common parameters can be used by Dynamic File Services pair or policy actions.

-pairID

Specify the pair identifier. You can provide the pair name, or provide the GUID of the pair.

Syntax

```
-pairID=< "pairname" | "GUID" >
```

Example

```
-pairID="MyPair"
```

-policyID

Specify the policy identifier. You can provide the policy name, or provide the GUID of the policy.

Syntax

```
-policyID=< "policyname" | "GUID" >
```

Examples

```
-policyID="MyPolicy"
```

```
-policyID="My JPG and BMP Policy"
```

```
-policyID="My Last Modified GT 6 Months Policy"
```

-policyIDlist

Specify a comma-separated list of policyID parameters. You can provide the policy name, or provide the GUID of the policy.

Syntax

```
-policyIDlist="<policyname|GUID>,<policyname|GUID>,..."
```

Examples

```
-policyIDlist="MyPolicy,MyPolicy100"
```

```
-policyID="My JPG and BMP Policy"
```

```
-policyID="My Last Modified GT 6 Months Policy"
```

-silent

Use this option when you do not want to display errors or help on execution, such as in scripts for batch files where the batch file checks for return codes. This option returns a 0 if the command is successful. It returns a 1 if the command fails.

If a command fails, you can enter the command at the *Command Prompt* console without the -silent option to view the error messages.

A.8 Using DynamicFS Commands in Scripts

When you use Dynamic File Services commands in scripts, you can use the -silent option to prevent the results from displaying to a console. The script should check for an exit code to report whether a command succeeded or failed. The `-silent` option can be added to any DynamicFS pair or policy command.

-silent

Use this option when you do not want to display errors or help on execution, such as in scripts for batch files where the batch file checks for exit codes.

If a command fails, you can enter the command at the *Command Prompt* console without the `-silent` option to view the error messages.

Syntax

```
DswCli.exe [authentication_parameters] -pair -silent [pair_actions]
[pair_parameters] [pair_options]
```

```
DswCli.exe [authentication_parameters] -policy -silent [policy_actions]
[policy_parameters] [policy_options]
```

For information about the DynamicFS command options, see the following resources:

Option	Reference
authentication_parameters	Section A.3, "Authentication Options," on page 142
-pair pair_actions pair_parameters pair_options	Section A.5, "Pair Commands," on page 147
-policy policy_actions policy_parameters policy_options	Section A.6, "Policy Commands," on page 152

Exit Codes

The DswCli.exe command returns an exit code of 0 or 1.

Return Code	Description
0	Success
1	Failure

A.9 Example Scripts Using DynamicFS CLI Commands

This section provides example scripts for Dynamic File Services.

A.9.1 Creating a Pair and Policy

This example uses the DynamicFS CLI to set up one pair named *myPair* with a primary path of *e:\Primary* and a secondary path of *f:\Secondary*. It creates three policies and associates them to the pair:

- The GRAPHICS policy moves graphic files to the secondary path. It is scheduled to run daily at midnight.
- The OLD FILES policy moves files that have not been accessed or modified within two weeks to the secondary path. It is scheduled to run weekly on Saturday at midnight.
- The ACCESSED FILES policy moves files accessed during the past day from the secondary to the primary. It is scheduled to run hourly.

```
ECHO Create DynamicFS Setup of one pair and three policies

ECHO Create the pair named myPair

DswCli.exe -pair -add -name=myPair -primaryPath=e:\Primary -
secondaryPath=f:\Secondary -description="DynamicFS Pair linking user home
directories and old storage" -serverName=192.168.1.3 -port=8999 -
userName=Administrator -password=myPassword

ECHO Create the policy named GRAPHICS to secondary

DswCli.exe -policy -add -name="GRAPHICS to secondary" -
fileExtension=JPG,JPEG,BMP,GIF,PNG,RAW -daily="00:00" -primaryToSecondary -
description="Moves all graphic files to secondary storage. Runs daily at
midnight." -serverName=192.168.1.3 -port=8999 -userName=Administrator -
password=myPassword

ECHO Associate the policy to myPair

DswCli.exe -associate -policyID="GRAPHICS to secondary" -pairID=myPair -
serverName=192.168.1.3 -port=8999 -userName=Administrator -password=myPassword

ECHO Create the policy named OLD FILES to secondary

DswCli.exe -policy -add -name="OLD FILES to secondary" -lastModified="gt2w" -
lastAccessed="gt2w" -primaryToSecondary -description="Moves files that have
not been modified or accessed for over two weeks to secondary. Runs weekly on
Saturday morning at midnight" -weekly="05@00:00" -serverName=192.168.1.3 -
port=8999 -userName=Administrator -password=myPassword

ECHO Associate the policy to myPair

DswCli.exe -associate -policyID="OLD FILES to secondary" -pairID=myPair -
serverName=192.168.1.3 -port=8999 -userName=Administrator -password=myPassword

ECHO Create the policy named ACCESSED FILES to primary

DswCli.exe -policy -add -name="ACCESSED FILES to primary" -lastModified="lt1d"
-primaryToSecondary -description="Moves files that were accessed within the
last day to the primary. Runs hourly every day." -hourly -
serverName=192.168.1.3 -port=8999 -userName=Administrator -password=myPassword

ECHO Associate the policy to myPair

DswCli.exe -associate -policyID="ACCESSED FILES to primary" -pairID=myPair -
serverName=192.168.1.3 -port=8999 -userName=Administrator -password=myPassword
```

A.9.2 Running the Policies Manually

The following command uses a DynamicFS CLI command to run the three policies manually for the
pair named myPair:

```
ECHO Manually run all policies

DswCli.exe -run -policyIDList="OLD FILES to secondary","ACCESSED FILES to
primary","OLD FILES to secondary" -pairID=myPair -serverName=192.168.1.3 -
port=8999 -userName=Administrator -password=myPassword
```

A.9.3 Deleting the Policies

The following example uses the DynamicFS CLI to delete the three policies. The policies'
associations to the pair are also deleted.

```
ECHO Delete the policies

DswCli.exe -policy -delete -policyID="GRAPHICS to secondary" -
serverName=192.168.1.3 -port=8999 -userName=Administrator -password=myPassword

DswCli.exe -policy -delete -policyID="OLD FILES to secondary" -
serverName=192.168.1.3 -port=8999 -userName=Administrator -password=myPassword

DswCli.exe -policy -delete -policyID="ACCESSED FILES to primary" -
serverName=192.168.1.3 -port=8999 -userName=Administrator -password=myPassword
```

A.9.4 Deleting the Pair Relationship

The following example uses the DynamicFS CLI to delete the link between the primary path and
secondary path. No files are deleted.

```
DswCli.exe -pair -delete -pairID="myPair" -serverName=192.168.1.3 -port=8999 -
userName=Administrator -password=myPassword
```

Dynamic File Services File System Inventory Utility

B

The Novell® Dynamic File Services (DynamicFS) File System Inventory utility (`DswInventory.exe`) creates an inventory of the files in a pair, and writes the report to a file. On computers where the DynamicFS Service is installed, the File System Inventory utility is found in the directory where you installed DynamicFS. By default, DynamicFS is installed in the `C:\Program Files\Dynamic File Services` directory. The output inventory files are written in XML format. There are currently no tools to read the inventories that you run manually.

IMPORTANT: A file system inventory of each pair is automatically generated daily with the pair history run. For information, see Section 10.3, "Viewing the Pair History," on page 122.

- Section B.1, "DswInventory," on page 165
- Section B.2, "Preparing a Command File for a File System Inventory," on page 165
- Section B.3, "Example of a General Inventory," on page 168
- Section B.4, "Example of a Filtered Inventory," on page 175
- Section B.5, "Additional Information," on page 179

B.1 DswInventory

Description

The Dynamic File Services File System Inventory utility is used to create an inventory of the file system and write the desired output to a file. You must create a command file for each report that you want to create that specifies the options to use and the output file where you want write the results.

Syntax

```
DswInventory.exe commandFile [commandFile2...]
```

Log in to the DynamicFS server as the Administrator user (or a user with Administrator privileges), then issue the command in the *Command Prompt* console. It does not matter if the user is also a member of the Dynamic File Services group.

For information about creating the command file, see Section B.2, "Preparing a Command File for a File System Inventory," on page 165.

B.2 Preparing a Command File for a File System Inventory

Before you can use the Dynamic File Services File System Inventory tool, you must create a text file (referred to as the command file) where you specify the path to be inventoried, the type of reports to create, the filenames to use for the output reports, and the inventory options to use. You can create multiple command files to generate different inventory reports that meet the criteria that are specified in their respective command files.

In a command file, specify the following information about the inventory report that you want to create. Put each command on a separate line in the following order:

```
inventory_path
report_type
[inventory_option]
```

IMPORTANT: If there are errors in any parameter that you specify, the generated report files are empty.

The syntax for each of the required and optional elements is described in more detail in the following sections:

- Section B.2.1, "Inventory Path," on page 166
- Section B.2.2, "Report Types and Filenames," on page 166
- Section B.2.3, "Action List Filename," on page 167
- Section B.2.4, "Inventory Options," on page 167

B.2.1 Inventory Path

Specify the path that you want to inventory for this report. The inventory path can be the primary path for the pair or for any path in the pair.

```
inventory_path
```

Specify the full path, including the drive letter. For example:

```
C:\DATA\dir1\dir2
```

A command file can contain multiple paths. Place each path on a separate line. The combined output is written to the same report file. To write the inventory for each path to separate output files, create a separate command file for each path.

B.2.2 Report Types and Filenames

You can generate a summary report, a detailed report, or both reports. The summary report contains the statistics about the files, but does not contain the filenames. The detailed report includes both statistics and the matching filenames.

Specify a different filename for each report. The output files are in the .xml format.

Report Option	Description
/summary=*summary_report_filename*.xml	After an inventory is performed, creates a summary report file with the specified filename.
/detailed=*detailed_report_filename*.xml	After an inventory is performed, creates a detailed report file with the specified filename.

For example:

```
/summary=DATA_summary.xml
/detailed=DATA_detailed.xml
```

B.2.3 Action List Filename

You can request that a list of the filtered files be written to a separate file by using the /actionlist parameter. Specify a filename for a file where a list of files will be written.

Action List Option	Description
/actionlist=*filename*	Requests a list of files to be generated in the specified file.
/actionlistappend	Append the list of files to the specified action list file instead of overwriting its existing content.

B.2.4 Inventory Options

Specify one inventory option per line. If no inventory options are specified, then all options are enabled for the report. The inventory results are written to the report files that you requested.

You can specify none, one, or multiple general inventory options in any combination:

Inventory Option	Description
/access	Inventories files by last access time.
/create	Inventories files by creation time.
/modify	Inventories files by modification time.
/owner	Inventories files by owner name.
/size	Inventories files by file length.
/extension	Inventories files by file extension.
/empty	Tracks empty files and folders and adds the list to the report.

If you want to specify constraints for any one of the inventory options, you must specify constraints for each of the inventory options that you use in the same command file. For each parameter type, you can specify only one of its constraints.

In the following commands, the time duration notation ddd.hh:mm:ss indicates days (0 to 999), hours (0 to 24), minutes (0 to 60), and seconds (0 to 60). You can also specify days (ddd) alone.

Inventory Option	Description
/access>*ddd.hh:mm:ss*	Inventories files by last access times that are greater than the specified time duration.
/access<*ddd.hh:mm:ss*	Inventories files by last access times that are less than the specified time duration.
/create>*ddd.hh:mm:ss*	Inventories files by creation times that are greater than the specified time duration.

Inventory Option	Description
`/create<`*`ddd.hh:mm:ss`*	Inventories files by creation times that are less than the specified time duration.
`/modify>`*`ddd.hh:mm:ss`*	Inventories files by modification times that are greater than the specified time duration.
`/modify<`*`ddd.hh:mm:ss`*	Inventories files by modification times that are less than the specified time duration.
`/owner=`*`name`*`[,`*`nextName`*`...]`	Inventories files by the specified owner name or names. Delimit multiple names with a comma and no spaces.
`/size>amount`	Inventories files by file length that is greater than the amount specified. Specify the amount in bytes. For example, to inventory files greater than 1 MB, specify: `/size>1024`
`/size<amount`	Inventories files by file length that is less than the amount specified. Specify the amount in bytes. For example, to inventory files less than 1 MB, specify: `/size<1024`
`/extension=*.`*`extension`*`[,*.`*`extension2`*`...]`	Inventories files with the specified file extension. Separate entries with a comma and no spaces.

B.3 Example of a General Inventory

In this example, assume that you want an inventory for the Dynamic File Services pair that has a primary path of `e:\`. You perform the following tasks to manually generate a report:

- Section B.3.1, "Create a Command File," on page 168
- Section B.3.2, "Run the File System Inventory Utility," on page 169
- Section B.3.3, "View the Summary Report," on page 169
- Section B.3.4, "View the Detailed Report," on page 171

B.3.1 Create a Command File

Use a text editor to create a command file called `FSommands.txt` in the `DynamicFS` folder. The first line is the primary path for the DynamicFS pair. The second line requests a summary report to be created and specifies the output file for the summary report. The third line requests a detailed report to be created and specifies the output file for the detailed report. No inventory options are specified, so all inventory options are enabled.

```
e:\
/summary=e:\mySummary.xml
/detailed=e:\myDetails.xml
```

B.3.2 Run the File System Inventory Utility

1 Log in to the server as the Administrator user, or as a user in the Administrators group.

2 Open a *Command Prompt* console, then go to the `DynamicFS` folder.

3 At the prompt, enter

```
DswInventory.exe FSCommands.txt
```

B.3.3 View the Summary Report

The summary results are written to the `e:\mySummary.xml` file. The following is sample output of a summary report:

```xml
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
- <DswInventory GenerationDateTime="8/27/2009 3:10:37 PM" generation="summary"
platform="Win32NT" OS="Microsoft Windows NT 5.2.3790 Service Pack 2">
- <folderlist>
- <folder>
- <![CDATA[ e:\
  ]]>
  </folder>
  </folderlist>
- <list type="Accessed">
  <criteria filter="Within Last Day" filecount="31" totalsize="74811"
sizeunit="1024" />
  </list>
- <list type="Creation">
  <criteria filter="Within Last Day" filecount="31" totalsize="74811"
sizeunit="1024" />
  </list>
- <list type="EmptyFiles">
  <criteria filter="Empty Files" filecount="11" totalsize="0" sizeunit="0" />
  </list>
- <list type="Extension">
  <criteria filter=".10file" filecount="10" totalsize="0" sizeunit="1024" />
  <criteria filter=".doc" filecount="1" totalsize="57" sizeunit="1024" />
  <criteria filter=".docx" filecount="1" totalsize="57" sizeunit="1024" />
  <criteria filter=".exe" filecount="1" totalsize="16" sizeunit="1024" />
  <criteria filter=".gif" filecount="1" totalsize="888" sizeunit="1024" />
  <criteria filter=".jpeg" filecount="1" totalsize="468" sizeunit="1024" />
  <criteria filter=".jpg" filecount="5" totalsize="2569" sizeunit="1024" />
  <criteria filter=".ods" filecount="1" totalsize="3" sizeunit="1024" />
  <criteria filter=".odt" filecount="4" totalsize="828" sizeunit="1024" />
  <criteria filter=".pdf" filecount="1" totalsize="641" sizeunit="1024" />
  <criteria filter=".rtf" filecount="1" totalsize="1" sizeunit="1024" />
  <criteria filter=".txt" filecount="1" totalsize="0" sizeunit="1024" />
  <criteria filter=".xml" filecount="2" totalsize="6" sizeunit="1024" />
  <criteria filter=".zip" filecount="1" totalsize="69277" sizeunit="1024" />
  </list>
- <list type="Modified">
  <criteria filter="Within Last Day" filecount="3" totalsize="69283"
sizeunit="1024" />
  <criteria filter="1 Month - 2 Months" filecount="1" totalsize="16"
sizeunit="1024" />
  <criteria filter="6 Months - 1 Year" filecount="27" totalsize="5512"
sizeunit="1024" />
  </list>
- <list type="Owner">
  <criteria filter="Administrators" filecount="31" totalsize="74811"
sizeunit="1024" />
  </list>
- <list type="Length">
  <criteria filter="Less than 1KB" filecount="2" totalsize="2" sizeunit="1024"
/>
  <criteria filter="1KB - 4KB" filecount="1" totalsize="3" sizeunit="1024" />
  <criteria filter="4KB - 16KB" filecount="1" totalsize="5" sizeunit="1024" />
  <criteria filter="16KB - 64KB" filecount="6" totalsize="193" sizeunit="1024"
/>
  <criteria filter="64KB - 256KB" filecount="1" totalsize="161"
sizeunit="1024" />
  <criteria filter="256KB - 1MB" filecount="8" totalsize="5170"
sizeunit="1024" />
```

```
  <criteria filter="64MB - 256MB" filecount="1" totalsize="69277"
sizeunit="1024" />
  </list>
  </DswInventory>
```

B.3.4 View the Detailed Report

The detailed results are written to the `e:\myDetails.xml` file. The following is sample output from a detailed report. Omitted entries are replaced by ellipsis (…).

```xml
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
- <DswInventory GenerationDateTime="8/27/2009 3:10:37 PM"
generation="detailed" platform="Win32NT" OS="Microsoft Windows NT 5.2.3790
Service Pack 2">
- <folderlist>
- <folder>
- <![CDATA[ e:\
  ]]>
  </folder>
  </folderlist>
- <list type="Accessed">
- <criteria filter="Within Last Day" filecount="31" totalsize="74811"
sizeunit="1024">
- <information name="Spreadsheet.ods" matchvalue="8/26/2009 7:50:17 PM">
- <![CDATA[ e:\Primary\subfolder\Text Files\Spreadsheet.ods
  ]]>
  </information>
…
  </criteria>
  </list>
- <list type="Creation">
- <criteria filter="Within Last Day" filecount="31" totalsize="74811"
sizeunit="1024">
- <information name="Spreadsheet.ods" matchvalue="8/26/2009 7:50:17 PM">
- <![CDATA[ e:\Primary\subfolder\Text Files\Spreadsheet.ods
  ]]>
  </information>
…
  </criteria>
  </list>
- <list type="EmptyFiles">
- <criteria filter="Empty Files" filecount="11" totalsize="0" sizeunit="0">
- <information name="10file1.10file" matchvalue="0">
- <![CDATA[ e:\Primary\subfolder\10Files.10file\10file1.10file
  ]]>
  </information>
…
  </criteria>
  </list>
- <list type="Extension">
- <criteria filter=".10file" filecount="10" totalsize="0" sizeunit="1024">
- <information name="10file1.10file" matchvalue=".10file">
- <![CDATA[ e:\Primary\subfolder\10Files.10file\10file1.10file
  ]]>
  </information>
…
  </criteria>
- <criteria filter=".doc" filecount="1" totalsize="57" sizeunit="1024">
- <information name="Proposal.doc" matchvalue=".doc">
- <![CDATA[ e:\Primary\subfolder\Text Files\Proposal.doc
  ]]>
  </information>
  </criteria>
- <criteria filter=".docx" filecount="1" totalsize="57" sizeunit="1024">
- <information name="Advanced&.docx" matchvalue=".docx">
- <![CDATA[ e:\Primary\subfolder\Text Files\Advanced&.docx
  ]]>
  </information>
  </criteria>
```

```xml
- <criteria filter=".exe" filecount="1" totalsize="16" sizeunit="1024">
- <information name="GimmeFiles.exe" matchvalue=".exe">
- <![CDATA[ e:\Primary\subfolder\GimmeFiles.exe
  ]]>
…
  </information>
  </criteria>
- <criteria filter=".gif" filecount="1" totalsize="888" sizeunit="1024">
- <information name="poppies1920.gif" matchvalue=".gif">
- <![CDATA[ e:\Primary\subfolder\Pictures\poppies1920.gif
  ]]>
  </information>
  </criteria>
- <criteria filter=".jpeg" filecount="1" totalsize="468" sizeunit="1024">
- <information name="backtrack.jpeg" matchvalue=".jpeg">
- <![CDATA[ e:\Primary\subfolder\Pictures\backtrack.jpeg
  ]]>
  </information>
  </criteria>
- <criteria filter=".jpg" filecount="5" totalsize="2569" sizeunit="1024">
- <information name="arctica1920.jpg" matchvalue=".jpg">
- <![CDATA[ e:\Primary\subfolder\Pictures\arctica1920.jpg
  ]]>
  </information>
  </criteria>
- <criteria filter=".ods" filecount="1" totalsize="3" sizeunit="1024">
- <information name="Spreadsheet.ods" matchvalue=".ods">
- <![CDATA[ e:\Primary\subfolder\Text Files\Spreadsheet.ods
  ]]>
  </information>
  </criteria>
- <criteria filter=".odt" filecount="4" totalsize="828" sizeunit="1024">
- <information name="Investment Final.odt" matchvalue=".odt">
- <![CDATA[ e:\Primary\subfolder\Text Files\Investment Final.odt
  ]]>
  </information>
…
  </criteria>
- <criteria filter=".pdf" filecount="1" totalsize="641" sizeunit="1024">
- <information name="dep_stats.pdf" matchvalue=".pdf">
- <![CDATA[ e:\Primary\subfolder\Text Files\dep_stats.pdf
  ]]>
  </information>
  </criteria>
- <criteria filter=".rtf" filecount="1" totalsize="1" sizeunit="1024">
- <information name="Another Document.rtf" matchvalue=".rtf">
- <![CDATA[ e:\Primary\subfolder\Text Files\Another Document.rtf
  ]]>
  </information>
  </criteria>
- <criteria filter=".txt" filecount="1" totalsize="0" sizeunit="1024">
- <information name="Some Document.txt" matchvalue=".txt">
- <![CDATA[ e:\Primary\subfolder\Text Files\Some Document.txt
  ]]>
  </information>
  </criteria>
- <criteria filter=".xml" filecount="2" totalsize="6" sizeunit="1024">
- <information name="myDetails.xml" matchvalue=".xml">
- <![CDATA[ e:\myDetails.xml
```

```
    ]]>
    </information>
…
    </criteria>
- <criteria filter=".zip" filecount="1" totalsize="69277" sizeunit="1024">
- <information name="Text Files.zip" matchvalue=".zip">
- <![CDATA[ e:\Primary\subfolder\Text Files.zip
    ]]>
    </information>
    </criteria>
    </list>
- <list type="Modified">
- <criteria filter="Within Last Day" filecount="3" totalsize="69283"
sizeunit="1024">
- <information name="Text Files.zip" matchvalue="8/26/2009 4:01:18 PM">
- <![CDATA[ e:\Primary\subfolder\Text Files.zip
    ]]>
    </information>
…
    </criteria>
- <criteria filter="1 Month - 2 Months" filecount="1" totalsize="16"
sizeunit="1024">
- <information name="GimmeFiles.exe" matchvalue="7/17/2009 2:00:44 PM">
- <![CDATA[ e:\Primary\subfolder\GimmeFiles.exe
    ]]>
    </information>
    </criteria>
- <criteria filter="6 Months - 1 Year" filecount="27" totalsize="5512"
sizeunit="1024">
- <information name="Spreadsheet.ods" matchvalue="12/16/2008 8:29:00 AM">
- <![CDATA[ e:\Primary\subfolder\Text Files\Spreadsheet.ods
    ]]>
    </information>
…
    </criteria>
    </list>
- <list type="Owner">
- <criteria filter="Administrators" filecount="31" totalsize="74811"
sizeunit="1024">
- <information name="myDetails.xml" matchvalue="Administrators">
- <![CDATA[ e:\myDetails.xml
    ]]>
    </information>
…
    </criteria>
    </list>
- <list type="Length">
- <criteria filter="Less than 1KB" filecount="2" totalsize="2"
sizeunit="1024">
- <information name="Another Document.rtf" matchvalue="7">
```

```
- <![CDATA[ e:\Primary\subfolder\Text Files\Another Document.rtf
  ]]>
  </information>
…
  </criteria>
- <criteria filter="1KB - 4KB" filecount="1" totalsize="3" sizeunit="1024">
- <information name="Spreadsheet.ods" matchvalue="2274">
- <![CDATA[ e:\Primary\subfolder\Text Files\Spreadsheet.ods
  ]]>
  </information>
  </criteria>
- <criteria filter="4KB - 16KB" filecount="1" totalsize="5" sizeunit="1024">
- <information name="myDetails.xml" matchvalue="4597">
- <![CDATA[ e:\myDetails.xml
  ]]>
  </information>
  </criteria>
- <criteria filter="16KB - 64KB" filecount="6" totalsize="193"
sizeunit="1024">
- <information name="Proposal.doc" matchvalue="57856">
- <![CDATA[ e:\Primary\subfolder\Text Files\Proposal.doc
  ]]>
  </information>
…
  </criteria>
- <criteria filter="64KB - 256KB" filecount="1" totalsize="161"
sizeunit="1024">
- <information name="Eastern Fire.jpg" matchvalue="164026">
- <![CDATA[ e:\Primary\subfolder\Pictures\Eastern Fire.jpg
  ]]>
  </information>
  </criteria>
- <criteria filter="256KB - 1MB" filecount="8" totalsize="5170"
sizeunit="1024">
- <information name="Rough (Formated).odt" matchvalue="782959">
- <![CDATA[ e:\Primary\subfolder\Text Files\Rough (Formated).odt
  ]]>
  </information>
- <information name="dep_stats.pdf" matchvalue="655518">
…
  </criteria>
- <criteria filter="64MB - 256MB" filecount="1" totalsize="69277"
sizeunit="1024">
- <information name="Text Files.zip" matchvalue="70938669">
- <![CDATA[ e:\Primary\subfolder\Text Files.zip
  ]]>
  </information>
  </criteria>
  </list>
  </DswInventory>
```

B.4 Example of a Filtered Inventory

In this example, assume that you want a filtered inventory for the Dynamic File Services pair that has a primary path of e:\. You want to find JPG files with file sizes greater than 1 MB. You perform the following tasks to manually generate a report:

B.4.1 Create a Command File

Use a text editor to create a command file called `FSCommands.txt` in the DynamicFS folder. The first line is the primary path for the DynamicFS pair. The second line requests a summary report to be created and specifies the output file for the summary report. The third line requests a detailed report to be created and specifies the output file for the detailed report. No inventory options are specified, so all inventory options are enabled.

```
e:\
/summary=e:\mySummary.xml
/detailed=e:\myDetails.xml
/size>1024
/extension=*.jpg
```

B.4.2 Run the File System Inventory Utility

1 Log in to the server as the Administrator user, or as a user in the Administrators group.

2 Open a *Command Prompt* console, then go to the `DynamicFS` folder.

3 At the prompt, enter

```
DswInventory.exe FSCommands.txt
```

B.4.3 View the Summary Report

The summary results are written to the `e:\mySummary.xml` file. The following is sample output of a summary report:

```
 <?xml version="1.0" encoding="utf-8" standalone="yes" ?>
- <DswInventory GenerationDateTime="8/27/2009 3:13:10 PM" generation="summary"
platform="Win32NT" OS="Microsoft Windows NT 5.2.3790 Service Pack 2">
- <folderlist>
- <folder>
- <![CDATA[ e:\
  ]]>
  </folder>
  </folderlist>
- <list type="Extension">
  <criteria filter=".jpg" filecount="5" totalsize="2569" sizeunit="1024" />
  </list>
- <list type="Length">
  <criteria filter="64KB - 256KB" filecount="1" totalsize="161"
sizeunit="1024" />
  <criteria filter="256KB - 1MB" filecount="4" totalsize="2408"
sizeunit="1024" />
  </list>
  </DswInventory>
```

B.4.4 View the Detailed Report

The detailed results are written to the `e:\myDetails.xml` file. The following is sample output from a detailed report:

```xml
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
- <DswInventory GenerationDateTime="8/27/2009 3:13:10 PM"
generation="detailed" platform="Win32NT" OS="Microsoft Windows NT 5.2.3790
Service Pack 2">
- <folderlist>
- <folder>
- <![CDATA[ e:\
  ]]>
  </folder>
  </folderlist>
- <list type="Extension">
- <criteria filter=".jpg" filecount="5" totalsize="2569" sizeunit="1024">
- <information name="arctica1920.jpg" matchvalue=".jpg">
- <![CDATA[ e:\Primary\subfolder\Pictures\arctica1920.jpg
  ]]>
  </information>
- <information name="Eastern Fire.jpg" matchvalue=".jpg">
- <![CDATA[ e:\Primary\subfolder\Pictures\Eastern Fire.jpg
  ]]>
  </information>
- <information name="eventide1920.jpg" matchvalue=".jpg">
- <![CDATA[ e:\Primary\subfolder\Pictures\eventide1920.jpg
  ]]>
  </information>
- <information name="lastlight1920.jpg" matchvalue=".jpg">
- <![CDATA[ e:\Primary\subfolder\Pictures\lastlight1920.jpg
  ]]>
  </information>
- <information name="vigil1920.jpg" matchvalue=".jpg">
- <![CDATA[ e:\Primary\subfolder\Pictures\vigil1920.jpg
  ]]>
  </information>
  </criteria>
  </list>
- <list type="Length">
- <criteria filter="64KB - 256KB" filecount="1" totalsize="161"
sizeunit="1024">
- <information name="Eastern Fire.jpg" matchvalue="164026">
- <![CDATA[ e:\Primary\subfolder\Pictures\Eastern Fire.jpg
  ]]>
  </information>
  </criteria>
- <criteria filter="256KB - 1MB" filecount="4" totalsize="2408"
sizeunit="1024">
- <information name="vigil1920.jpg" matchvalue="642827">
- <![CDATA[ e:\Primary\subfolder\Pictures\vigil1920.jpg
  ]]>
  </information>
- <information name="lastlight1920.jpg" matchvalue="705456">
- <![CDATA[ e:\Primary\subfolder\Pictures\lastlight1920.jpg
  ]]>
  </information>
- <information name="eventide1920.jpg" matchvalue="544622">
- <![CDATA[ e:\Primary\subfolder\Pictures\eventide1920.jpg
  ]]>
  </information>
- <information name="arctica1920.jpg" matchvalue="572311">
- <![CDATA[ e:\Primary\subfolder\Pictures\arctica1920.jpg
  ]]>
```

```
</information>
</criteria>
</list>
</DswInventory>
```

B.5 Additional Information

A file system inventory of each Dynamic File Services pair is automatically generated daily with the pair history run. You can use the Management Console to view graphical displays of this report, and to drill down into the report to see the individual files in various categories. For information, see Section 10.3, "Viewing the Pair History," on page 122.

Dynamic File Services Synchronize Pair Utility

C

The Novell® Dynamic File Services (DynamicFS) Synchronize Pair utility (`DswSyncPair.exe`) provides a way to detect and report conflicts for duplicate files and mismatched ACL permissions and attributes on folders. On Windows servers, the Synchronize Pair utility is found in the directory where you installed DynamicFS. By default, DynamicFS is installed in the `C:\Program Files\Dynamic File Services` directory.

- ◆ Section C.1, "DswSyncPair," on page 181
- ◆ Section C.2, "Additional Information," on page 183

C.1 DswSyncPair

Description

The Dynamic File Services Synchronize Pair utility is used to detect duplicate files in the DynamicFS pair structure or to detect folders with attribute or ACL permission differences. It can generate reports in CSV and XML format.

Syntax

```
DswSyncPair.exe -pair="<pairname | guid>" [options]

DswSyncPair.exe -source="path" -target="path" [options]
```

Log in to the DynamicFS server as the Administrator user (or a user with Administrator privileges), then issue the command in the *Command Prompt* console. It does not matter if the user is also a member of the Dynamic File Services group.

If you are using this command in a script, you must escape the quotation mark characters by preceding them with a backslash (\). You can also use the `-silent` option to turn off the screen output. For example:

```
DswSyncPair.exe -pair=\"<pairname | guid>\" [options] -silent

DswSyncPair.exe -source=\"path\" -target=\"path\" [options] -silent
```

Options

-pair="<pairname | guid>"

Use this option look for the specified pair in the pair database to determine the paths to use for the source and target paths. Do not use this option with the `-source` and `-target` options.

Example

```
-pair="MyPair"
```

-source="path"

Use this option to specify the path to use for the primary path. This option must be used in combination with the `-target` option.

Do not use this option with the -pair option.

Example

```
-source="c:\primary"
```

-target="path"

Use this option to specify the path to use for the secondary path. This option must be used in combination with the -source option.

Do not use this option with the -pair option.

Example

```
-target="g:\shadow"
```

-silent

If this option is specified, screen output is not generated.

Example

```
-silent
```

-csv="reportname"

Use this option to generate an output report in CSV format.

If this option is used with the -files option, the output file is named *reportname*.files.csv.

If this option is used with the -folders option, the output file is named *reportname*.folders.csv.

Example

```
-csv="cvsReport"
```

The possible reports generated are csvReport.files.csv and csvReport.folders.csv.

-xml="reportname"

Use this option to generate an output report in XML format.

If this option is used with the -files option, the output file is named *reportname*.files.xml.

If this option is used with the -folders option, the output file is named *reportname*.folders.xml.

Example

```
-xml="xmlReport"
```

The possible reports generated are xmlReport.files.xml and xmlReport.folders.xml.

-files

If this option is specified, a check is performed for duplicate files on the specified source and target paths.

Example

```
-files
```

-folders

If this option is specified, a check is performed for folder attribute and ACL permission differences on the specified source and target paths.

Example

```
-folders
```

Examples

Check for Duplicate Files

```
DswSyncPair.exe -pair="My DSW Pair" -files -csv="myCsvReport"
```

Looks in the pair database for the source and target paths of the pair named My DSW Pair. Checks for duplicate files on the source and target paths. Produces a report in CSV format. The report file generated is `myCsvReport.files.csv`.

Check for Folders with Mismatched Attributes and ACLs

```
DswSyncPair.exe -pair="My DSW Pair" -folders -xml="myXmlReport"
```

Looks in the pair database for the source and target paths of the pair named My DSW Pair. Checks for folders that have mismatched attributes and ACLs on the source and target paths. Produces a report in XML format. The report file generated is `myXmlReport.folders.xml`.

Check for Duplicate Files and Folders Mismatched Attributes and ACLs

```
DswSyncPair.exe -pair="My DSW Pair" -folders -files -xml="myXmlReport"
-csv="myCsvReport"
```

Looks in the pair database for the source and target paths of the pair named My DSW Pair. Checks for duplicate files and for folders that have mismatched attributes and ACLs on the source and target paths. Produces a report in XML format and in CSV format.

The report files generated are:

```
myCsvReport.files.csv
myCsvReport.folders.csv
myXmlReport.files.xml
myXmlReport.folders.xml
```

C.2 Additional Information

For information about using the DswSyncPair utility for reporting on files and folders in a Dynamic File Services pair, see the following:

- Section 8.8, "Reporting Conflicts for Attributes and ACL Permissions on Folders," on page 90
- Section 8.9, "Reporting Conflicts for Duplicate Files," on page 91

Dynamic File Services Configuration Dump Utility

<div style="text-align: right; font-size: 2em;">D</div>

The Novell® Dynamic File Services (DynamicFS) Configuration Dump utility (`DswDump.exe`) reports a server's DynamicFS configuration, settings, and logs to a file called `Config.txt` in the folder where you installed DynamicFS. The default location of the install folder is `C:\Program Files\Dynamic File Services`.

- Section D.1, "DswDump," on page 185
- Section D.2, "Config.txt Output," on page 185

D.1 DswDump

Description

The Dynamic File Services Configuration Dump utility is a tool that consolidates current information about DynamicFS running on the server, and writes it all to a single file. This tool reads the DynamicFS configuration files, database files, and logs, and dumps the information into a single file called `Config.txt` in the folder where you installed DynamicFS.

Syntax

Log in as the Administrator user, or as a user in the Dynamic File Services group, then issue this command in a *Command Prompt* console.

```
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 DynamicFS).

D.2 Config.txt Output

The Dynamic File Services Configuration Dump utility writes information to the `Config.txt` file in the following major categories:

```
[ DswDump Runtime Information ]

[ Windows Configuration ]

[ Dynamic File Services Configuration ]

[ Filter Information ]

[ Dynamic File Services Folder Hierarchy ]

[ Pairs ]

[ Policies ]
[ Audit Information ]

[ MS Event Logger ]

[ Log files ]
```

Quick Reference for the Dynamic File Services Management Tools

<div style="text-align: right; font-size: 3em;">E</div>
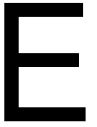
This section provides a quick reference for the Novell® Dynamic File Services (DynamicFS) tools, including the Management Console, Service Controller, Repair GUI, and Uninstall Wizard.

E.1 Server Properties

- General
  - System
    - Operating system
    - Server time zone
  - Computer
    - Processor
    - RAM
  - DynamicFS Version
- Disk details
  - Disks on the computer that are seen as native drives
  - Capacity (GB)
  - Free space (GB)
  - Free space (%)
  - Graphical display of capacity
  - History
    - Graphical display of the disk capacity over time

- Log files
  - `DswMcpCore.log`
  - `DswEnforcer.log`

E.2 Pair Properties

- General
  - Primary path
  - Secondary path
  - Share name
- Associations
  - Add policy associations for the pair.
  - Remove policy associations for the pair.
- Include/Exclude
  - Restriction options: None, Exclude, None.
  - Add/Remove directories to be included or to be excluded.
- Pair history
  - Schedule when to run the pair history scan.

E.3 Policy Properties

- General
  - Direction
    - Primary to Secondary
    - Secondary to Primary
  - Frequency
    - Scheduled/Not Scheduled
    - Frequency and when
      - Hourly
      - Daily
      - Weekly
      - Monthly
  - Filter options
    - File size
    - Last accessed
    - Last modified
    - File extensions
  - Description

- Associations
    - Add pair associations for the policy.
    - Remove pair associations for the policy.

E.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
        - Run 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
  - Preview results

E.5 Server Wizard

- IP/DNS
- Port
- Username
- Password

E.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 (<)
      - Size
      - Units: Bytes, Kilobytes, Megabytes, Gigabytes
    - Last accessed
      - Greater than (>) or Less than (<)
      - Period
      - Units: Days, Weeks, Months, Years
    - Last modified
      - Greater than (>) or Less than (<)
      - Period
      - Units: Days, Weeks, Months, Years
    - File extensions
      - Comma delimited list of extensions with no spaces before or after commas.
- 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
- Policy name and description
- Policy summary

E.7 Pair Wizard

- Pair paths
  - Primary path
  - Secondary path
- Pair name
- Policy to pair association

E.8 Policy Wizard

- Policy rules
  - Direction
    - Primary to Secondary
    - Secondary to Primary
  - Filter options
    - File size
      - Greater than (>) or Less than (<)
      - Size
      - Units: Bytes, Kilobytes, Megabytes, Gigabytes
    - Last accessed
      - Greater than (>) or Less than (<)
      - Period
      - Units: Days, Weeks, Months, Years
    - Last modified
      - Greater than (>) or Less than (<)

- ◆ Period
  - ◆ Units: Days, Weeks, Months, Years
- ◆ File extensions
  - ◆ Comma delimited list of extensions with no spaces before or after commas.
- ◆ 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
- ◆ Policy name and description
- ◆ Pair to policy association

E.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 directory
    - Language
    - Product version
    - Copyright

E.10 Right-Click Menus

E.10.1 Server Folder

- Server Wizard

E.10.2 Server

- Disconnect / Connect
- Setup Wizard
- Properties

E.10.3 Pair Folder

- Pair Wizard

E.10.4 Pair

- Unlink
- Execute now
  - Policy list (if multiple policies)
- Preview now
  - Policy list (if multiple policies)
- Stop running process
- Statistics
- Properties

E.10.5 Policy Folder

- Policy Wizard
- Import policy

E.10.6 Policy

- Export
- Delete
- Execute now
  - Pair list (if multiple pairs)
- Properties

E.11 Dynamic File Services 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
- ◆ Service enabled/Stop Service
- ◆ Service disabled/Start Service
- ◆ About Novell Dynamic File Services

E.12 Dynamic File Services Repair Tool

- ◆ Repair type
  - ◆ Repair
  - ◆ Report
- ◆ Repair option
  - ◆ Full
  - ◆ Pairs
  - ◆ Policies

E.13 Dynamic File Services Uninstall Wizard

- ◆ Modify
- ◆ Repair
- ◆ Remove

Keyboard Shortcuts for the Dynamic File Services Management Console

<div style="text-align: right">**F**</div>

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.

- Section F.1, "Using Keyboard Shortcuts," on page 197
- Section F.2, "Quick Reference for Keyboard Shortcuts," on page 197
- Section F.3, "Navigating with Keyboard Shortcuts," on page 198

F.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.

F.2 Quick Reference for Keyboard Shortcuts

Table F-1 *Dynamic File Services 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

To do this	Press
Go to the next pane in a wizard. Apply the changes and close the wizard (when there is no *Next* button).	Alt+N
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
Move down one topic in a displayed menu. Move down to the next option in a radio-button selection.	Down-arrow
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. Move up to the previous option in a radio-button selection.	Up-arrow
Select (check) or deselect (clear) a check box. Perform the action assigned to the selected button.	Spacebar
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

F.3 Navigating with Keyboard Shortcuts

F.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.

F.3.2 Wizards

In the DynamicFS 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 key and press Enter to close without saving.

F.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.

Silent Install Options for Dynamic File Services

G

The Novell® Dynamic File Services (DynamicFS) InstallShield Wizard application supports InstallShield silent install options.

G.1 InstallShield Silent Install Options

The following table identifies commonly used silent install options of InstallShield:

InstallShield Option	Description
`/r`	Records installation responses to an answer file.
	Use this option with the graphical installer to create the answer file (such as `C:\Windows\setup.iss`) that is needed to perform a silent install.
`/s`	Silently installs the application.
`/sms`	Causes the installer to pause until the installation finishes.
`/f1"answer_file_filename.iss"`	Specifies the filename of the answer file.

For information about other InstallShield silent and unattended install options, see *Unattended/ Silent Installation Switches* (http://unattended.sourceforge.net/installers.php) on the SourceForge.Net* Web site.

G.2 Creating the Silent Install Answer File for Dynamic File Services

1 Log in as the Administrator user (or as a user with Administrator privileges).

2 Create the InstallShield answer file on the same platform and hardware setup where you plan to use the silent install.

  2a In a *Command Prompt* console, start the GUI install and use the `/r` option to record your responses.

Architecture	Enter
32-bit	`DswSetup-x86.exe /r`
64-bit	`DswSetup-x64.exe /r`

The answer file is saved to the Windows System root folder, such as
`C:\Windows\setup.iss`.

2b Using the InstallShield GUI, install Dynamic File Services as described in Section 4.2, "Installing Dynamic File Services with the InstallShield GUI," on page 44.

Your responses to the install options in the GUI are captured to the answer file, such as `C:\Windows\setup.iss`.

2c Copy `setup.iss` to the same location as the DynamicFS GUI install executable file.

You can rename the answer file to a name that indicates the install scenario.

2d Repeat the process for each additional install scenario you need to create for the current platform and hardware setup.

G.3 Silently Installing Dynamic File Services

1 On the machine where you want to silently install Dynamic File Services, copy the DynamicFS setup file and answer file into a folder.

2 In a *Command Prompt* console on the machine, enter

```
DswSetup-<platform>.exe /s /f1"answer_file_filename"
```

Replace *platform* with x86 (for 32-bit platforms) or x64 (for 64-bit platforms). Replace the *answer_file_filename* with the InstallShield answer file, such as `setup.iss`.

For example, to install DynamicFS on a 32-bit platform, use the `DswSetup-x86.exe` file and specify the answer file that you want to use, enter the following in the *Command Prompt* console:

```
DswSetup-x86.exe /s /f1"setup.iss"
```

The following command assumes the file is named `setup.iss` and is in the `C:\Windows` directory or in the same directory as the install executable:

```
DswSetup-x86.exe /s
```

You can also use the `/sms` option to cause the installer to pause until the installation completes:

```
DswSetup-x86.exe /s /sms
```

Using the Uninstall Tool to Modify, Repair, or Remove Dynamic File Services

H

You can use the Uninstall tool to modify, repair, or uninstall Novell® Dynamic File Services (DynamicFS).

- Section H.1, "Modifying Dynamic File Services," on page 203
- Section H.2, "Repairing Dynamic File Services," on page 203
- Section H.3, "Removing Dynamic File Services," on page 204

H.1 Modifying Dynamic File Services

The *Modify* option in the Dynamic File Services Uninstall tool allows you to add or remove the Service component of the Dynamic File Services software on a computer. The DynamicFS Service is typically installed only on those servers where you want to create pairs and policies.

1 Log in as the Administrator user or as a user with Administrator privileges that is a member of the Dynamic File Services group.

2 Disable the DynamicFS Service as described in Section 6.2.3, "Stopping the Dynamic File Services Service," on page 62.

3 Select *Start > Programs > DynamicFS > Uninstall DynamicFS*.

The InstallShield Wizard opens.

4 Select *Modify*, then click *Next*:

5 Select *Custom*, then do one of the following:

- Select the *Service* check box to add the service to the computer.
- Deselect (clear) the *Service* check box to remove the service from the computer.

6 Click *Next* and follow the on-screen instructions to complete the software change.

7 After the change is complete, click *Finish* to close the wizard.

8 Enable the DynamicFS Service as described in Section 6.2.2, "Starting the Dynamic File Services Service," on page 62.

H.2 Repairing Dynamic File Services

The *Repair* option in the Dynamic File Services Uninstall tool allows you to reinstall the currently installed components of the Dynamic File Services software on a computer.

1 Log in as the Administrator user or as a user with Administrator privileges that is a member of the Dynamic File Services group.

2 Disable the DynamicFS Service as described in Section 6.2.3, "Stopping the Dynamic File Services Service," on page 62.

3 Select *Start > Programs > DynamicFS > Uninstall DynamicFS*.

The InstallShield Wizard opens.

4 Select *Repair*, then click *Next* and follow the on-screen instructions to complete the software repair.

5 Click *Finish* to close the wizard.

6 Enable the DynamicFS Service as described in Section 6.2.2, "Starting the Dynamic File Services Service," on page 62.

H.3 Removing Dynamic File Services

The *Remove* option in the Dynamic File Services Uninstall tool automatically removes the Dynamic File Services program files that were installed. You can separately specify whether you want to also remove all of the files in the `DynamicFS` folder that were created since the install, which includes the pair and policy databases.

- Section H.3.1, "Planning to Uninstall Dynamic File Services," on page 204
- Section H.3.2, "Before Uninstalling Dynamic File Services," on page 205
- Section H.3.3, "Uninstalling Dynamic File Services," on page 205

H.3.1 Planning to Uninstall Dynamic File Services

Consider the guidelines in this section when planning to uninstall Dynamic File Services.

- "Locating Files" on page 204
- "Stopping Policy Runs" on page 204
- "Keeping Pair and Policy Database Configuration Files" on page 204

Locating Files

When you uninstall the DynamicFS software, the two paths in a pair are automatically unlinked. The files in each pair remain in their current locations at the time of the uninstall (that is, residing on the primary path or on the secondary path).

Before uninstalling DynamicFS, we recommend that for each pair on the server, you verify that the primary path and secondary path contain the files that you intend. You might need to create new policies to move the files to the desired final destination. After you have located the files, you should disassociate all policies from the pair, or unlink the pairs so that the files remain where you intend them to be.

Stopping Policy Runs

Policies should be in an *Idle* state before you attempt to uninstall the software. Policy runs are not completed gracefully if you uninstall the software in mid-run. You can wait until all policy runs are completed, or stop the policy runs manually.

Keeping Pair and Policy Database Configuration Files

If you plan to reinstall DynamicFS, you can reuse the existing pair and policy databases if you specify that you want to keep them during the uninstall.

H.3.2 Before Uninstalling Dynamic File Services

On some Windows platforms, you might be asked to reboot after an uninstall if the Dynamic File Services Service and Service Controller are running when you begin the uninstall.

1 Log in as the Administrator user or as a user in the Dynamic File Services group.

2 Disable the DynamicFS Service as described in Section 6.2.3, "Stopping the Dynamic File Services Service," on page 62.

3 Right-click the *Dynamic File Services Service Controller* icon in the Windows notification area, then select *Exit*.

H.3.3 Uninstalling Dynamic File Services

1 Log in as an Administrator user (or as a user with Administrator privileges).

2 Select *Start > Programs > Dynamic File Services > Uninstall Dynamic File Services*.

The InstallShield Wizard opens.

3 Select *Remove*, then click *Next*.

4 In the confirmation dialog box, specify whether you want to *Remove all files created by Dynamic File Services*. These are files in the `Dynamic File Services` folder that were created since the install, which includes the pair and policy databases.

Do one of the following:

- ◆ Deselect the check box to keep the files. This is the default.
- ◆ Select the check box to remove the files.

5 Click *OK* to confirm the uninstall.

6 After the uninstall is complete, click *Finish* to close the Uninstall tool.

7 If you are prompted to do so, restart the computer.

Using the Uninstall Tool to Modify, Repair, or Remove Dynamic File Services in a Windows Cluster

You can use the Novell® Dynamic File Services (DynamicFS) Uninstall tool to modify, repair, or remove the software components. This section provides general guidelines for modifying, repairing, or removing DynamicFS on servers in a Windows cluster.

> **IMPORTANT:** The Windows cluster configuration, management, terminology, and tools can vary depending on the version of Windows Server you are running and on how you set up your cluster and cluster resources. Adjust the instructions in this section as needed for your cluster environment.
>
> For all issues related to Windows cluster configuration and management, see the official Microsoft documentation for your Windows Server operating system in the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/default.aspx).

- Section I.1, "Modifying Dynamic File Services in a Cluster," on page 207
- Section I.2, "Repairing Dynamic File Services in a Cluster," on page 208
- Section I.3, "Removing Dynamic File Services in a Cluster," on page 208

I.1 Modifying Dynamic File Services in a Cluster

The *Modify* option in the Dynamic File Services Uninstall tool allows you to add or remove the DynamicFS Service component on a computer. The DynamicFS Service is typically installed only on those servers where you want to create pairs and policies.

In a cluster, you must modify the software on each node in turn in order to update the information stored locally on each server. The following procedure assumes a two-node failover cluster. Modify the steps as necessary if you have more nodes.

1 Modify the installation setup on the active node:

    1a Log in as the Administrator user or as a user with Administrator privileges that is a member of the Dynamic File Services group.

    1b Use the Windows cluster administration tool to stop the DynamicFS Service by taking its cluster resource offline.

    1c Modify the installed components as described in Step 3 through Step 7 in Section H.1, "Modifying Dynamic File Services," on page 203.

2 Use Windows cluster administration tool to move the following cluster resources to the second node:

- The shared disk that contains the DynamicFS software
- The DynamicFS Service

3 Repeat Step 1 for the second cluster node, then continue with Step 4.

4 (Optional) Use the Windows cluster administration tool to move the DynamicFS Service and disk resources back to the first node.

5 Log in to the active cluster node as the Administrator user or as a user that is a member in the Dynamic File Services group.

6 Use the Windows cluster administration tool to start the DynamicFS Service by bringing its cluster resource online.

I.2 Repairing Dynamic File Services in a Cluster

The *Repair* option in the Dynamic File Services Uninstall tool allows you to reinstall the currently installed components of the Dynamic File Services software on a computer.

In a cluster, you must repair the software on each node in turn to update the information stored locally on each server. The following procedure assumes a two-node failover cluster. Modify the steps as necessary if you have more nodes.

1 Repair the currently installed components on the active node:

    1a Log in as the Administrator user or as a user with Administrator privileges that is a member of the Dynamic File Services group.

    1b Use the Windows cluster administration tool to stop the DynamicFS Service by taking its cluster resource offline.

    1c Repair the installed components as described in Step 3 through Step 5 in Section H.2, "Repairing Dynamic File Services," on page 203.

2 Use Windows cluster administration tool to move the following cluster resources to the second node:

    ◆ The shared disk that contains the DynamicFS software

    ◆ The DynamicFS Service

3 Repeat Step 1 for the second node, then continue with Step 4.

4 (Optional) Use the Windows cluster administration tool to move the DynamicFS Service and disk resources back to the first node.

5 Log in to the active cluster node as the Administrator user or as a user in the Dynamic File Services group.

6 Use the Windows cluster administration tool to start the DynamicFS Service by bringing its cluster resource online.

I.3 Removing Dynamic File Services in a Cluster

The *Remove* option in the Dynamic File Services Uninstall tool removes the DynamicFS software from a computer. By default, it deletes all of the configuration and log files in the DynamicFS installation location (default `C:\Program Files\Dynamic File Services`), clears DynamicFS entries in the registry, and removes the SSL certificate and Dynamic File Services group. The uninstall allows you to specify whether to keep the pair and policy databases. The files on the primary paths and secondary paths are untouched.

I.3.1 Planning to Uninstall Dynamic File Services in a Cluster

For general uninstall guidelines, see Section H.3.1, "Planning to Uninstall Dynamic File Services," on page 204.

In a cluster, you must remove the software on each node in turn. Before you attempt to uninstall, make a copy of the DynamicFS installation folder (default is `C:\Program Files\Dynamic File Services`) and store it in a temporary location on the server. After the uninstall is complete, copy the files back to the install location on the shared disk, then move the shared disk and the DynamicFS Service to the next node. This rolling uninstall approach allows the Uninstall tool to successfully clean up the registry and other information that is stored locally on each server in the cluster.

I.3.2 Uninstalling Dynamic File Services in a Cluster

The following procedure assumes a two-node failover cluster. Modify the steps as necessary if you have more nodes.

1 Uninstall DynamicFS on the active node:

  1a Log in as the Administrator user or as a user with Administrator privileges that is a member of the Dynamic File Services group.

  1b Make a copy of the `DynamicFS` folder.

     For example, copy `S:\DynamicFS` to `S:\Copy of DynamicFS`.

  1c Use the Windows cluster administration tool to stop the DynamicFS Service by taking its cluster resource offline.

  1d Uninstall DynamicFS on the first node as described in Section H.3.3, "Uninstalling Dynamic File Services," on page 205.

  1e Move the copy of the `Dynamic File Services` folder back to the shared disk install location.

     For example, rename `S:\Copy of DynamicFS` to `S:\DynamicFS`.

2 Use Windows cluster administration tool to move the following cluster resources to the second node:

   ◆ The shared disk that contains the DynamicFS software

   ◆ The DynamicFS Service

3 Uninstall DynamicFS on the second cluster node.

  3a Log in as the Administrator user or as a user with Administrator privileges that is a member of the Dynamic File Services group.

  3b Use the Windows cluster administration tool to stop the DynamicFS Service by taking its cluster resource offline.

  3c Uninstall DynamicFS on the second node as described in Section H.3.3, "Uninstalling Dynamic File Services," on page 205.

4 (Optional) Use the Windows cluster administration tool to move shared disk back to the first node.

Dynamic File Services Components

J

This section identifies the various components for Novell® Dynamic File Services (DynamicFS) and their primary use. The files are located in the folder where you installed the software. The default install location is `C:\Program Files\Dynamic File Services`.

- Table J-1, "Dynamic File Services Components," on page 211
- Table J-2, "Open Source and Third-Party Components," on page 213

Table J-1 *Dynamic File Services Components*

Component	Used for
`audit\DswAuditCfg.xml`	Configuration for logging events for the DynamicFS management events.
`audit\DswAuditLog.xml`	Event log for DynamicFS management events.
`DswApi.dll`	Web Services API.
`DswBuiltInRules.dll`	Policy rules engine.
`DswCert.exe`	Manages the DynamicFS SSL certificate.
`DswCertificateLib.dll`	DynamicFS SSL certificate handling library.
`DswCli.exe`	DynamicFS command line interface management utility for pairs and policies.
`DswCore.xml`	DynamicFS configuration information.
`DswDump.exe`	Configuration Dump utility for use when working with Novell Support.
`DswEnforcer.config.xml`	Configuration for logging events for the DynamicFS Enforcer. This file is not created until the `DswEnforcer.exe` application first runs.
`DswEnforcer.exe`	Executes policy tasks to move files from the primary path to the secondary path, or from the secondary path to the primary path.
`DswEnforcer.log`	Event log for the DynamicFS Enforcer that runs policies. This file is not created until the `DswEnforcer.exe` application first runs.
`dswflt` folder	Contains information used by the DynamicFS Filter Driver.
`dswflt.exe`	DynamicFS Filter Driver. Provides the merged file tree view to users via the network share on a pair.

Component	Used for
`DswInventory.config.xml`	Configuration for logging events for the DynamicFS file system inventory. This file is not created until the `DswInventory.exe` application first runs.
`DswInventory.exe`	File System Inventory application.
`DswInventory.log`	Event log for the DynamicFS file system inventory. This file is not created until the `DswInventory.exe` application first runs.
`DswIoctlsLib.dll`	Win32 `Ioctl` to Filter Driver communication.
`DswIpcClient.dll`	Local IPC client.
`DswIpcCore.dll`	Local IPC core engine.
`DswIpcListener.dll`	Local IPC server.
`DswLib.dll`	DynamicFS Common Library.
`DswMcpCore.config.xml`	Configuration for logging events for the DynamicFS Service.
`DswMcpCore.dll`	DynamicFS Service engine.
`DswMcpCore.log`	Event log for the DynamicFS Service.
`DswMcpDatabase.dll`	Pair and policy database engine.
`DswMgmtConsole.exe`	DynamicFS Management Console for creating and managing pairs and policies.
`DswRepair.exe`	Repairs DynamicFS database files.
`DswResources.dll`	Strings for localization.
`DswServers.xml`	Configuration information about the servers set up in the DynamicFS Management Console on this computer. This file is created when you first set up a server for management.
`DswService.exe`	DynamicFS Service application.
`DswServiceController.exe`	DynamicFS applet for the Windows notification area: ◆ Launches the DynamicFS Management Console ◆ Starts or stops the DynamicFS Service ◆ Enables or disables the Windows Firewall access ◆ Configures the DynamicFS Service port ◆ Configures the DynamicFS SSL certificate
`DswSyncPair.config.xml`	Configuration for logging events for the DynamicFS Synchronize Pair application. This file is not created until you use the `DswSyncPair.exe` application.
`DswSyncPair.exe`	Detects and reports duplicate files or mismatched attributes and ACL permissions for folders on the DynamicFS pair.

Component	Used for
DswSyncPair.log	Event log for the DynamicFS Synchronization Pair application.
	This file is not created until you use the DswSyncPair.exe application.
LocalDrives folder	Contains information about the local drives on the server.
Pairs folder	Contains the pairs database files.
Policies folder	Contains the policies database files.
SnapShot folder	Contains backup copies of the pair and policies databases for use by the Repair tool.

Table J-2   *Open Source and Third-Party Components*

Component	Used for
log4net.dll	Apache Logging Services open source project. Provides cross-language logging services for application debugging and auditing.
ZedGraph.dll	ZedGraph open source project. Uses the Plossum library for creating two-dimensional line and bar graphics.
Plossum.dll C5.dll	Plossum open source project. A class library collection written in C# to provide functionality for writing and communicating with console applications.
InstallShield 2009	Flexera* Software (formerly Acresso Software). Provides the install, modify, repair, and uninstall features for the DynamicFS software.