docsys (en) 25 September 2013

Administration Guide

Novell Storage Manager 3.1.1 for Active Directory

October 17, 2013

Novell

Legal Notices

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

Further, Condrey Corporation makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to make changes to any and all parts of the software at any time, without obligation to notify any person or entity of such revisions or changes. See the Software EULA for full license and warranty information with regard to the Software.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Condrey Corporation assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2013 Condrey Corporation. All Rights Reserved.

No part of this publication may be reproduced, photocopied, or transmitted in any fashion with out the express written consent of the publisher.

Condrey Corporation
125 The Parkway, Suite 500
Greenville, SC 29615
U.S.A.
www.condreycorp.com

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.

Contents

About This Guide 9

1 What's New 11

1.1 New in Version 3.1.1 . . . 11
1.2 New in Version 3.1 . . . 12
1.3 New in Version 3.0.4 . . . 13
1.4 New in Version 3.0.3 . . . 13
1.5 New in Version 3.0.2 . . . 13
1.6 New in Version 3.0.1 . . . 13
1.7 New in Version 3.0 . . . 14

2 Overview 17

3 Using NSMAdmin 19

3.1 Launching NSMAdmin . . . 19
3.1.1 Overriding Proxy Settings at Login . . . 20
3.1.2 Enabling Temporary Logging Override . . . 20
3.2 Using the NSMAdmin Interface . . . 21

4 Managing Existing User Storage 23

4.1 Running the GSR Collector . . . 24
4.2 Viewing Anomaly Reports . . . 24
4.3 Running Consistency Check Reports on Existing Storage . . . 25
4.4 Assigning Missing Home Folder Attributes . . . 25
4.5 Standardizing User Home Folder Attributes . . . 27
4.6 Creating a Blocking Policy . . . 27
4.7 Creating a User Home Folder Policy . . . 29
4.8 Removing a Preexisting Process for Creating User Home Folders . . . 34
4.9 Testing the User Home Folder Policy . . . 35
4.10 Performing a Consistency Check . . . 35
4.11 Testing a Rename Event . . . 36
4.12 Testing a Cleanup Rule . . . 36
4.13 What's Next . . . 36

5 Managing User Home Folders 39

5.1 Overview . . . 39
5.2 User Policies . . . 39
5.3 Setting Up a Vaulting Location . . . 40
5.4 Enabling Your Network for Quota Management . . . 40
5.5 Creating a User Home Folder Policy . . . 42
5.5.1 Setting Policy Options . . . 43
5.5.2 Setting Associations . . . 44
5.5.3 Provisioning Options . . . 45
5.5.4 Setting Target Paths . . . 46

5.5.5 Setting Quota Options . . . 47
5.5.6 Setting the Move Schedule . . . 49
5.5.7 Setting Cleanup Options . . . 49
5.5.8 Setting Vault Rules . . . 49
5.5.9 Setting Grooming Rules . . . 51
5.5.10 Notes . . . 51
5.5.11 Policy Summary . . . 51
5.6 Creating a User Profile Path Policy . . . 52
5.6.1 To Create a User Profile Path Policy . . . 52
5.7 Creating a User Remote Desktop Services Home Folder Policy . . . 53
5.7.1 To Create a User Remote Desktop Services Home Folder Policy . . . 53
5.8 Creating a User Remote Desktop Services Profile Path Policy . . . 55
5.8.1 To Create a User Remote Desktop Services Profile Path Policy: . . . 55
5.9 Using a Policy to Manage Inactive Users . . . 57
5.9.1 Creating an Inactive Users Organizational Unit . . . 57
5.9.2 Creating an Inactive Users Folder . . . 57
5.9.3 Creating an Inactive Users Policy . . . 58
5.9.4 Setting Inactive Users Policy Associations . . . 58
5.9.5 Setting Inactive Users Policy Provisioning Options . . . 58
5.9.6 Setting Inactive Users Policy Target Paths . . . 59
5.9.7 Setting Inactive Users Policy Cleanup Options . . . 59
5.10 Copying Policy Data . . . 59
5.11 Using a Policy to Manage Auxiliary Storage . . . 60
5.11.1 Creating an Auxiliary Storage Policy . . . 61
5.11.2 Linking a User Home Folder Policy to an Auxiliary Storage Policy . . . 63
5.11.3 Provisioning Auxiliary Storage for Existing Users . . . 64
5.12 Exporting Policies . . . 64
5.13 Importing Policies . . . 65

6 Managing Existing Collaborative Storage 67

6.1 Assigning a Managed Path to Existing Group-based or Container-based Storage . . . 67
6.2 Creating a Collaborative Storage Policy . . . 70
6.3 Performing Management Actions . . . 73
6.4 Editing Collaborative Storage Policies . . . 75

7 Managing Collaborative Storage 77

7.1 Creating Collaborative Storage Objects in Active Directory . . . 77
7.2 Understanding Collaborative Storage Template Folders . . . 78
7.3 Determining How You Want to Structure Your Collaborative Storage . . . 78
7.4 Creating a Collaborative Storage Template . . . 79
7.5 Setting Up Security for a Collaborative Storage Template . . . 80
7.5.1 Establishing Permissions . . . 83
7.5.2 Configuring Rights for the Group Manager . . . 84
7.5.3 Configuring Rights for the Group Members' Personal Folders . . . 84
7.5.4 Configuring Group Member Rights to Other Folders . . . 84
7.6 Understanding Collaborative Storage Policies . . . 85
7.7 Creating a Group Collaborative Storage Policy . . . 85
7.7.1 Setting Group Policy Options . . . 86
7.7.2 Setting Group Policy Associations . . . 86
7.7.3 Setting Group Policy Provisioning Options . . . 87
7.7.4 Setting Group Policy Target Paths . . . 88
7.7.5 Setting Group Policy Quota Options . . . 89
7.7.6 Setting the Group Policy Move Schedule . . . 91
7.7.7 Setting Group Policy Dynamic Template Processing . . . 91
7.7.8 Setting Group Policy Cleanup Options . . . 92

7.7.9 Setting Group Policy Vault Rules . . . 93
7.7.10 Setting Group Policy Grooming Rules . . . 94
7.8 Creating a Container Collaborative Storage Policy . . . 95
7.8.1 Setting Container Policy Options . . . 95

8 Using Quota Manager 97

8.1 Quota Management Prerequisites . . . 97
8.2 Managing Quotas Through Quota Manager . . . 98
8.3 Understanding Quota Manager Status Indicators . . . 100

9 Mobile Management 103

10 The Network Operations Center Dashboard 105

10.1 Prerequisites . . . 105
10.2 Installing and Configuring the Network Operations Center Dashboard . . . 105
10.3 Using the Network Operations Center Dashboard . . . 108

11 Performing a Cross-Empire Data Migration 111

11.1 Understanding Cross-Empire Data Migration . . . 111
11.1.1 User Storage Migration . . . 112
11.1.2 Collaborative or Group Storage Migration . . . 113
11.1.3 Direct Folder Storage Migration . . . 113
11.2 Security and Ownership . . . 114
11.2.1 Defining an Identity Map for Security and Ownership Migration . . . 114
11.2.2 Using an Identity Map . . . 115
11.3 Prerequisites . . . 115
11.3.1 Prerequisite Tasks . . . 116
11.4 Creating the Migration Proxy Account . . . 117
11.5 Creating and Modifying an Identity Map . . . 119
11.5.1 Creating an Identity Map . . . 119
11.5.2 Importing a Source Path List . . . 127
11.5.3 Adding Source Entries to the Identity Map . . . 129
11.5.4 Adding or Modifying Target Entries to the Identity Map . . . 131
11.5.5 Saving the Identity Map . . . 132
11.5.6 Exporting an Identity Map . . . 132
11.5.7 Importing an Identity Map . . . 132
11.5.8 Generating a Preview Report . . . 133
11.5.9 Review Rights and Trustee Assignment Mappings . . . 135
11.5.10 Adding Entries from Preview Reports . . . 136
11.6 Migration Options . . . 137
11.6.1 Data and Trustees . . . 137
11.6.2 Trustees Only . . . 138
11.6.3 Data Only . . . 138
11.7 Viewing the Migration Log File . . . 138
11.8 Performing a User to User Data Migration . . . 139
11.9 Performing a Folder to User Data Migration . . . 146
11.10 Performing a Group to Group Data Migration . . . 153
11.11 Performing a Folder to Group Migration . . . 159
11.12 Performing a Folder to Folder Migration . . . 166
11.12.1 Migrating to an Existing Target Folder . . . 167
11.12.2 Creating a Target Folder in the Data Migration Wizard . . . 196

12 Reference **205**

12.1 Main Tab . . . 205
12.1.1 Start Page . . . 205
12.1.2 Engine Status . . . 206
12.1.3 Storage Management . . . 207
12.1.4 Management Actions . . . 209
12.1.5 Policy Management . . . 216
12.1.6 Pending Events . . . 219
12.1.7 Path Analysis . . . 220
12.1.8 Object Properties . . . 221
12.1.9 Storage Resource List . . . 221
12.1.10 GSR Collector . . . 223
12.1.11 Scheduled Tasks . . . 224
12.1.12 Data Migration . . . 224
12.2 Reports Tab . . . 224
12.2.1 Consistency Check Reports . . . 224
12.2.2 Action Reports . . . 226
12.2.3 Anomaly Reports . . . 227
12.2.4 Runtime Config . . . 228
12.2.5 Storage Resource Statistics . . . 228
12.2.6 Global Statistics . . . 229
12.3 Configure Tab . . . 230
12.3.1 Engine Config . . . 230
12.3.2 Event Servers . . . 234
12.3.3 Agent Servers . . . 234
12.3.4 File Reporter . . . 237
12.3.5 Client Config . . . 237
12.3.6 Check Updates . . . 239

A Security Specifications **241**

A.1 Windows Firewall Requirements . . . 241
A.2 LSA Rights and Privileges . . . 242
A.3 ProxyRights Group . . . 243
A.4 Windows Clustering via Proxy Agents . . . 244
A.5 NAS Devices . . . 244

B Distributed File System (DFS) **245**

B.1 Creating DFS Namespace Permissions . . . 245
B.2 Configuring DFS Folders . . . 251
B.2.1 Providing Only One Target Per DFS Link . . . 251
B.2.2 Disabling All but One Target Per DFS Link . . . 252
B.2.3 Enabling Multiple Target Paths . . . 253

C Active Directory Schema Extensions **255**

C.1 Attributes . . . 255
C.1.1 ccx-FSFAuxiliaryStorage . . . 255
C.1.2 ccx-FSFManagedPath . . . 256
C.2 Classes . . . 256
C.2.1 ccx-FSFManagedAttributes . . . 256

D AuxMap **259**

E Glossary **263**

F Documentation Updates **265**

F.1 October 17, 2013 . . . 265
F.2 September 26, 2013 . . . 265
F.3 June 12, 2013 . . . 266
F.4 February 13, 2013 . . . 266
F.5 January 18, 2013 . . . 266
F.6 October 15, 2012 . . . 267
F.7 May 18, 2012 . . . 267
F.8 February 2, 2012 . . . 267
F.9 July 5, 2011 . . . 267
F.10 May 16, 2011 . . . 267
F.11 March 16, 2011 . . . 268
F.12 March 1, 2011 . . . 268
F.13 February 14, 2011 . . . 268

About This Guide

This administration guide is written to provide network administrators the conceptual and procedural information for managing user and collaborative storage by using Novell Storage Manager for Active Directory.

- Chapter 1, “What’s New,” on page 11
- Chapter 2, “Overview,” on page 17
- Chapter 3, “Using NSMAdmin,” on page 19
- Chapter 4, “Managing Existing User Storage,” on page 23
- Chapter 5, “Managing User Home Folders,” on page 39
- Chapter 6, “Managing Existing Collaborative Storage,” on page 67
- Chapter 7, “Managing Collaborative Storage,” on page 77
- Chapter 8, “Using Quota Manager,” on page 97
- Chapter 9, “Mobile Management,” on page 103
- Chapter 10, “The Network Operations Center Dashboard,” on page 105
- Chapter 11, “Performing a Cross-Empire Data Migration,” on page 111
- Chapter 12, “Reference,” on page 205
- Appendix A, “Security Specifications,” on page 241
- Appendix B, “Distributed File System (DFS),” on page 245
- Appendix C, “Active Directory Schema Extensions,” on page 255
- Appendix D, “AuxMap,” on page 259
- Appendix E, “Glossary,” on page 263
- Appendix F, “Documentation Updates,” on page 265

Audience

This guide is intended for network administrators who manage user and collaborative network storage resources.

Feedback

We want to hear your comments and suggestions about this guide and the other documentation included with this product. Please use the User Comment 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 Storage Manager 3.1.1 for Active Directory Administration Guide*, visit the Novell Storage Manager Web site (http://www.novell.com/documentation/storagemanager3/index.html).

Additional Documentation

For additional Novell Storage Manager documentation, see the following guide at the Novell Storage Manager Documentation Web site (http://www.novell.com/documentation/storagemanager3/index.html):

- *Novell Storage Manager 3.1.1 for Active Directory Installation Guide*

1 What's New

Novell Storage Manager 3.1.1 for Active Directory has significant architectural and feature enhancements compared to previous versions of the product. An overview of some of the more notable changes in architecture, performance, and features follows:

- Section 1.1, "New in Version 3.1.1," on page 11
- Section 1.2, "New in Version 3.1," on page 12
- Section 1.3, "New in Version 3.0.4," on page 13
- Section 1.4, "New in Version 3.0.3," on page 13
- Section 1.5, "New in Version 3.0.2," on page 13
- Section 1.6, "New in Version 3.0.1," on page 13
- Section 1.7, "New in Version 3.0," on page 14

1.1 New in Version 3.1.1

Leveling Algorithm

The Leveling Algorithm setting of a policy's Target Paths page now lets you structure the home folders so that they are categorized by the first or last letter of a username through a subordinate folder. A new *Leveling Length* field allows you to enter up to 4 characters, making it so that you can organize home folders by year. For more information, see Section 5.5.4, "Setting Target Paths," on page 46.

Pending Events

You can now place comments on deferred pending events. This allows an administrator to specify to other administrators the reason why he or she deferred the event. For more information, see Section 12.1.6, "Pending Events," on page 219.

Bypassable Events

Allows Novell Storage Manager to automatically attempt to address any pending events that can bypass administrative action. For more information, see Section 5.5.1, "Setting Policy Options," on page 43.

Deleting Event Monitors and Agents

Event Monitors and Agents must be deauthorized before they can be deleted. For more information, see "Deleting an Event Monitor" on page 234 and "Deleting an Agent" on page 235.

Displaying Administrative and Hidden Shares:

You have the option to display Active Directory administrative and hidden shares in NSMAdmin. For more information, see Section 12.3.1, “Engine Config,” on page 230.

1.2 New in Version 3.1

Cross-Empire Data Migration

For file to file migrations, Novell Storage Manager now lets you identify and move all files that are new or have been modified after a given date. Additionally, you can verify that all of the files you wanted to migrate from a source server have been migrated. You use four new utilities to perform these tasks:

- **novscan.nlm:** A NetWare NLM that scans the contents of the target server and determines which files have been modified or created since you performed a preliminary file to file migration.
- **NovScanConfig.exe:** This Windows executable configures what file system data you want identified from the NetWare or Novell Open Enterprise Server source.
- **WinScan.exe:** This Windows executable lists the contents of the file system on the target Microsoft server following a file to file migration.
- **ScanCompare.exe:** This Windows executable compares the files on the NetWare or Open Enterprise Server source server and the Microsoft Server target server.

All of these new utilities are used in Section 11.12, “Performing a Folder to Folder Migration,” on page 166.

Mobile Management

You can now perform many management tasks by using a hand-held device running the iO6 or Android operating systems. For more information, see Chapter 9, “Mobile Management,” on page 103.

Network Operations Center (NOC) Dashboard

The Network Operations Center Dashboard monitors and displays Novell Storage Manager activity. Its multiple monitoring regions help you track Novell Storage Manager activity, performance, and potential problems. For more information, see Chapter 10, “The Network Operations Center Dashboard,” on page 105.

Integration with Novell File Reporter 2.0

Novell File Reporter 2.0 can report on the files and folders of the target paths of Novell Storage Manager 3.1 policies.

1.3 New in Version 3.0.4

Tivoli Support

Novell Storage Manager 3.0.4 for AD now supports IBM Tivoli Hierarchical Storage Management.

Certificate Management

Enhanced SSL Certificate Management enables you to generate your own SSL certificates. For more information, see "Upgrading from Storage Manager 2.5x to 3.1.1 " or "Installing Novell Storage Manager 3.1.1 for Active Directory"in the *Novell Storage Manager 3.0.x for Active Directory Installation Guide.*

Enhanced DFS Namespace Support

Enhanced Microsoft Distributed File System support now allows for multiple namespaces to be managed. For more information, see Appendix B, "Distributed File System (DFS)," on page 245.

1.4 New in Version 3.0.3

Performance Enhancements

This update includes significant performance enhancements that speed up provisioning user storage, processing templates, enforcing policy paths, cross-empire data migrations, and vaulting.

1.5 New in Version 3.0.2

Identity Mapping in Cross-Empire Data Migration

To retain security and ownership information for files and folders being migrated from a Novell network platform to a Microsoft network platform, an identity mapping technology has been added to Cross-Empire Data Migration. Within the identity map, you indicate object equivalence from the Novell network source to the Microsoft network target.

For more information, see Section 11.2.1, "Defining an Identity Map for Security and Ownership Migration," on page 114.

1.6 New in Version 3.0.1

Cross-Empire Data Migration

Cross-Empire Data Migration is a subsystem within Novell Storage Manager that allows for the movement of file system data between storage infrastructures on different platforms governed by different identity and security frameworks. You can perform the following types of data copying:

- User to User
- Folder to User
- Group to Group

- Folder to Group
- Folder to Folder

For more information, see Chapter 11, "Performing a Cross-Empire Data Migration," on page 111.

Microsoft DFS Namespace Support

Distributed File System (DFS) namespace technology helps Microsoft network administrators group shared folders located on different servers and presents them to users as a virtual tree of folders known as a namespace. Novell Storage Manager now presents these namespaces as available storage resources in the Storage Resource List.

Copy Policy Data

Copy Policy Data allows you to copy all or a portion of the policy settings of one policy into another policy. For more information, see Section 5.10, "Copying Policy Data," on page 59.

Export Policy

Provides the ability to export policies so that they can be imported later. For more information, see Section 5.12, "Exporting Policies," on page 64.

Import Policy

Provides the ability to import policies that were previously exported. For more information, see Section 5.13, "Importing Policies," on page 65.

1.7 New in Version 3.0

Collaborative Storage

Novell Storage Manager 3.0 for Active Directory provides administrators the ability to create and manage collaborative storage areas for groups and containers. These storage areas can be structured in multiple ways including:

- A single project folder where all project members have access
- A project folder with personal subfolders for each of the members of a group. This configuration is done through Dynamic Template Processing
- Classroom-based storage for education customers providing the ability to structure the storage to support assignment and class work turn-in folders for each student

For more information, see Chapter 7, "Managing Collaborative Storage," on page 77.

Quota Management

Quota management lets administrators set storage quota limits for users based on their roles in the organization. Additionally, administrators can designate individuals as quota managers, who can then grant storage quota increase requests when needed. For user storage quota management, see Section 5.4, "Enabling Your Network for Quota Management," on page 40 and Section 5.5.5, "Setting

Quota Options," on page 47. For collaborative storage quota management, see Section 7.7.5, "Setting Group Policy Quota Options," on page 89. For administering quota, see Chapter 8, "Using Quota Manager," on page 97.

Profile Path and Remote Desktop Services Support

In addition to creating User Home Folder policies, administrators can create a User Profile Path policy, a User Remote Desktop Services Home Folder policy, and a User Remote Desktop Services Profile Path policy, with each of these policies governing storage management independently. For more information, see Section 5.6, "Creating a User Profile Path Policy," on page 52, Section 5.7, "Creating a User Remote Desktop Services Home Folder Policy," on page 53, and Section 5.8, "Creating a User Remote Desktop Services Profile Path Policy," on page 55.

Auxiliary Storage Policies

Auxiliary storage allows administrators to create one or more policies for creating and managing auxiliary storage folders when a new user is created. This auxiliary storage can even be hidden from the user for whom it was created. For example, administrators can create an HR Folder for confidential information about the user. For more information, see Section 5.11, "Using a Policy to Manage Auxiliary Storage," on page 60.

GSR Collector

The Global Statistics Reporting (GSR) Collector collects data for general statistics, presents historical data, reports on anomalies such as potential orphaned home folders, and catalogs managed storage movement. For more information, see Section 12.1.10, "GSR Collector," on page 223.

Anomaly Reports

The GSR Collector generates anomaly reports that identify issues that might need to be addressed before you create storage policies. For more information, see Section 12.2.3, "Anomaly Reports," on page 227.

Policy Location

In previous versions of Novell Storage Manager for Active Directory, the policies were stored as text files in a `POLICY` folder where the NSM Engine was installed. Policies are now stored in an SQLite database.

2 Overview

Novell Storage Manager introduces management and structure to an unmanaged and unstructured network storage system. In the process, it automates the full life cycle management of user and group storage. Leveraging directory services (commonly referred to as "the directory"), Novell Storage Manager automates a comprehensive set of storage management tasks based on events, identity, and policies.

The Directory

Microsoft Active Directory stores the identity information about the users and groups that Novell Storage Manager manages. When Novell Storage Manager is installed, it adds or modifies user and group attributes so that they can be managed through Novell Storage Manager.

Events

When a user in Active Directory is added, moved, renamed, disabled, or deleted, it is known as a directory "event."

Policies

Policies within Novell Storage Manager indicate what storage-specific actions to enact when an event in Active Directory takes place. These actions include creating user or collaborative storage when a new user is added to Active Directory, moving storage when a user is moved from one organizational unit or group to another, and archiving or deleting storage when a user is removed.

Novell Storage Manager lets you create the following types of policies:

User Home Folder: Manages home folders for users who access their storage from an assigned user workstation.

User Profile Path: Used for profile path management

User Remote Desktop Services Home Folder: Used for users who get network access from remote client machines. Prior to Windows Server 2008, these were referred to as Terminal Services Home Folders.

User Remote Desktop Services Profile Path: Used for profile path management for users who get network access from remote client machines.Prior to Windows Server 2008, these were referred to as Terminal Services Profile Paths.

Container: Manages the users located in an organizational unit.

Group: Manages the users that are members of a group.

Auxiliary: Manages one or more additional storage locations in association with one of the four user policy types.

NSM Engine

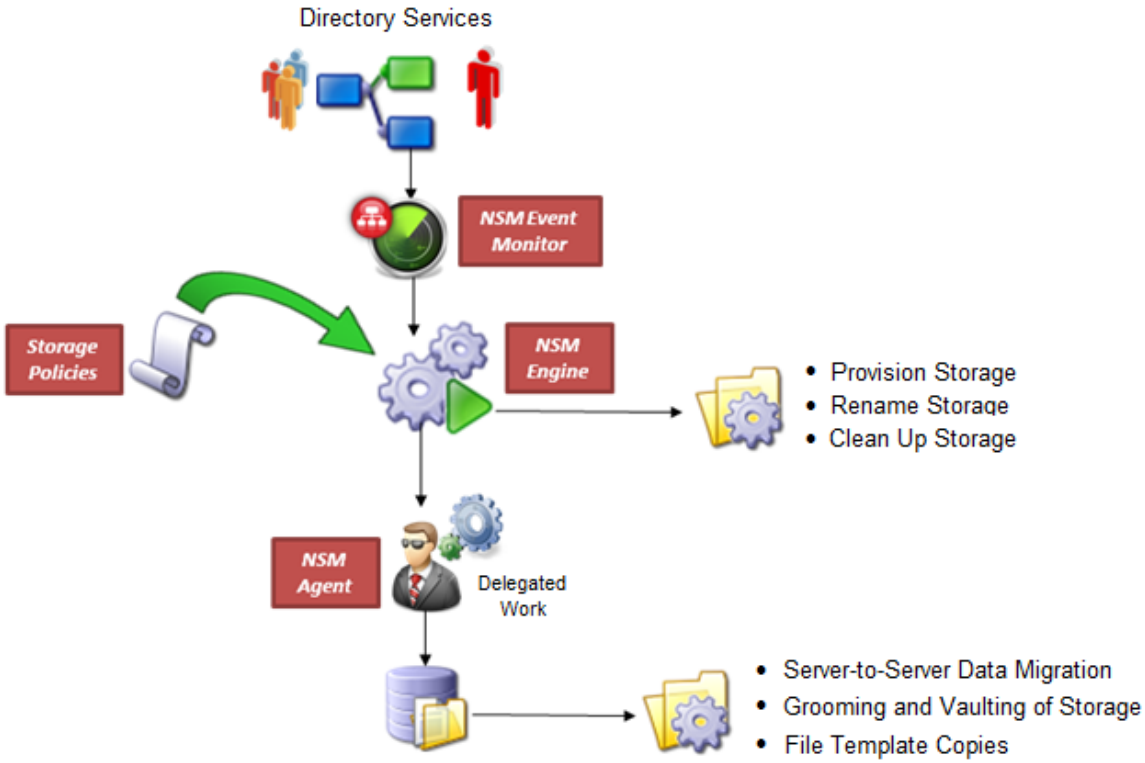
The NSM Engine performs actions based on events in Active Directory and the defined Novell Storage Manager policies. These actions include provisioning, moving, grooming, deleting, renaming, and vaulting in the file system. There is only a single NSM Engine per forest and it can be installed on a domain controller or a member server. The NSM Engine runs as a native NT service on Windows.

Event Monitor

The Event Monitor monitors changes to Active Directory based on create, move, rename, and delete events. You install one Event Monitor per domain, and it can run on a domain controller or a member server. If you install the Event Monitor on a domain controller, the Event Monitor always monitors the local server for changes in the domain. If the Event Monitor is installed on a member server, it identifies the closest available domain controller and monitors it for changes in the domain. The Event Monitor runs as a native NT service on Windows.

NSM Agent

NSM Agents perform copying, moving, grooming, deleting, and vaulting through directives from the NSM Engine. For optimum performance, NSM Agents should be installed on all servers with storage managed by Novell Storage Manager. The NSM Agent runs as a NT native service on Windows.



3 Using NSMAdmin

NSMAdmin is the administrative interface for Novell Storage Manager. All management tasks run from this easy-to use Windows application. NSMAdmin is built from the Microsoft .NET Framework and must run on a Windows workstation or server with .NET 3.5 installed.

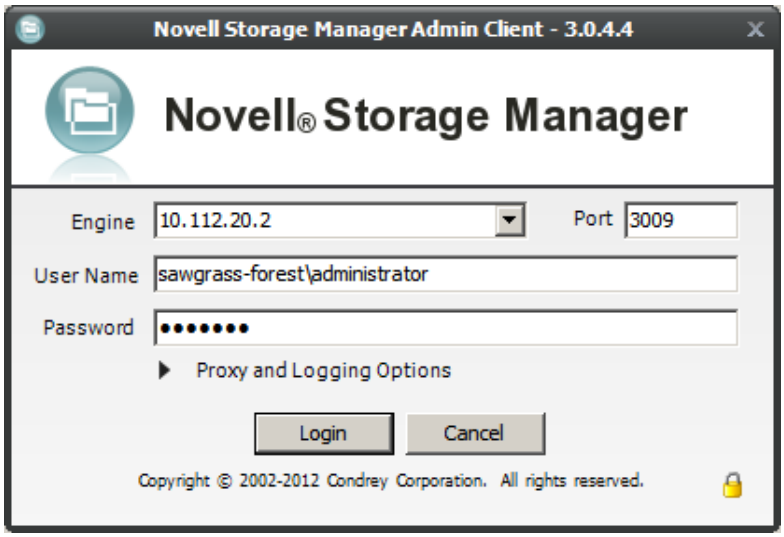
Procedures for installing NSMAdmin are included in "Installing Novell Storage Manager 3.1.1 for Active Directory" of the *Novell Storage Manager 3.1.1 for Active Directory Installation Guide*. If you have not yet installed NSMAdmin, go to that guide to install it before proceeding with this section.

- Section 3.1, "Launching NSMAdmin," on page 19
- Section 3.2, "Using the NSMAdmin Interface," on page 21

3.1 Launching NSMAdmin

1 Double-click the NSMAdmin icon from the Windows desktop.

An authentication dialog box appears.



2 In the *Engine* field, specify the DNS name or IP address where the NSM Engine service is installed.

3 In the *Port* field, specify the secure port number.

The default setting is 3009.

4 Specify the username.

You must specify the username in the form *Domain\username*.

5 Specify the password.

The user must be a member of the NSMAdmins group to be able to log in.

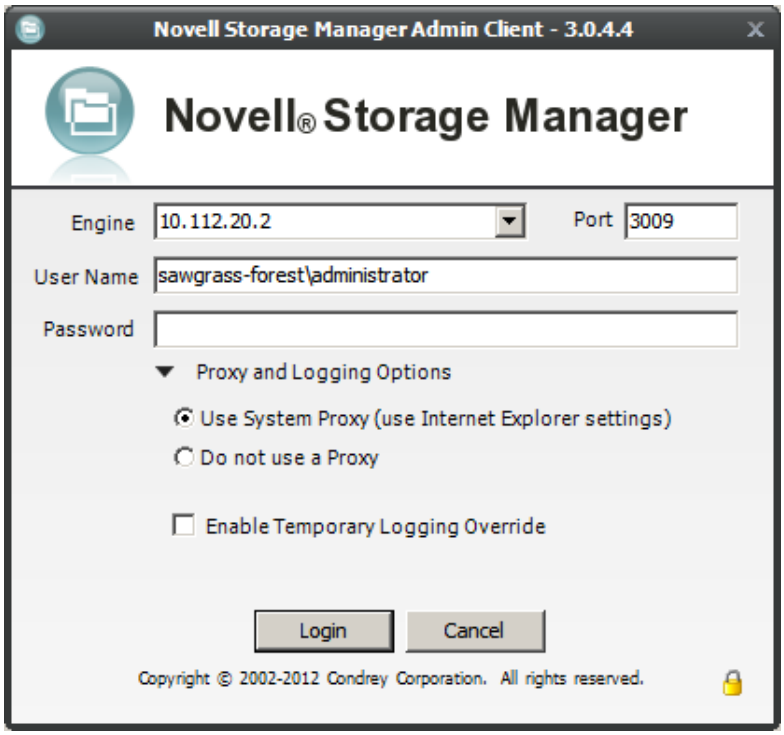
6 Click *Login*.

3.1.1 Overriding Proxy Settings at Login

As a .NET application, NSMAdmin is managed by the proxy configurations and exceptions of Microsoft Internet Explorer. If you do not have an exception in your proxy settings to allow for NSMAdmin, the NSMAdmin application might not launch.

Try to launch NSMAdmin using the default setting first. If you are unable to log in, use the following procedures:

1 Repeat Step 1 on page 19 through Step 5, then click the *Proxy and Logging Options* button to expand the authentication dialog box.



2 Select *Do not use a Proxy*.

3 Click *Login*.

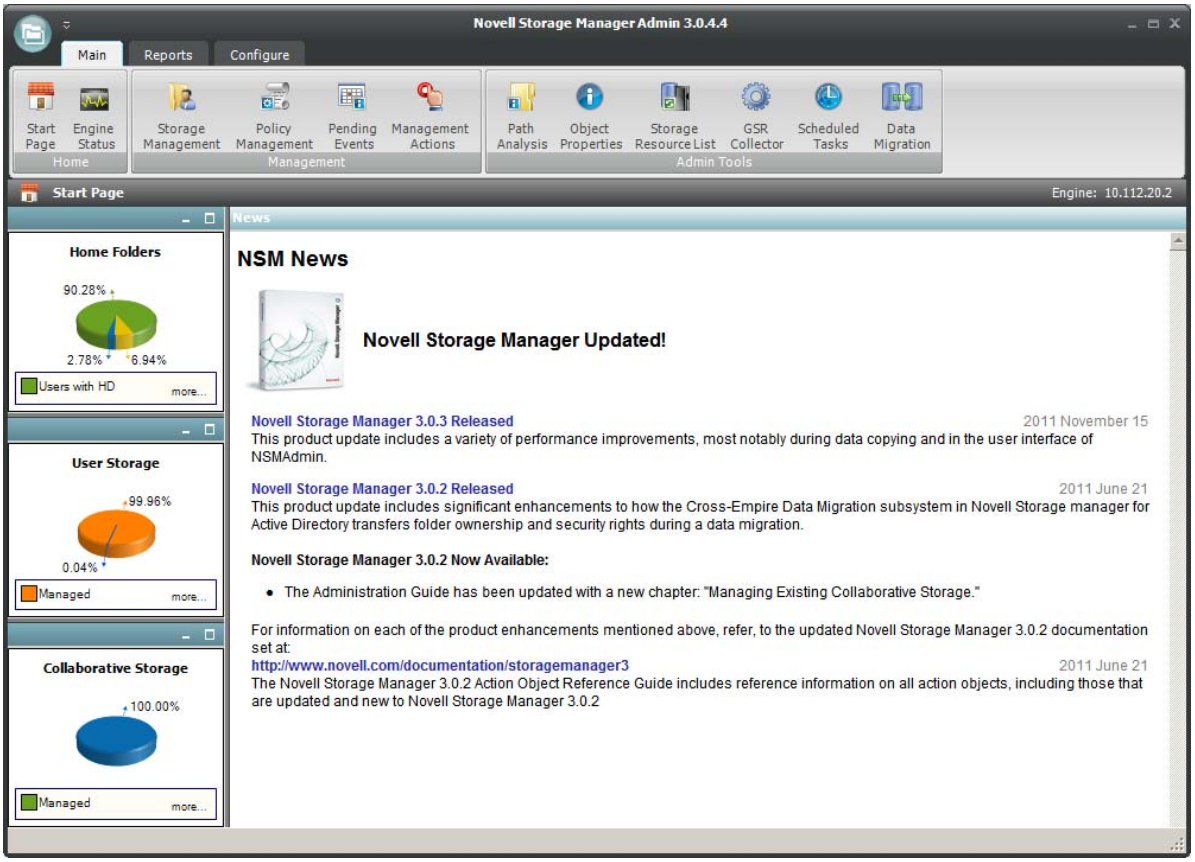
3.1.2 Enabling Temporary Logging Override

Selecting Enable Temporary Logging Override indicates that you want Novell Storage Manager to override any logging configuration settings you have set for the NSM Engine and the NSM Agent in NSMAdmin, and to create log files during this session. The data contained in the log files might be useful for troubleshooting.

3.2 Using the NSMAdmin Interface

The NSMAdmin interface has three tabs: *Main*, *Reports*, and *Configure*. Clicking each tab displays an associated toolbar directly below the tabs. The toolbar is divided into sections based on the actions that are available. Clicking a tool displays data or an interface for performing a management task.

The left panes of the Start Page tool display an at-a-glance view of the management status of user storage, collaborative storage, and users and groups that have home folders. The right pane displays links to resources and product news.



All other Novell Storage Manager tools are covered in the other sections of this guide.

4 Managing Existing User Storage

Because Novell Storage Manager 3.1.1 for Active Directory is deployed into an existing Microsoft network with users, groups, containers, and domains already established in Active Directory, your principle focus should be to start managing the storage that is assigned to these users. This process involves several tasks:

- Running reports to determine the status of your user storage
- Creating policies that standardize the storage allocation, quota, rights, and more
- Managing the users through Manage Operations
- Testing these policies to verify that they are working as desired

By completing this section, you not only put your existing users' storage into a managed state and set it up for ongoing management through Novell Storage Manager, but you also learn the basic procedures for reporting and for setting user policies.

- Section 4.1, "Running the GSR Collector," on page 24
- Section 4.2, "Viewing Anomaly Reports," on page 24
- Section 4.3, "Running Consistency Check Reports on Existing Storage," on page 25
- Section 4.4, "Assigning Missing Home Folder Attributes," on page 25
- Section 4.5, "Standardizing User Home Folder Attributes," on page 27
- Section 4.6, "Creating a Blocking Policy," on page 27
- Section 4.7, "Creating a User Home Folder Policy," on page 29
- Section 4.8, "Removing a Preexisting Process for Creating User Home Folders," on page 34
- Section 4.9, "Testing the User Home Folder Policy," on page 35
- Section 4.10, "Performing a Consistency Check," on page 35
- Section 4.11, "Testing a Rename Event," on page 36
- Section 4.12, "Testing a Cleanup Rule," on page 36
- Section 4.13, "What's Next," on page 36

After completing the procedures in this section, refer to the remainder of the *Novell Storage Manager 3.1.1 for Active Directory Administration Guide* for more detailed content on these tasks as well as many others.

4.1 Running the GSR Collector

The Global Statistics Reporting (GSR) Collector collects data for general statistics, presents historical data, reports on anomalies such as potential orphaned home folders, and catalogs managed storage movement. For more information, see Section 12.1.11, "Scheduled Tasks," on page 224.

As the first step in managing your existing user storage through Novell Storage Manager, you should run the GSR Collector. Depending on the size of your network, running the GSR Collector might be resource intensive and can take some time to complete. After you run the GSR Collector the first time, you should schedule it to run at a regularly scheduled time, preferably after regular business hours.

1. Launch NSMAdmin.
2. In the *Main* tab options, click *GSR Collector*.
3. Click *Run Collector*.

4.2 Viewing Anomaly Reports

The GSR Collector can generate anomaly reports to identify issues that might need to be addressed before you create storage policies. The anomaly report, which is generated through data collected by the GSR Collector, lists potential problems according to seven different categories:

Tab Name	Explanation
Orphan Candidates	Lists home folders that are not currently assigned to a User object in Active Directory.
Name Mismatch	Lists cases where a username and the associated home folder name do not match. This is frequently the case when a User object is renamed, but the corresponding home folder is not.
Path Overlap	Lists home folders that are parent paths of other user home folders. For example, a user's home folder attribute in Active Directory is set to \\SERVER\SHARE\HOME\USERS instead of \\SERVER\SHARE\HOME\USERS\JBANKS. This is a potential conflict because if you move an object that resides in the first path, it moves all users below the user.
Duplicate Storage Pointer	Lists users that have identical home folder paths.
Missing Primary Folders	Lists users who do not have assigned home folders.
Missing Auxiliary Folders	Lists users that have auxiliary storage assigned, but the storage is not yet created.
Objects Not Managed	Lists users in Active Directory whose storage is presently not managed through Novell Storage Manager.

1. In NSMAdmin, click the *Reports* tab.
2. Click *Anomaly Reports*.
3. Click the tab for the category you want to view.

   At this point, because none of your existing users are being managed through Novell Storage Manager, each user in Active Directory should be listed when you click the *Objects Not Managed* tab. Additionally, you might notice other potential problems by viewing data categorized through the other tabs.

4.3 Running Consistency Check Reports on Existing Storage

When Novell Storage Manager is installed, you need to analyze and correct any issues that might exist in the current user storage environment. Issues might include missing storage quotas, inconsistent home folder attributes, inconsistent home folder rights, missing home folders, and inconsistent file paths. Storage analysis begins by running consistency check reports on existing user storage prior to creating and implementing storage policies.

In addition to reporting on storage issues, consistency check reports let you review current quota assignments and can help you in designing and planning storage policies.

1. In NSMAdmin, click the *Main* tab.
2. Click *Storage Management*.
3. In the left pane, browse through the domain so that an organizational unit with the users for whom you want to generate the consistency check report is displayed in the right pane.
4. In the right pane, right-click the container and select *User Actions* > *Consistency Check*.
5. Click *Run* and view the results in the bottom panel.
6. Click *Expand* to expand the view.

   Because none of the users are currently managed through Novell Storage Manager, each user has a Management status of Not Managed. Additionally, there are no established storage quotas and there might be inconsistent directory attributes, rights, flags, and file paths, along with various warnings or errors that you can mouse over to view the specifics.

   To export a consistency check report for printing, see Section 12.2.1, “Consistency Check Reports,” on page 224.

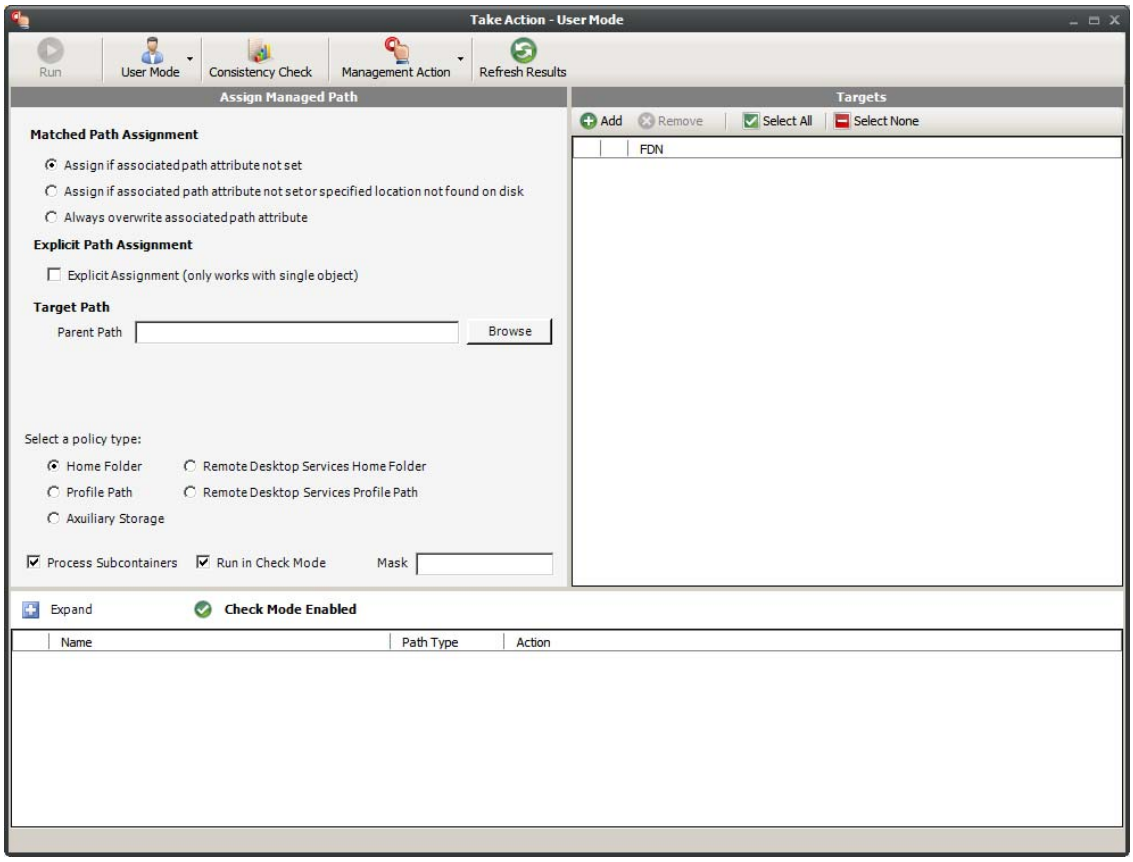
4.4 Assigning Missing Home Folder Attributes

The consistency check report’s *DS Path* column indicates the path (also referred to as “attributes”) of the user’s assigned home folder. If no path is indicated, it is because the home folder attribute is not set in Active Directory.

Novell Storage Manager allows you to populate any missing home folder attributes or correct attributes that are not configured correctly. You do this by selecting a path and looking for a match on each user’s ID. You also have the option to overwrite an existing attribute based on a match found.

If no home folder exists for the user, Novell Storage Manager can create one automatically when the target path for the home folder is indicated in the policy. For more information, see Section 4.5, “Standardizing User Home Folder Attributes,” on page 27.

1. In NSMAdmin, click the *Main* tab.
2. Click *Storage Management*.
3. In the left pane, browse through the domain so that an organizational unit with users that need home folder attributes appears in the right pane.
4. In the right pane, select the desired container.
5. Click *User Actions* > *Assign Managed Path*.



6 In the Matched Path Assignment portion of the window, make sure the *Assign if Home Directory attribute not set* option is selected.

7 Click *Browse*, use the Path Browser dialog box to browse to the path where your user home folders in the selected organizational unit reside, then click *OK*.

   The selected path appears in the *Parent Path* field.

8 Verify that the *Run in Check Mode* check box is selected.

   Check mode allows you to view the results of the action, without actually making changes.

9 Click *Run*.

10 Click *Expand* to expand the view.

   Novell Storage Manager summarizes any problems it can resolve in the *Action* column.

11 Click *Collapse*.

12 If you approve of the actions Novell Storage Manager took in Check mode, deselect *Run in Check Mode* and click *Run*.

13 Run a new consistency check report by selecting the organizational unit you selected in Step 3 on page 25, clicking *Consistency Check*, then clicking *Run*.

14 Observe that all users now have home folder attributes listed in the *DS Path* column.

4.5 Standardizing User Home Folder Attributes

As a best practice, you should have all of your user home folder attributes set to a path that ends with the user's home folder name, rather than the parent path. For example, instead of user EBROWN having a home folder attribute of *SERVER-NAME**SHARE-NAME*\HOME\USERS, it should be set to *SERVER-NAME**SHARE-NAME*\HOME\USERS\EBROWN.

Novell Storage Manager lets you easily standardize home folder attributes by overwriting attributes linked to the parent path.

1. In NSMAdmin, click the *Main* tab.
2. Click *Storage Management*.
3. In the left pane, browse through the domain so that a container with users that need standard home folder attributes appears in the right pane.
4. In the right pane, right-click the desired organizational unit and select *User Actions* > *Assign Managed Path*.
5. Select the *Always overwrite Managed Path attribute* option.
6. Click *Browse*, use the Path Browser dialog box to browse to the path where you want all home folders in the selected container to reside, then click *OK*.
7. Verify that the *Run in Check Mode* check box is selected.
8. Click *Run*.
9. Click *Expand* to expand the view.

   Novell Storage Manager summarizes any problems it can resolve in the *Action* column. Resulting home folder attributes that will be created are displayed as "Match found. Managed Path would be set."
10. Click *Collapse*.
11. If you approve of the actions Novell Storage Manager took in check mode, deselect *Run in Check Mode* and click *Run*.
12. Run a new consistency check report by selecting the organizational unit you selected in Step 4, clicking *Consistency Check*, then clicking *Run*.
13. Observe that all users who did not previously have proper home folder attributes, now do.

4.6 Creating a Blocking Policy

Novell Storage Manager provides the ability to create "blocking policies" that block other Novell Storage Manager policies from affecting members of organizational units, members of groups, or even individual users. For example, you might have proxy users such as a BACKUP PROXY or VIRUS SCAN PROXY who do not need a home folder. Or, you might have an organizational unit within an organizational unit whose members you do not want to be assigned home folders.

Creating a blocking policy is as easy as creating a group, adding the users you want to block from a policy to the group, and then using NSMAdmin to create the blocking policy and associate it to the group.

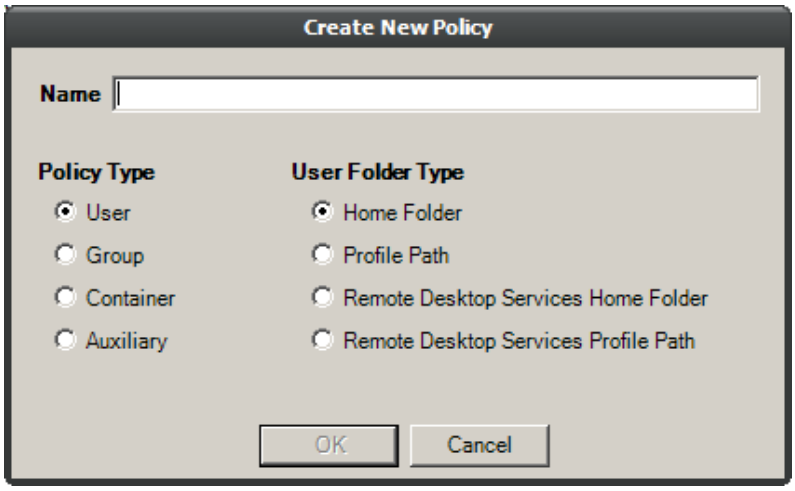
IMPORTANT: Before proceeding, you should create a group in Active Directory whose members you want to block from the effects of any Novell Storage Manager policies that you create.

---

1. In NSMAdmin, click the *Main* tab.
2. Click *Policy Management*.

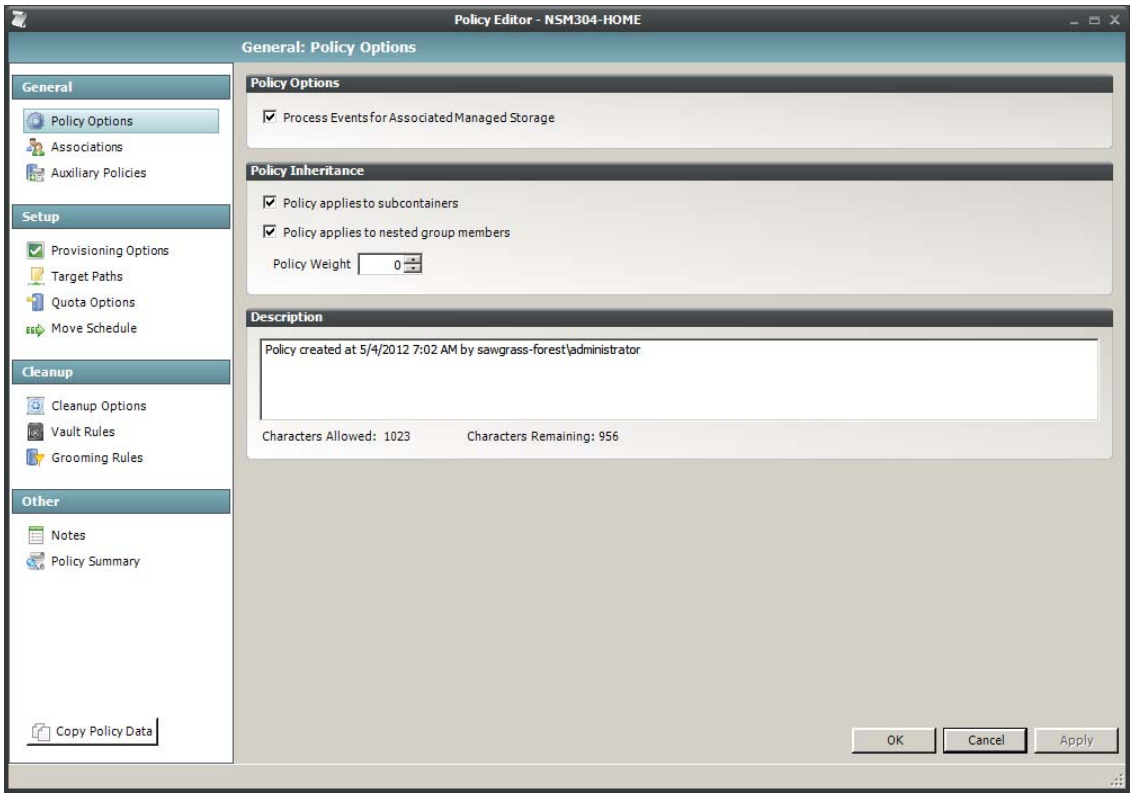
3 In the *Manage Policies* menu, select *Create Policy* > *Create User Home Folder Policy*.

The following screen appears:



4 Specify a descriptive name in the *Name* field, such as "Block Policy," leave the *User* and *Home Folder* options selected, then click *OK*.

The Policy Options page appears.



5 Deselect the *Process Events for Associated Managed Storage* check box.

A description at the right of the check box indicates that the policy is now a blocking policy.

6 In the left pane, click *Associations*.

7 Click the + sign.

8 Browse down and locate the group that you want to block from the effects of Novell Storage Manager policies, then drag it to the *Selected Items* pane.

9 Click *OK* to save the setting.

10 Click *OK* to save the block policy.

4.7 Creating a User Home Folder Policy

A policy in Novell Storage Manager is the means by which Novell Storage Manager provisions, manages, deletes, and archives storage. The parameters within the policy dictate where user storage is created, what rights are granted, what quota to assign, what to do when a user leaves an organization, and much more.

IMPORTANT: Only one policy of the same type can be associated with a domain, organizational unit, group, or user.

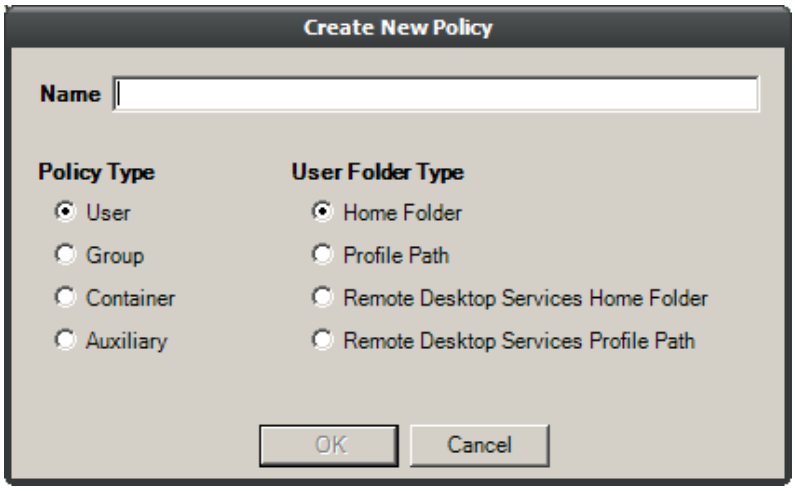
---

1 In NSMAdmin, click the *Main* tab.

2 Click *Policy Management*.

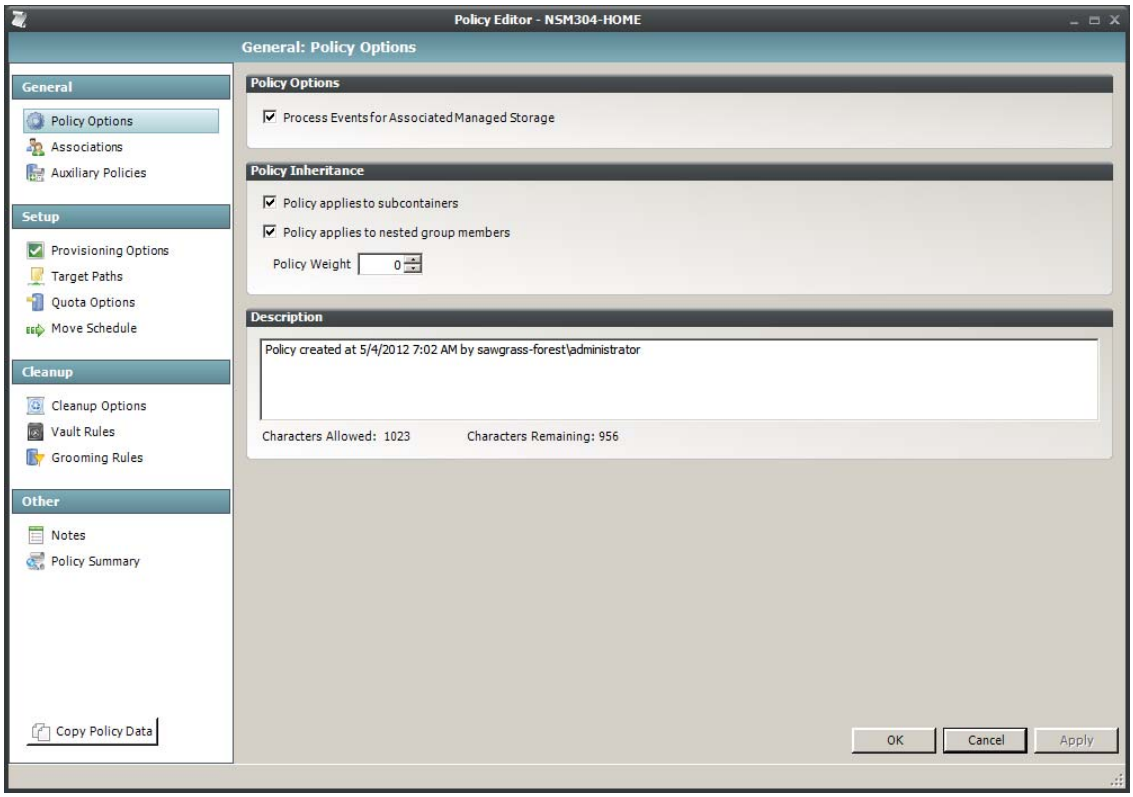
3 In the *Manage Policies* menu, select *Create Policy* > *Create User Home Folder Policy*.

The following screen appears:



4 Specify a descriptive name for the policy, such as “Los Angeles Division,” then click *OK*.

The Policy Options page appears.



5 Set the Policy Options specifications for the policy:

5a If you want the container's subcontainers to inherit the policy settings, leave the *Policy applies to subcontainers* check box selected. Otherwise, deselect it.

5b If you will have users that are members of multiple groups, which means they could be affected by multiple policies, use the *Policy Weight* field to indicate a weight for this policy.

When multiple policies pertain to a user, Novell Storage Manager uses the highest weight number to determine which policy to apply.

5c Click *Apply* to save your settings.

6 Set the associations:

6a In the left pane, click *Associations*.

6b Click the + button.

6c Browse to and locate the domain, organizational unit, Group object, or User object you want the policy applied to, then drag it to the Selected Items pane.

6d Click *Apply* to save the settings.

7 Set the provisioning specifications:

7a In the Folder Properties region, specify the settings you want for the rights to be applied to network home folders that are created through this policy. Select the *Policy-Defined Default Attributes* check box, to activate additional check boxes.

7b In the Template Folder region, click the *Browse* button to locate and place a path to a template directory that can be copied into each home folder.

For more information on templates, see Step 4 on page 46.

7c In the Home Folder region, indicate the network drive letter to assign to your users.

7d Click *Apply* to save the settings.

8 Set the target paths:

8a In the left pane, click *Target Paths*.

8b Click the + button, browse to the share or folder where you want your home folders to reside, right-click and choose *Select* to add the target path to the Selected Paths pane.

8c If you want to set the location of home directories among different paths, repeat Step 8b to include all the paths you want.

8d If you have multiple paths listed, select a distribution method from the *Distribution* drop-down list.

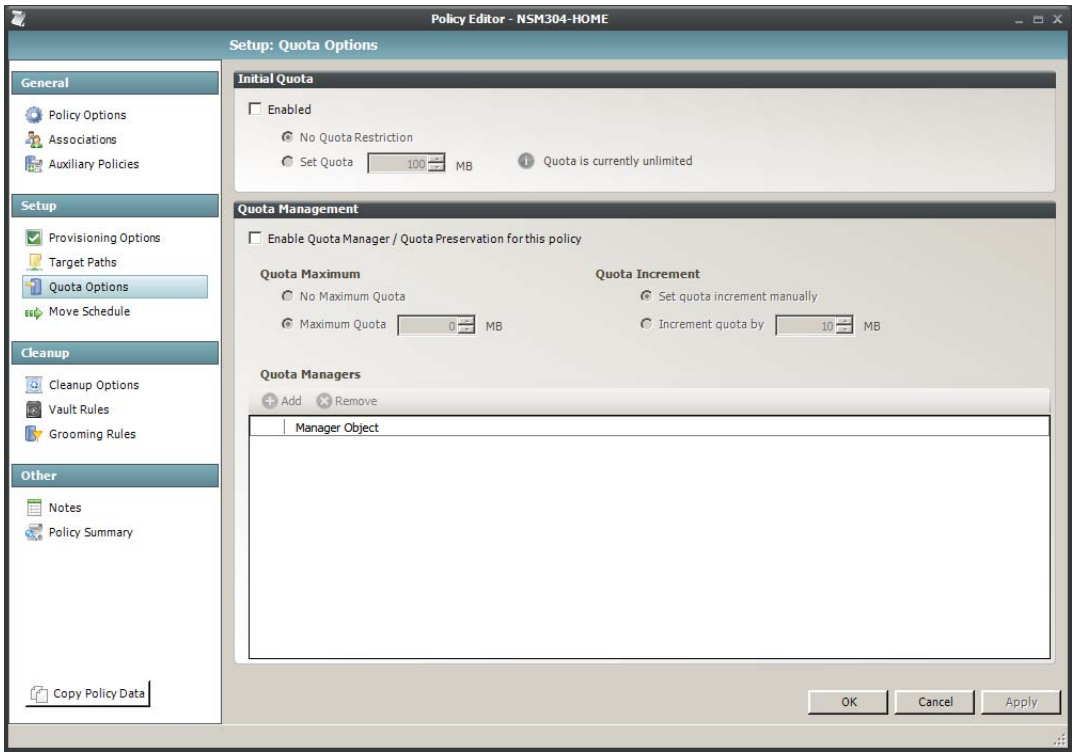
For an explanation of storage distribution, see Section 5.5.4, "Setting Target Paths," on page 46.

8e Leave the other fields as they are currently set.

8f Click *Apply* to save your settings.

9 Set the quota options:

9a In the left pane, click *Quota Options*.



9b In the Initial Quota region, specify the amount of initial storage space to be allocated to all users associated with this policy.

9c (Optional) In the Quota Management region, click the *Enable Quota Manager / Quota Preservation for this Policy* check box, to display additional options.

9d Select one of the following Quota Maximum options:

- Use the *No Maximum Quota* option to specify that the users managed by this policy will be granted additional storage quota when they need more.
- Use the *Maximum Quota* field to specify the maximum amount of storage that is allocated to a user. This allocation comes through the quota increment settings below.

9e (Optional) Select one of the following Quota Increment options:

- Select the *Set quota increment manually* option to allow users who are designated as quota managers to set quotas manually.
- Select the *Increment quota by* option to indicate the size in MB for each new allocation of additional storage quota.

9f Click *Apply* to save your settings.

10 Set the move schedule:

10a In the left pane, click *Move Schedule*.

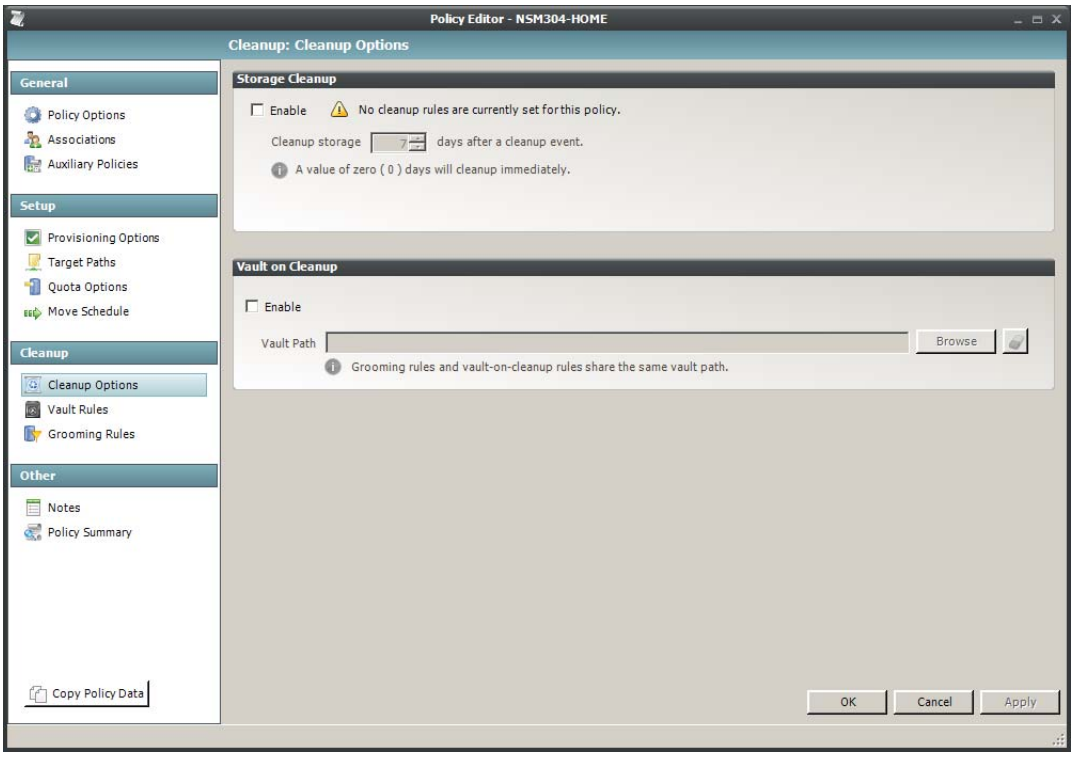
10b Specify the hours when Novell Storage Manager can perform data migrations.

For more information on data migrations, see Section 5.5.6, "Setting the Move Schedule," on page 49.

10c Click *Apply* to save the settings.

11 Set the cleanup options:

11a In the left pane, click *Cleanup Options*.



11b In the Storage Cleanup region, select the *Enable* check box to indicate if you want user storage associated with this policy deleted when a user is removed from Active Directory.

If you select the check box, you can specify the number of days a user home folder and its contents will remain before it is deleted.

11c If you want user storage associated with this policy vaulted, in the Vault on Cleanup region, select the *Enable* check box and use the *Browse* button to indicate a path to the vault location.

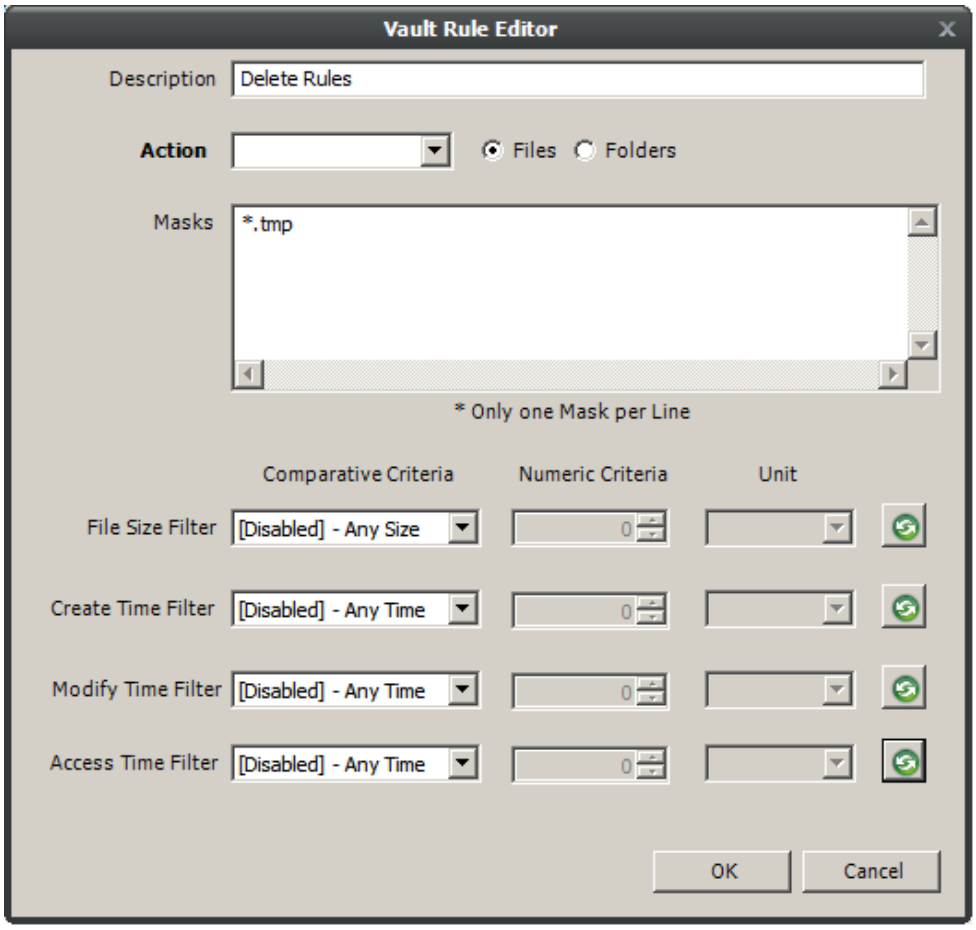
11d Click *Apply* to save your settings.

If you have both Storage Cleanup and Vault on Cleanup enabled, Novell Storage Manager vaults the data and then deletes it after the specified period of time. If you have Vault on Cleanup but not Storage Cleanup enabled, Novell Storage Manager vaults the data immediately and never cleans it up.

12 Set the vault rules:

12a In the left pane, click *Vault Rules*.

12b Click the + button to create vault rules.



For example, in the rule above, all `.tmp` files are deleted prior to their home folder being vaulted. When the specified number of days in the *Cleanup storage after* field has passed, the home folder is deleted from the specified vault location.

12c Click *Apply* to save your settings.

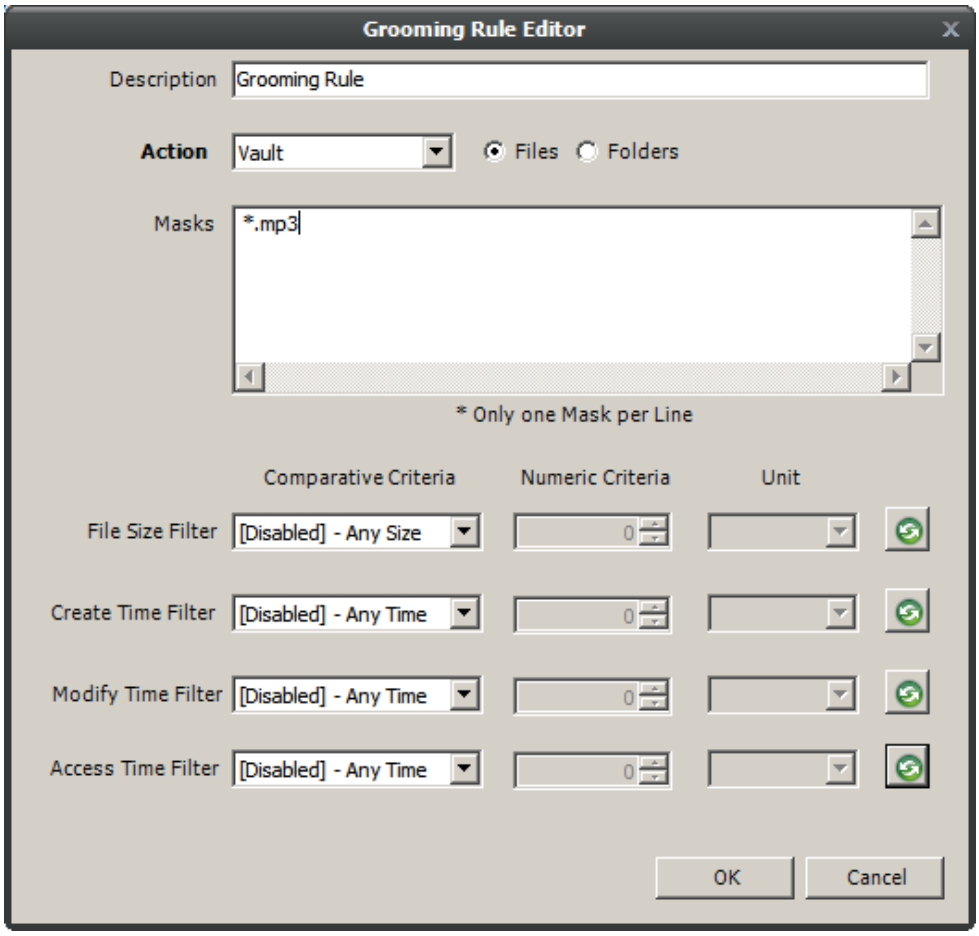
13 Set the grooming rules:

13a In the left pane, click *Grooming Rules*.

13b Click the + button.

13c Select either *Vault* or *Delete* from the *Action* drop-down menu to specify whether to vault or delete a particular type of file.

13d In the *File Name Mask* field, indicate the type of file for which this grooming rule will take action. For example, *.MP3.



To narrow the scope of the grooming rule, you can use the filter settings in the lower portion of the dialog box.

For example, if you select *Greater than* from the *File Size Filter* drop-down menu, enter 2 as the Numeric Criteria, and select *MBs* as the Unit setting, the grooming rule in this example vaults all MP3 files greater than 2 MB. Setting additional filters narrows the scope of the grooming action even more.

13e Click *OK* to save the grooming rule.

13f Repeat Step 13a through Step 13e to create additional grooming rules.

13g Click *Apply* to apply the grooming rules.

14 Click *OK* to save the policy settings.

4.8 Removing a Preexisting Process for Creating User Home Folders

When you create and configure a policy, it is important to understand that Novell Storage Manager is now set up to provision and manage all new users that are created in the associated container.

If you have a network tool such as Microsoft Active Directory Users and Computers creating home folders when a new user is added to the domain, organizational unit, or group associated with a policy, you need to remove the setting that creates the home folder.

You might also need to notify anyone who previously managed storage for those users that are now being managed by Novell Storage Manager, to cease any manual storage management tasks such as home folder creation, renames, moves, etc., and let Novell Storage Manager now manage the user storage.

4.9 Testing the User Home Folder Policy

You should now create a test user to confirm that Novell Storage Manager will provision and deprovision the test user's home folder according to the policy rules that you created.

1. Use Active Directory Users and Computers to create a new user such as TESTUSER in the organizational unit associated with the policy you configured in Section 4.7, "Creating a User Home Folder Policy," on page 29.
2. In NSMAdmin, click the *Main* tab.
3. Click *Path Analysis*.
4. In the left pane, browse down to the location where the new home folder for the new TESTUSER is located.
5. Select the TESTUSER home folder, then select *Folder Trustees*.

   This displays the View Trustees page.
6. Verify that the rights that you set in Step 7a on page 30 are those that you set in the policy.
7. Click *OK* to close the View Trustees page.
8. Click *Quota*.

   This displays the View Quota dialog box.
9. Verify that the quota specifications that you set in Step 9 on page 31 are those that you set in the policy.
10. Click *OK* to close the View Quota dialog box.

4.10 Performing a Consistency Check

Performing a follow-up consistency check allows you to verify that other policy specifications that you established in the user home folder policy are being enacted.

1. In NSMAdmin, click the *Main* tab.
2. Click *Storage Management*.
3. In the left pane, browse to select the organizational unit associated with the policy that you created earlier.
4. Select the *Filters* check box that is associated with Users.
5. In the right pane, locate and right-click TESTUSER, then select *User Actions* > *Consistency Check.*

   The Take Action – User Mode page appears.
6. Click *Process Selected Targets*.
7. Verify that the settings for the home folder attribute (DS Path), Flags, Rights, and Quota are what you established when you configured the policy. Additionally, verify that the Management status is set to "Managed" and that the Mgmt Path and DS Path match (a check mark in the *Paths Match* column indicates a match).

4.11 Testing a Rename Event

This procedure lets you verify that a user's home folder attribute is updated following a rename event.

1. Use Active Directory Users and Computers to rename the user from the suggested TESTUSER name to a name such as TESTUSER2.
2. In NSMAdmin, while you are still displaying the users through the Storage Management page, click *Refresh* to refresh the screen and see the renamed user.
3. Right-click the renamed user and select *User Actions* > *Consistency Check*.
4. Verify that the home folder and the directory attribute have been updated in the *DS Path* and *Mgmt Path* columns.

4.12 Testing a Cleanup Rule

This procedure lets you verify that Novell Storage Manager cleans up a user's storage according to the user home folder policy that you created earlier.

1. Use Active Directory Users and Computers to delete TESTUSER2.
2. If you chose to delay the cleanup of user storage for a set amount of days in Step 11b on page 32, open NSMAdmin, click the *Main* tab > *Pending Events* > *Deferred* to view any information indicating the deferred number of days for the storage cleanup.
3. Click *Path Analysis*.
4. In the left pane, browse to the location where the TESTUSER2 resided and verify that the folder has been deleted.
5. (Conditional) If you set your policy to vault deleted storage, browse to the location in the left pane where you chose to vault deleted storage in Step 11c on page 32 and verify that TESTUSER2 was vaulted:
   - **5a** If you set your policy to delay the cleanup of user storage for a set amount of days in Step 11b on page 32, click *Pending Events* to view details on deferred action.
   - **5b** Right-click the listed deferred action, then select *Properties*. In the Properties dialog box, then verify that the *Next Eligible Time* displays a date that corresponds to the number of days you set in your policy for the deleted storage to be cleaned up.
   - **5c** Click *OK* to close the dialog box.
6. Because this is a test user, perform the storage cleanup immediately by once again right-clicking the listed deferred action and selecting *Make Eligible*.
7. Click *Path Analysis* and browse to the location in the left pane where you viewed the vaulted storage, then verify that the storage has been cleaned up.

4.13 What's Next

Now that you have created and tested a User Home Folder policy, you can create User Home Folder policies for the users in other organizational units or groups. You can do so based on the overview and procedures you were given in this chapter, or you can review Chapter 5, "Managing User Home Folders," on page 39, which provides a more comprehensive discussion of performing user-based storage tasks in NSMAdmin.

When you have a better understanding of the user-based storage capabilities in Novell Storage Manager, you can proceed to have Novell Storage Manager manage your collaborative-based storage. Refer to Chapter 7, "Managing Collaborative Storage," on page 77 for a comprehensive discussion and procedures for performing collaborative storage tasks.

5 Managing User Home Folders

- Section 5.1, “Overview,” on page 39
- Section 5.2, “User Policies,” on page 39
- Section 5.3, “Setting Up a Vaulting Location,” on page 40
- Section 5.4, “Enabling Your Network for Quota Management,” on page 40
- Section 5.5, “Creating a User Home Folder Policy,” on page 42
- Section 5.6, “Creating a User Profile Path Policy,” on page 52
- Section 5.7, “Creating a User Remote Desktop Services Home Folder Policy,” on page 53
- Section 5.8, “Creating a User Remote Desktop Services Profile Path Policy,” on page 55
- Section 5.9, “Using a Policy to Manage Inactive Users,” on page 57
- Section 5.10, “Copying Policy Data,” on page 59
- Section 5.11, “Using a Policy to Manage Auxiliary Storage,” on page 60
- Section 5.12, “Exporting Policies,” on page 64
- Section 5.13, “Importing Policies,” on page 65

5.1 Overview

In Chapter 4, “Managing Existing User Storage,” on page 23, you created and configured a blocking policy and a User Home Folder policy to put your existing storage in a managed state. In this section you will learn in greater detail about how to create and configure User Home Folder policies, along with other policies associated with user storage. These include:

- User policies
- Auxiliary storage policies
- Profile path policies
- Remote Desktop Services policies that include
  - Remote desktop home folder
  - Remote desktop policy path

5.2 User Policies

User policies automate the provisioning, ongoing management, and disposition of network user home folders. A user policy can be associated with the following Active Directory objects:

- Domain
- Organizational Unit

- Group
- User

If you associate the user policy to a Domain or Organizational Unit object, the policy affects all users that reside in those areas of the directory, unless it is specifically blocked through a blocking policy. If you associate the policy to a group, it affects all members of the group.

NOTE: Although creating a user policy for an individual User object is possible, it is somewhat impractical and should only be done in rare circumstances.

User policies are stored in a database that is created during the NSM Engine installation.

5.3 Setting Up a Vaulting Location

Vaulting is the process of saving the contents of a user's home folder after the user's User object has been removed from Active Directory. If your user storage policies are to include vaulting rules, you must first set up a storage location (share) where the policy will vault the storage.

Ensure that the vault location has Full Control permission and Full Control security rights for the NSMProxyRights group.

5.4 Enabling Your Network for Quota Management

Novell Storage Manager leverages the quota capabilities of Windows Server 2008.

IMPORTANT: Novell Storage Manager cannot manage quotas on home folders, collaborative storage folders, or auxiliary storage hosted on Windows Server 2003 machines.

For all Windows Server 2008 servers hosting home, collaborative, or auxiliary storage managed by Novell Storage Manager with quota management enabled, you must have the File Server Resource Manager (FSRM) role installed. Additionally, if Windows Firewall is enabled, then you must set an exception rule on each server that permits remote FSRM management. FSRM management is needed because the NSM Engine is managing the quota remotely.

For more information, see Section A.1, "Windows Firewall Requirements," on page 241.

Setting an exception rule is different for Windows Server 2008 and Windows Server 2008 R2.

Figure 5-1 *Setting a Firewall Exception Rule for Windows Server 2008*

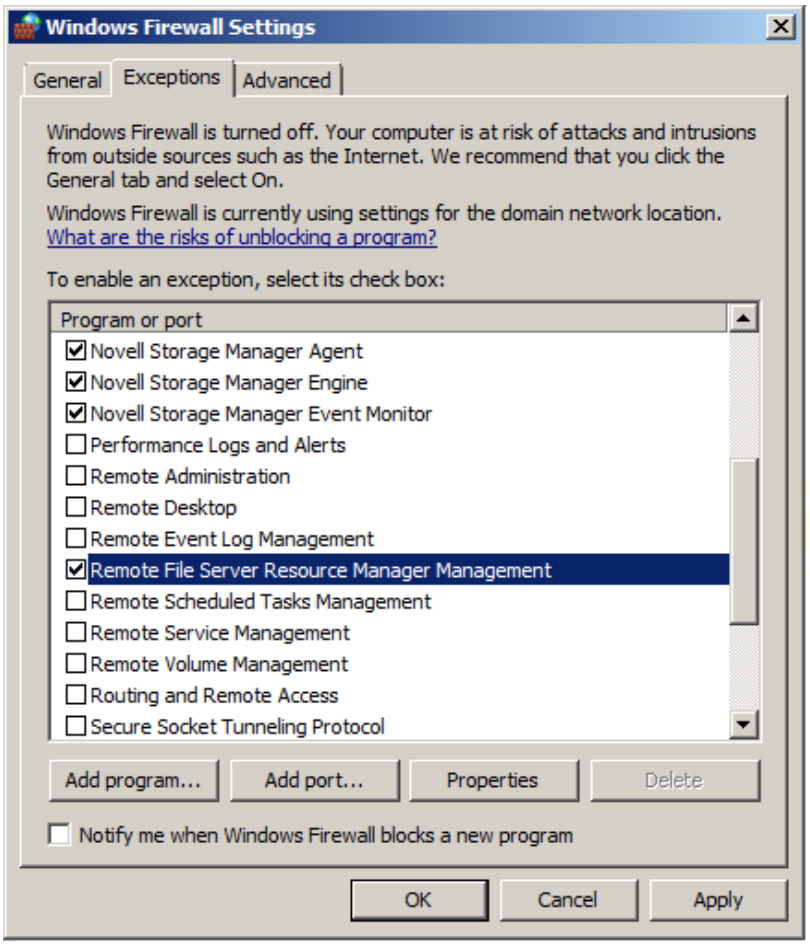
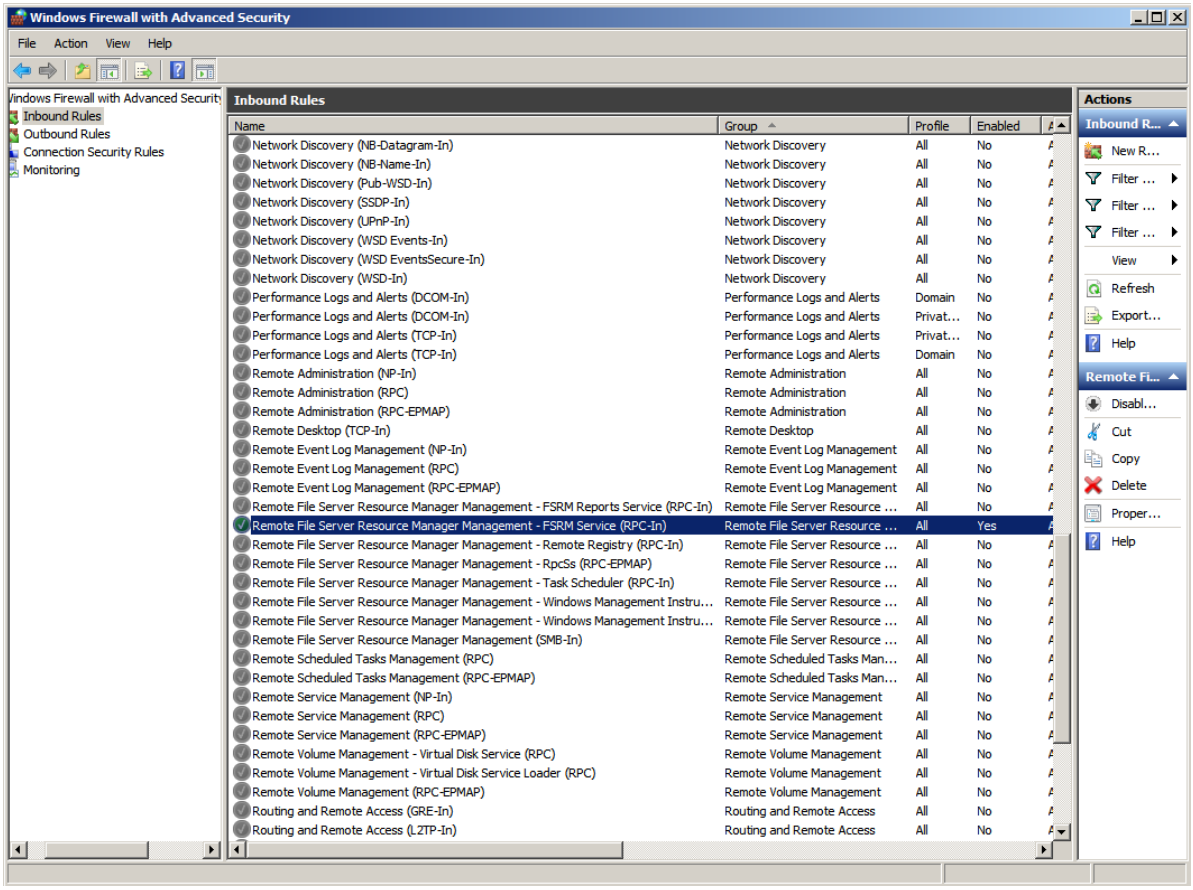


Figure 5-2 *Setting a Firewall Exception Rule for Windows Server 2008 R2*

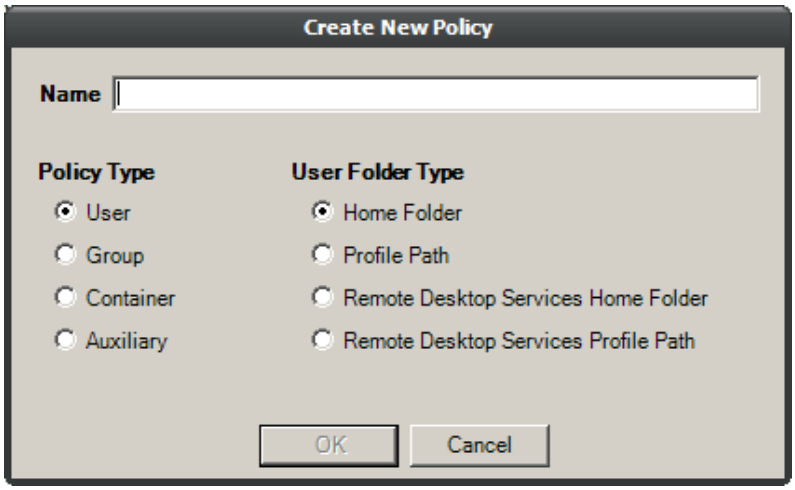


5.5 Creating a User Home Folder Policy

Prior to creating the user policy, you must determine if the policy should pertain to the members of the domain, organizational unit, or a group.

1. Launch NSMAdmin.
2. In the *Main* menu, click *Policy Management*.
3. In the *Manage Policies* menu, select *Create Policy* > *Create User Home Folder Policy.*

   The following screen appears:



4 Specify a descriptive name in the *Name* field and leave the *User* and *Home Folder* options selected.

The Policy Options page appears.

5 Continue with Section 5.5.1, "Setting Policy Options," on page 43.

5.5.1 Setting Policy Options

Settings within Policy Options let you indicate how to apply the policy, set policy inheritance and policy weight, and write an expanded policy description.

1 In the Policy options region, fill in the following fields:

Process Events for Associated Managed Storage: Select this check box to apply the settings in this policy to all users within the domain or organizational unit where this policy is assigned. Deselect this check box to create a blocking policy that can be applied to a specific user or group. For more information on blocking policies, see Section 4.6, "Creating a Blocking Policy," on page 27.

Automatically Attempt to Bypass Events in Bypassable State: Select this check box to allow Novell Storage Manager to automatically attempt to address any pending events that can bypass administrative action.

Be careful when considering applying this setting to a policy. Doing so has the potential to make incorrect associations and, thus, grant a user access to a folder that he or she shouldn't have. For example, suppose Tom Smith and Tammy Smith are in the same container and managed by the same policy, and that there is a home folder already created named TSMITH. Novell Storage Manager might consider this a bypassable event and, if this check box is selected, might associate the home folder to Tammy Smith, when it should belong to Tom Smith.

2 In the Policy Inheritance region, fill in the following fields:

Policy applies to subcontainers: Select this check box to have the settings in this policy inherited for all organizational units that reside within the domain or organizational unit where this policy is assigned.

Policy applies to nested group members: Select this check box to have the settings inherited by any nested groups you associate a policy to.

Policy Weight: When a user is a member of multiple groups and each group has a separate policy, Novell Storage Manager uses this setting to determine which policy to apply. Novell Storage Manager applies the policy with the largest numerical weight.

3 In the text field in the Description region, specify a description of the policy you are creating.

4 Click *Apply* to save your settings.

5 Proceed with Section 5.5.2, "Setting Associations," on page 44.

5.5.2 Setting Associations

The Associations page is where you assign the policy you are creating to a domain, organizational unit, Group object, or—if you are creating a blocking policy—a User object.

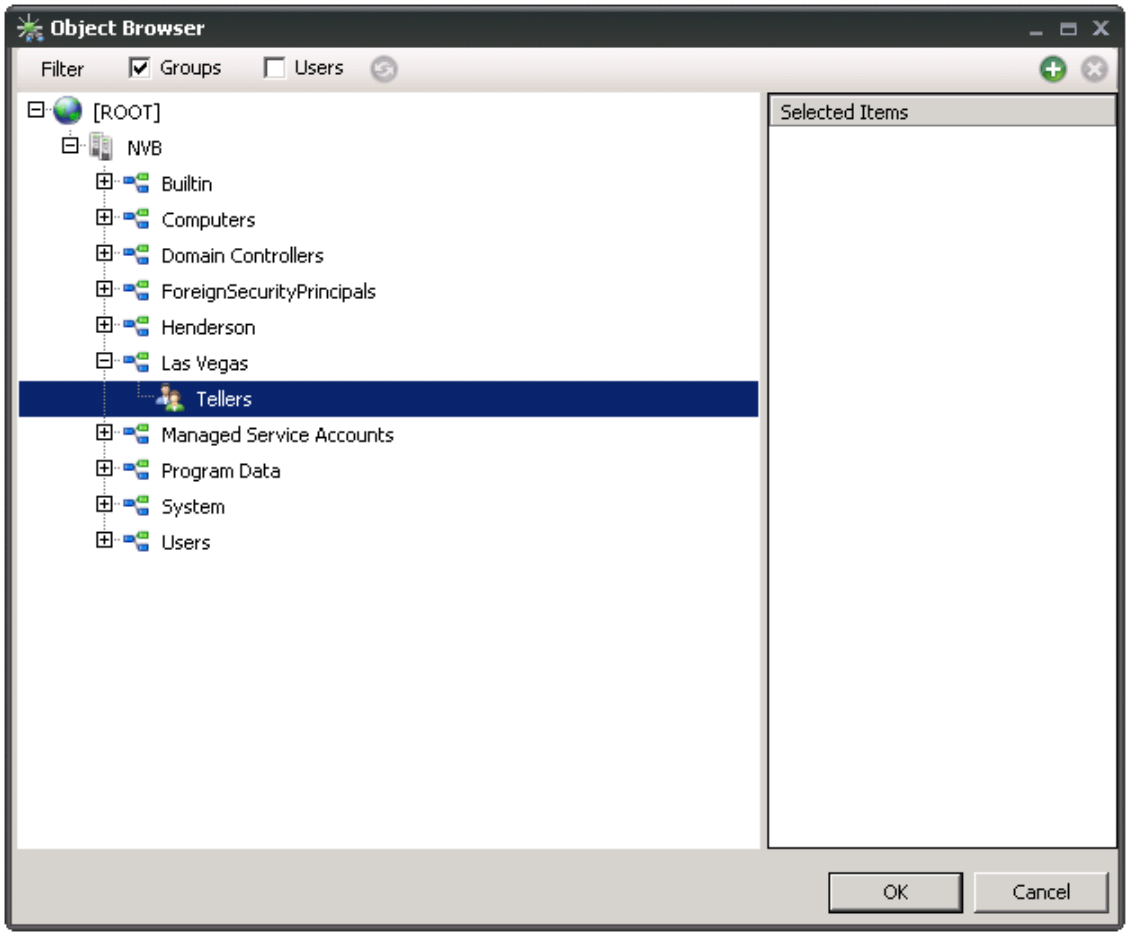
1 In the left pane, click *Associations*.

2 Click the + button to bring up the Object Browser.

3 If you plan to assign the policy to a User object, select the *Users* check box in the Filter region of the Object Browser.

4 Browse through the directory structure and select the domain, organizational unit, Group object, or User object you want to associate the policy to.

The Domain Users group cannot be a target for a policy association.



5 Drag the object to the Selected Items pane, then click *OK*.

The Object Browser is closed and the path is displayed in fully qualified name format in the right pane of the window. For example, CN=Tellers,OU=Las Vegas,DC=NVB,DC=local.

6 Click *OK* to close the Object Browser.

7 Click *Apply* to save your settings.

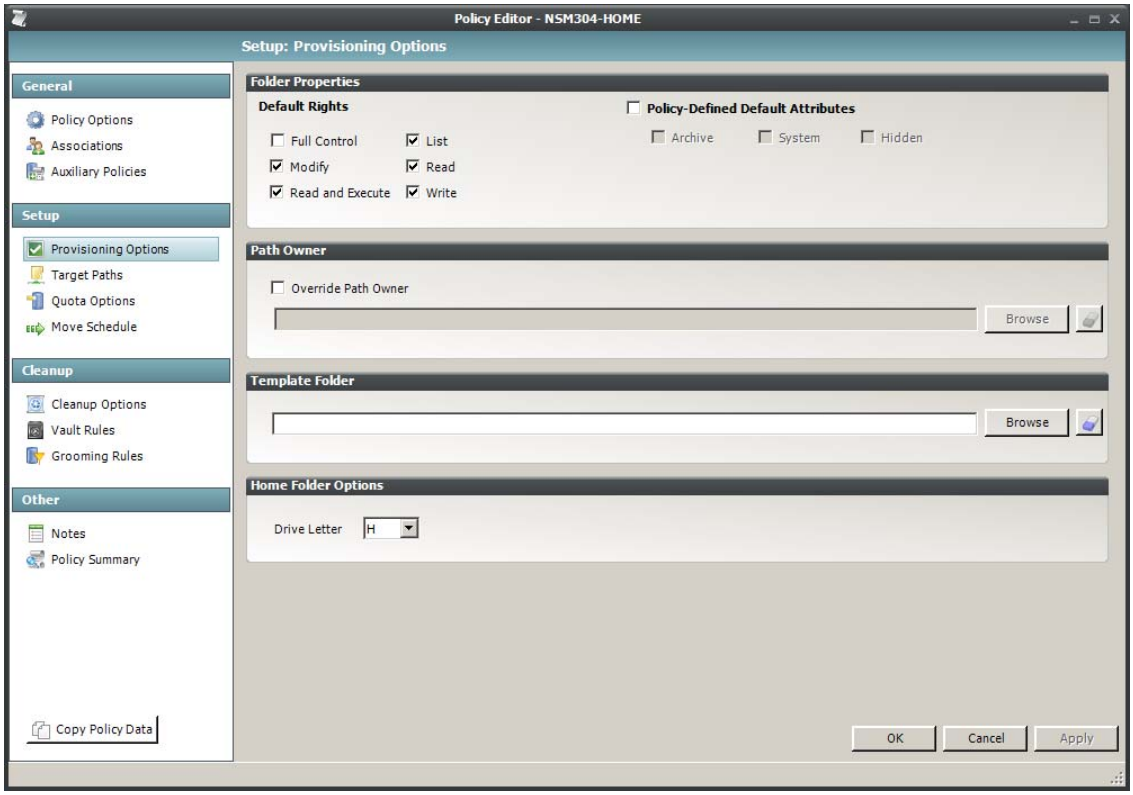
8 Proceed with Section 5.5.3, "Provisioning Options," on page 45.

5.5.3 Provisioning Options

The Provisioning Options page is where you indicate home folder rights, the network drive letter for the home folder, the location of a template for provisioning folder structure and content in a home folder when it is created, and more.

1 In the left pane, click *Provisioning Options*.

The following page appears:



2 In the Folder Properties region, specify the following settings:

Default Rights: By default, Novell Storage Manager grants the user all file rights to the home folder except for Full Control. Granting Full Control is not recommended because it provides administrator rights to the home folder, and enables the user to rename and delete the folder.

Policy Defined Default Attributes: Select this check box to enable the *Archive*, *System*, and *Hidden* check boxes, which provide the user the ability to set these attributes for the home folder. For example, if you wanted home folders to be hidden from view, you could enable the Hidden attribute by selecting the *Hidden* check box.

3 By default, Novell Storage Manager assigns the user for whom a home folder is created as the home folder owner. Because this essentially provides the owner administrative rights to the home folder, you might want to provide ownership to the network administrator instead. To override the ownership and indicate a new owner, click the *Override Path Owner* check box, then browse to and select the User object you want to establish as the owner.

The home folder user still has all rights—with the exception of administrative rights—to the home folder.

4 (Optional) To have subfolders and documents provisioned in the home folder when it is created, use an existing file path as a template.

For example, if you wanted each home folder to have an HR subfolder with some HR documents inside, click *Browse* to locate and select the HR folder in the file system.

Everything beneath the selected folder is copied into the user's home folder.

5 In the Home Folder Options region, indicate the network drive letter that users associated with this policy will use to access their home folders.

6 Click *Apply* to save your settings.

7 Proceed with Section 5.5.4, "Setting Target Paths," on page 46.

5.5.4 Setting Target Paths

The Target Paths page is where you set the paths to the shares where user home folders will be hosted.

1 In the left pane, click *Target Paths*.

2 In the Target Placement region, fill in the following fields:

Distribution: If you create more than one target path for a policy, you can indicate any of the following options:

- *Random:* Distributes storage in an ordered sequence. For example, if you have two target paths listed on this page, User A's home folder is created using the first path, User B's home folder is created using the second path, and User C's home folder is created using the first path.
- *Actual Free Space:* Distributes the creation of user home folders according to shares with the largest amount of absolute free space. For example, if you have two target paths listed, target path 1 has 15 GB of free space, and target path 2 has 10 GB, the home folders are created using target path 1.
- *Percentage Free Space:* Distributes the creation of user home folders to volumes with the largest percentage of free space. For example, if you have two target paths listed, target path 1 is to a 10 TB share that has 30 percent free space and target path 2 is to a 500 GB share with 40 percent free space, the home folders are created using target path 2, even though target path 1 has more absolute available disk space. You should be cautious when using this option with target paths to shares of different sizes.

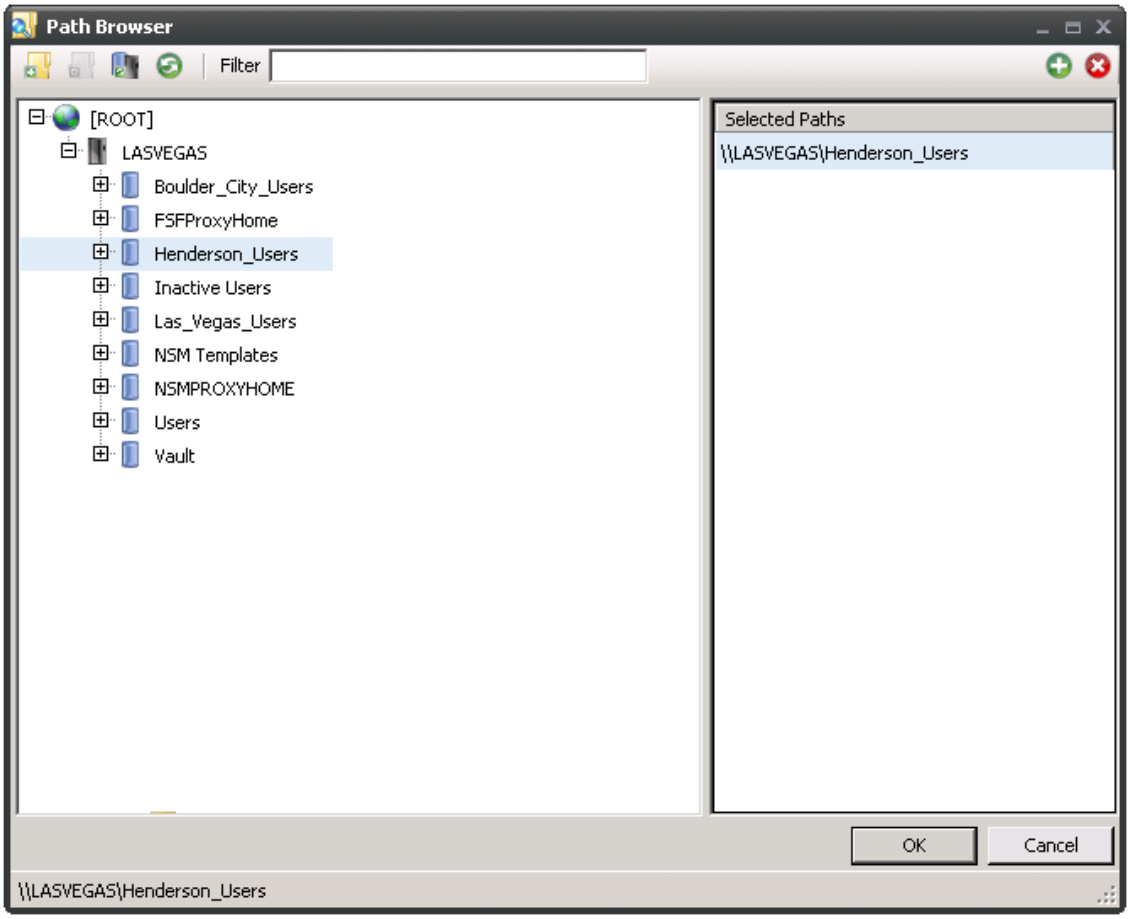
Leveling Algorithm: Use this option to structure the home folders so that they are categorized by the first or last letter of a username through a subordinate folder. For example, if you choose *Last Letter*, and the *Leveling Length* field is set to 1, a user named BSMITH has a home folder located in a path such as `\\SERVER1\HOME\S\BSMITH`.

The *Leveling Length* field allows you to enter up to 4 characters. This allows you to organize home folders by year. For example, if your Leveling Algorithm setting is *Last Letter*, and the *Leveling Length* setting is 4, a user named BMITH2013 has a home folder located in a path such as `\\SERVER\HOME\2013\BMITH2013`.

Maximum Unreachable Paths: If you have a substantial number of target paths listed on this page, this field lets you indicate the number of target paths Novell Storage Manager accesses to attempt to create a home folder before it suspends the attempt.

3 For each target path that you want to establish, click the + button to access the Path Browser.

4 Browse to the location of the target path you want and click the + button to add the target path to the Selected Paths pane.



5 Click *Apply* to save your settings.

6 Proceed to Section 5.5.5, "Setting Quota Options," on page 47.

5.5.5 Setting Quota Options

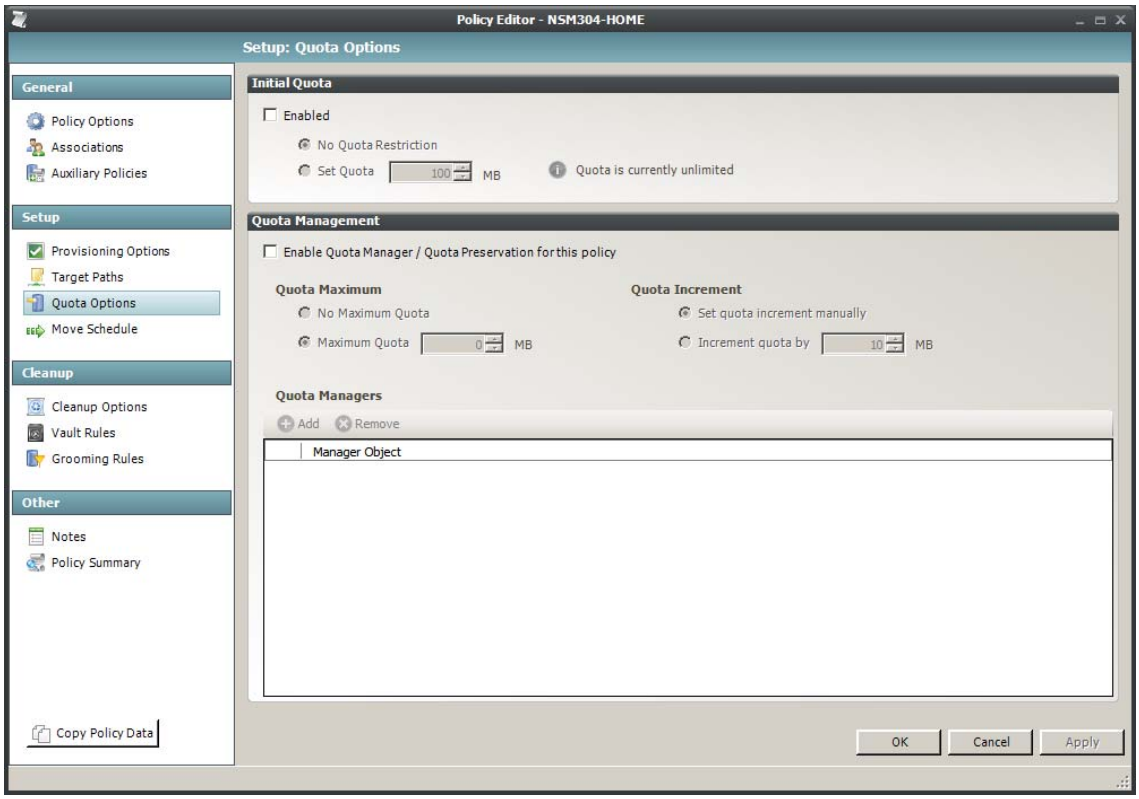
This page lets you establish user storage quotas. Until quota management is established, users have unlimited storage disk space for their home folders.

NOTE: Novell Storage Manager can manage quota on NAS devices only if the NAS device implements the Windows 2008 File Server Resource Manager DCOM interface for quota management.

This page is also where you establish quota management settings for quota managers. A quota manager is a specified user—for example, a help desk administrator or technical support rep—who is granted the ability to increase a user's quota, without having rights to the file system. Quota management actions are performed through Quota Manager, which is a separate Web browser-based management interface. For more information on Quota Manager, see Chapter 8, "Using Quota Manager," on page 97.

1 In the left pane, click *Quota Options*.

The following page appears:



2 Select the *Enabled* check box to enable an initial storage quota for users to whom this policy will apply.

   Leaving this check box deselected gives users unlimited user home folder storage.

3 In the *MB* field, specify the initial storage quota for the user home folders.

4 Set up quota managers and enable the Quota Manager Web interface for this policy by filling in the following fields:

   Enable Quota Manager / Quota Preservation for this Policy: Select this check box to enable the Quota Management region of the page and to enable quota preservation.

   Quota preservation preserves the home folder quota settings for users that are moved. For example, if a user is moved from the Sales organizational unit to the Marketing organizational unit, if the user's quota allocation for the policy that applies to Sales were higher than the quota allocation for the policy that applies to Marketing, the quota allocations from the policy associated with the Sales policy are preserved for the user.

   Quota Maximum: Indicate whether the user home folders associated with this policy will have a maximum quota setting. If so, indicate the maximum quota.

   Quota Increment: Indicate whether quota managers will set the quota manually or in set increments. If you use manual increments, the quota manager can increase the quota in any increment until it meets the maximum quota setting. If you establish set increments, the quota manager can only increase the quota by the increment setting.

   Quota Managers: Click the + button and use the Object Browser to browse to and select a user or group you want to serve as a quota manager by dragging the User or Group object over to the right pane. Repeat this for each user or group you want to establish as a quota manager.

   If you do not specify a user or group as a quota manager, only members of the NSMAdmins group will be able to use the Quota Manager Web interface.

5 Click *Apply* to save your settings.

6 Proceed with Section 5.5.6, "Setting the Move Schedule," on page 49.

5.5.6 Setting the Move Schedule

This page lets you use a grid to specify when data can be moved during data migration operations.

By default, all days and times are available for data movement. If data movement during regular business hours creates unacceptable network performance, you can choose to move data after regular business hours.

1 In the left pane, click *Move Schedule*.

2 In the Data Move Schedule grid, click the squares for the day and hour you want to disable for data movement.

3 Click *Apply* to save your settings.

4 Proceed with Section 5.5.7, "Setting Cleanup Options," on page 49.

5.5.7 Setting Cleanup Options

This page lets you enable and specify cleanup rules for the user policy. Options for cleanup include deleting a home folder after a set number of days following the removal of a User object from Active Directory, or vaulting (rather than deleting) the home folder.

1 In the left pane, click *Cleanup Options*.

2 Enable storage cleanup by filling in the following fields:

Enable: Select this check box to enable storage cleanup rules.

Cleanup storage: Specify the number of days a user home folder remains after the associated User object is removed from Active Directory.

3 Enable vault on cleanup by filling in the following fields:

Enable: Select this check box to enable vault on cleanup rules.

Vault Path: Click *Browse* to browse and select the share where you want the cleaned-up user home folders to be vaulted.

When you indicate this path, it also appears in the *Vault Path* field of the Grooming Rules page, because grooming rules and vault on cleanup rules share the same vault path.

4 Click *Apply* to save the settings.

5 Proceed with Section 5.5.8, "Setting Vault Rules," on page 49.

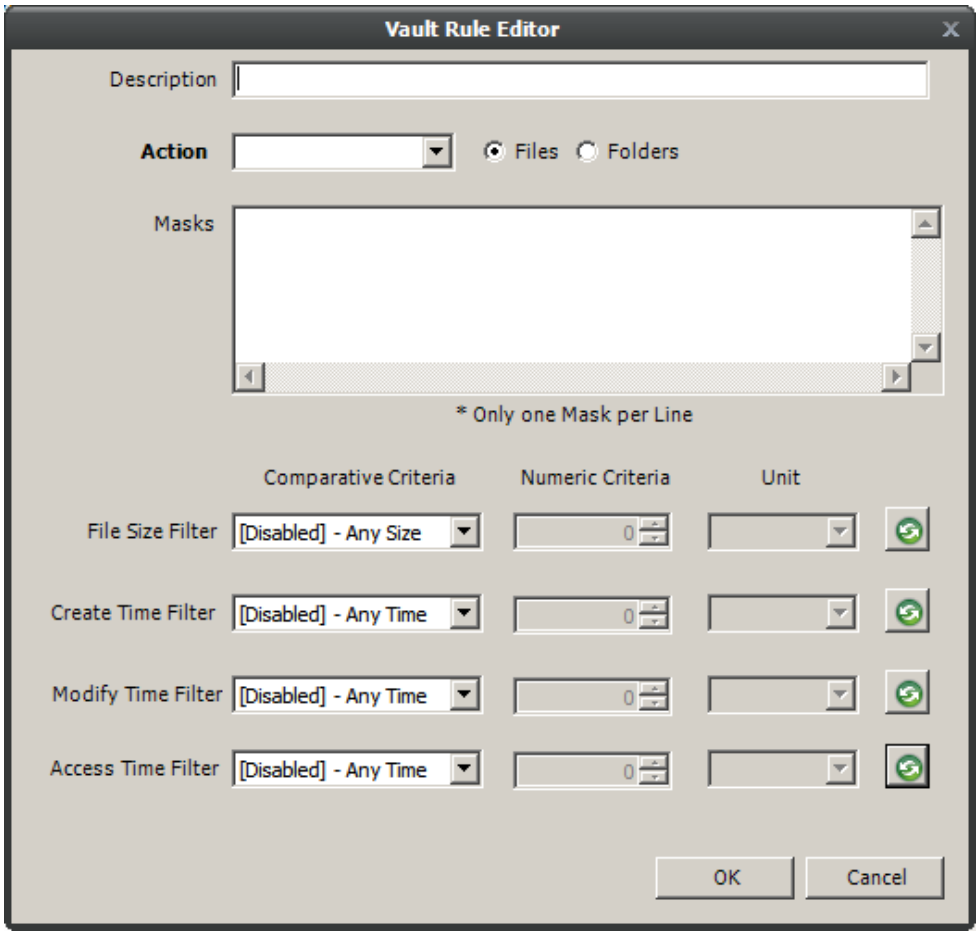
5.5.8 Setting Vault Rules

When a User object is removed from Active Directory, you can have Novell Storage Manager vault the contents of the user's home folder from a primary storage device to a less expensive secondary storage device. Novell Storage Manager lets you specify what to vault or delete through vault rules. For example, before vaulting a user's home folder, you might want to remove all `.tmp` files. Or, you might want to vault only the user's My Documents folder and nothing else in the home folder. You accomplish all of this through settings in the Vault Rules Editor.

1 In the left pane, click *Vault Rules*.

The *Vault Path* field displays the vault path that you established when you set up cleanup rules.

2 Click the + button to bring up the Vault Rules Editor.



3 In the *Description* field, specify a description of the vault rule.

For example, "Files to delete before vaulting," or "Files to vault."

4 Fill in the following fields:

Action: Select whether this vault rule will delete or vault files.

If you select *Vault*, only the files or folders that you list in the *Masks* text box are vaulted and the remainder of the home folder contents is deleted. Conversely, if you select *Delete*, only the files or folder that you list in the *Masks* text box is deleted and the remainder is vaulted.

Files: If the vault rule you are creating will vault or delete content at the file level, leave the *File* option selected.

Folders: If the vault rule you are creating will vault or delete content at the folder level, select the *Folders* option.

Selecting *Folders* disables the filter settings in the lower portion of the Vault Rules Editor.

Masks: List the files or folders you want to be vaulted or deleted, according to what is indicated in the *Action* drop-down menu.

File or folder names can contain an asterisk.

5 (Conditional) If the vault rule you are creating is specific to files, complete the applicable filter settings.

Leaving the setting as *[Disabled]-Any Size*, vaults or deletes all file types listed in the *Mask* text box according to what is indicated in the *Action* drop-down menu. Choosing any of the other options from the drop-down menu lets you indicate files to delete or vault according to size, when created, when last modified, and when last accessed.

6 Click *OK* to save the vault rule.

7 If necessary, create any needed additional vault rules by repeating the procedures above.

8 Proceed with Section 5.5.9, "Setting Grooming Rules," on page 51.

5.5.9 Setting Grooming Rules

Grooming rules in Novell Storage Manager specify the file types that you do not want network users storing in their home folders. Examples of these might be MP3 and MP4 files, MOV files, and many others. You specify in the grooming rule whether to delete or vault a groomed file.

Grooming takes place as a Management Action that is run by the administrator. A Management Action is a manual action that is enacted through NSMAdmin. For more information, see Section 12.1.4, "Management Actions," on page 209.

1 In the left pane, click *Grooming Rules*.

The *Vault Path* field displays the vault path that you established when you set up cleanup rules.

2 Click the + button to bring up the Grooming Rules Editor.

3 In the *Description* field, enter a description of the grooming rule.

For example, "Files to groom in Henderson OU."

4 Fill in the following fields:

Action: Select whether this grooming rule will delete or vault groomed files.

Files: If the grooming rule you are creating will vault or delete content at the file level, leave the *File* option selected.

Folders: If the grooming rule you are creating will vault or delete content at the folder level, select the *Folders* option.

Masks: List the files or folders you want to be vaulted or deleted, according to what is indicated in the *Action* drop-down menu.

File or folder names can contain an asterisk.

5 (Conditional) If the grooming rule you are creating is specific to files, complete the applicable filter settings.

Leaving the setting as *[Disabled]-Any Size*, vaults or deletes all file types listed in the *Mask* text box according to what is indicated in the *Action* drop-down menu. Choosing any of the other options from the drop-down menu lets you indicate files to delete or vault according to size, when created, when last modified, and when last accessed.

6 Click *OK* to save the grooming rule.

7 Proceed with Section 5.5.10, "Notes," on page 51.

5.5.10 Notes

The Notes page lets you enter up to 64,000 characters of notes for the policy you are creating. A practical use of this page is to provide a better description of the policy.

5.5.11 Policy Summary

The Policy Summary page displays a summary of the policy settings in HTML format. The Policy Summary page provides an easy way to view all of the policy settings in a single page.

5.6 Creating a User Profile Path Policy

For users in Active Directory who access the network through Remote Desktop Services, Novell Storage Manager can provision and manage a user's profile path, quota, grooming, and vaulting by setting and managing the profile path attribute.

Microsoft stores a user's profile path as follows: `\\server-name\share-name\users\user\profile`.

In managing the roaming profile user's profile path, Novell Storage Manager creates two separate profile paths in the workstation's file system. For Windows workstations running Windows Vista or Windows 7, the path is similar to the following: `\\server-name\share-name\users\user\profile.V2`.

For Windows workstations running Windows XP and earlier, the path is similar to the following: `\\server-name\share-name\users\user\profile`.

When a profile is specified for the policy, the profile is created in both of these locations. Additionally, when quota and vault paths are specified, the specifications also apply to both of the paths.

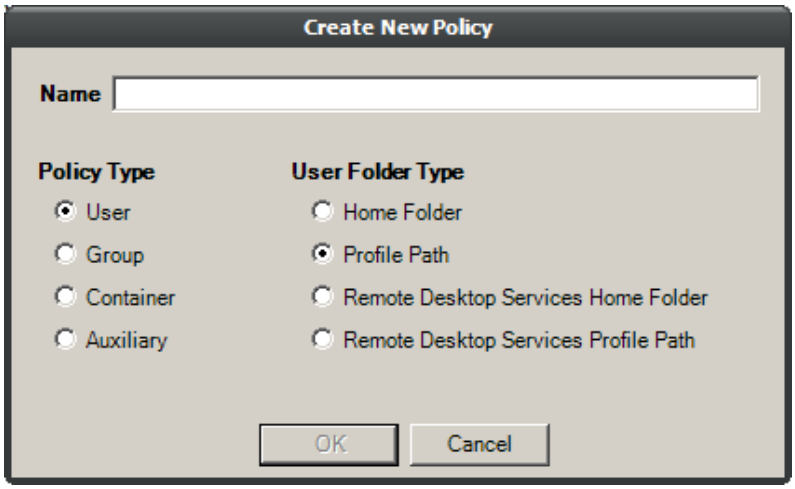
When Novell Storage Manager has provisioned a profile path for the Remote Desktop Services user, it enters settings in the *Profile path* field of the User object's Profile property.

NOTE: The Windows Full Control NTFS permission is established and cannot be modified.

5.6.1 To Create a User Profile Path Policy

1. In NSMAdmin, click *Policy Management*.
2. In the *Manage Policies* menu, select *Create Policy* > *Create User Profile Path Policy*.

   The following screen appears:



3. Specify a name in the *Name* field and leave the *User* and *Profile Path* options selected.

   The Policy Options page appears.
4. Select the options and settings that you want the policy to use.

User Profile Path Options: The fields presented on the Policy Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting policy options, see Section 5.5.1, "Setting Policy Options," on page 43.

User Profile Path Policy Associations: The Associations page is identical to the Associations page presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting associations, see Section 5.5.2, "Setting Associations," on page 44.

User Profile Path Provisioning Options: The Provisioning Options page provides only the Path Owner and Template Folder settings that are described in detail in Section 5.5.3, "Provisioning Options," on page 45.

NOTE: When you create a User Profile Path policy, the *Folder Properties* and *Home Folder Options* settings are included in the Provisioning Options page for User Home Folder policies are not included because you are only setting the profile path and not the user home folder storage.

User Profile Path Target Paths: The fields presented on the Target Paths page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting target paths, see Section 5.5.4, "Setting Target Paths," on page 46.

User Profile Path Quota Options: The fields presented on the Quota Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting quota options, see Section 5.5.5, "Setting Quota Options," on page 47.

User Profile Path Move Schedule: The fields presented on the Move Schedule page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 5.5.6, "Setting the Move Schedule," on page 49.

User Profile Path Cleanup Options: The fields presented on the Cleanup Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 5.5.7, "Setting Cleanup Options," on page 49.

User Profile Path Vault Rules: The fields presented on the Vault Rules page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting vault rules, see Section 5.5.8, "Setting Vault Rules," on page 49.

User Profile Path Grooming Rules: The fields presented in the Grooming Rules page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting grooming rules, see Section 5.5.9, "Setting Grooming Rules," on page 51.

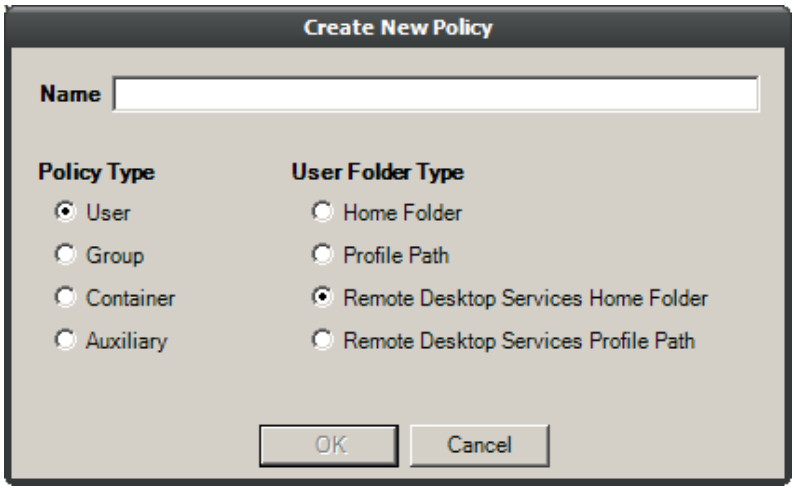
5.7 Creating a User Remote Desktop Services Home Folder Policy

Remote Desktop Services, formerly known as Terminal Services, provides users network access from remote client machines. Novell Storage Manager provisions and manages these users' home folders through User Remote Desktop Services Home Folder policies.

5.7.1 To Create a User Remote Desktop Services Home Folder Policy

1. In NSMAdmin, click *Policy Management*.
2. In the *Manage Policies* menu, select *Create Policy* > *Create User Remote Desktop Services Home Folder Policy*.

   The following screen appears:



3 Specify a name in the *Name* field and leave the *User* and *Remote Desktop Services Home Folder* options selected.

   The Policy Options page appears.

4 Select the options and setting that you want the policy to use:

User Remote Desktop Services Home Folder Policy Options: With the exception of the missing *Manage Corresponding Remote Desktop Path* check box, which is not applicable for a user Remote Desktop Services home folder policy, the fields presented on the Policy Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting policy options, see Section 5.5.1, "Setting Policy Options," on page 43.

User Remote Desktop Services Home Folder Policy Associations: The Associations page is identical to the Association page presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting associations, see Section 5.5.2, "Setting Associations," on page 44.

User Remote Desktop Services Home Folder Provisioning Options: The fields presented on the Provisioning Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting provisioning options, see Section 5.5.3, "Provisioning Options," on page 45.

User Remote Desktop Services Home Folder Target Paths: The fields presented on the Target Paths page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting target paths, see Section 5.5.4, "Setting Target Paths," on page 46.

User Remote Desktop Services Home Folder Quota Options: The fields presented on the Quota Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting quota options, see Section 5.5.5, "Setting Quota Options," on page 47.

User Remote Desktop Services Home Folder Move Schedule: The fields presented on the Move Schedule page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 5.5.6, "Setting the Move Schedule," on page 49.

User Remote Desktop Services Home Folder Cleanup Options: The fields presented on the Cleanup Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 5.5.7, "Setting Cleanup Options," on page 49.

User Remote Desktop Services Home Folder Vault Rules: The fields presented on the Vault Rules page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting vault rules, see Section 5.5.8, "Setting Vault Rules," on page 49.

User Remote Desktop Services Home Folder Grooming Rules: The fields presented on the Grooming Rules page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting grooming rules, see Section 5.5.9, "Setting Grooming Rules," on page 51.

5.8 Creating a User Remote Desktop Services Profile Path Policy

Novell Storage Manager provisions and manages Remote Desktop Services (formerly known as Terminal Services) profile policy paths through Remote Desktop Services profile path policies.

For users in Active Directory who access the network through Remote Desktop Services, Novell Storage Manager can provision and manage a user's profile path, quota, grooming, and vaulting by setting and managing the profile path attribute.

Microsoft stores a user's profile path as follows: `\\server-name\share-name\users\user\profile`

In managing the roaming profile user's profile path, Novell Storage Manager creates two separate profile paths in the workstation's file system. For Windows workstations running Windows Vista or Windows 7, the path is similar to: `\\server-name\share-name\users\user\profile.V2`

For Windows workstations running Windows XP and earlier, the path is similar to: `\\server-name\share-name\users\user\profile.`

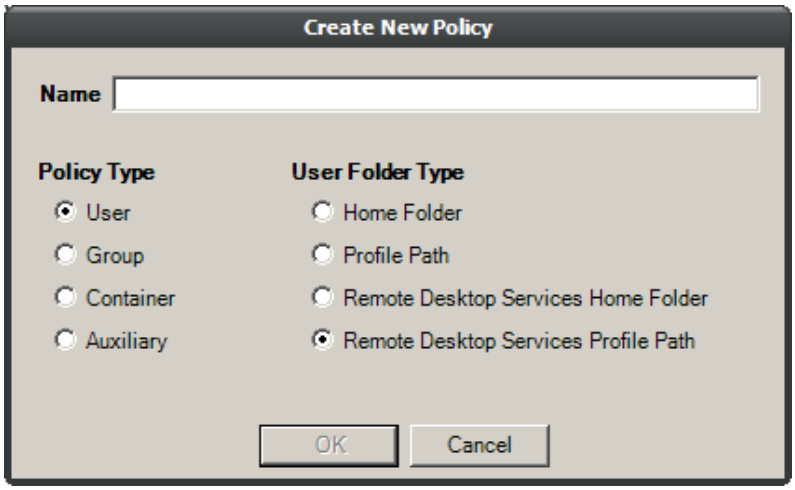
When a profile is specified for the policy, the profile is created in both of the locations above. Additionally, when quota and vault paths are specified, the specifications apply to both of the paths as well.

When Novell Storage Manager has provisioned a profile path for the Remote Desktop Services user profile, it enters settings in the *Profile path* field of the User object's Remote Desktop Services Profile property.

5.8.1 To Create a User Remote Desktop Services Profile Path Policy:

1. In NSMAdmin, click *Policy Management.*
2. In the *Manage Policies* menu, select *Create Policy* > *Create User Remote Desktop Services Profile Path Policy*.

   The following screen appears:



3 Specify a name in the *Name* field and leave the *User* and *Remote Desktop Services Profile Path* options selected.

   The Policy Options page appears.

4 Select the options and settings that you want the policy to use:

User Remote Desktop Services Profile Path Policy Options: The fields presented on the Policy Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting policy options, see Section 5.5.1, "Setting Policy Options," on page 43.

User Remote Desktop Services Profile Path Policy Associations: The Associations page is identical to the Association page presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting associations, see Section 5.5.2, "Setting Associations," on page 44.

User Remote Desktop Services Profile Path Provisioning Options: The Provisioning Options page provides only the Path Owner and Template Folder settings that are described in detail in Section 5.5.3, "Provisioning Options," on page 45.

NOTE: When you create a User Remote Desktop Services Profile Path policy, the Folder Properties and Home Folder Options settings that are included in the Provisioning Options page for User Home Folder policies are not included because you are only setting the profile path and not the user home folder storage.

User Remote Desktop Services Profile Path Target Paths: The fields presented on the Target Paths page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting target paths, see Section 5.5.4, "Setting Target Paths," on page 46.

User Remote Desktop Services Profile Path Quota Options: The fields presented on the Quota Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting quota options, see Section 5.5.5, "Setting Quota Options," on page 47.

User Remote Desktop Services Profile Path Move Schedule: The fields presented on the Move Schedule page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 5.5.6, "Setting the Move Schedule," on page 49.

User Remote Desktop Services Profile Path Cleanup Options: The fields presented on the Cleanup Options page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 5.5.7, "Setting Cleanup Options," on page 49.

User Remote Desktop Services Profile Path Vault Rules: The fields presented on the Vault Rules page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting vault rules, see Section 5.5.8, "Setting Vault Rules," on page 49.

User Remote Desktop Services Profile Path Grooming Rules: The fields presented on the Grooming Rules page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting grooming rules, see Section 5.5.9, "Setting Grooming Rules," on page 51.

5.9 Using a Policy to Manage Inactive Users

When a user leaves an organization, many organizations choose to make the User object inactive, rather than immediately delete the User object. This provides the organization an indefinite amount of time to review and determine what to do with the contents of the user's home folder before finally deleting the User object.

In Novell Storage Manager, you can easily create an Inactive Users policy that has all home folder property rights removed and apply it to an organizational unit set up specifically for inactive users. When the User object is moved to the organizational unit, the access rights for that user are immediately removed.

- Section 5.9.1, "Creating an Inactive Users Organizational Unit," on page 57
- Section 5.9.2, "Creating an Inactive Users Folder," on page 57
- Section 5.9.3, "Creating an Inactive Users Policy," on page 58
- Section 5.9.4, "Setting Inactive Users Policy Associations," on page 58
- Section 5.9.5, "Setting Inactive Users Policy Provisioning Options," on page 58
- Section 5.9.6, "Setting Inactive Users Policy Target Paths," on page 59
- Section 5.9.7, "Setting Inactive Users Policy Cleanup Options," on page 59

5.9.1 Creating an Inactive Users Organizational Unit

1. In NSMAdmin, click the *Main* tab.
2. Click Storage Management.
3. In the left pane, browse to where you want to create an inactive users organizational unit.
4. Right-click and select Create OU.
5. Give the object a descriptive name, such as "Inactive Users" and click *OK*.
6. Click *Refresh* to view the new organizational unit.

5.9.2 Creating an Inactive Users Folder

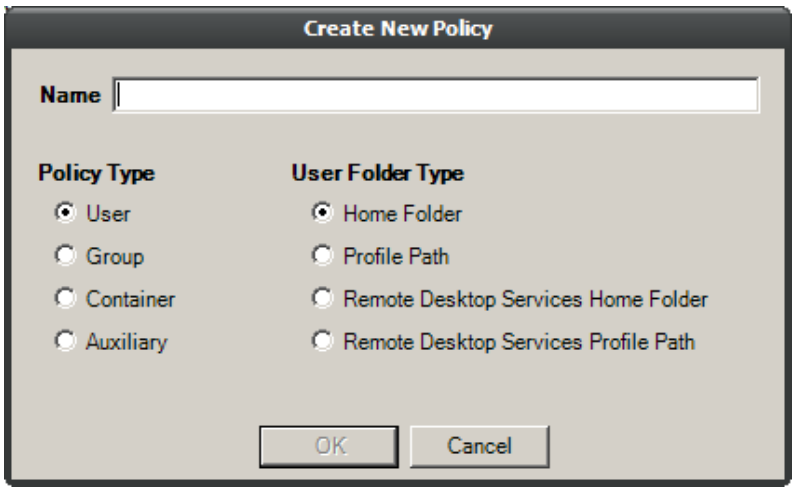
1. Launch Windows Explorer.
2. On a network share, create a folder to store inactive user home folders.

   Give the folder a descriptive name, such as "Inactive Users."

5.9.3 Creating an Inactive Users Policy

1. In NSMAdmin, click *Policy Management*.
2. In the *Manage Policies* menu, select *Create Policy* > *Create User Home Folder Policy.*

   The following screen appears:



3. Specify a descriptive name in the *Name* field, leave the *Home Folder* option selected, then click *OK*.

   The Policy Options page appears.
4. Continue with Section 5.9.4, “Setting Inactive Users Policy Associations,” on page 58.

5.9.4 Setting Inactive Users Policy Associations

1. In the left pane, click *Associations*.
2. Click the + button, then browse to and select the inactive users organizational unit you created in Step 3 on page 57.
3. Click the + button to add the inactive users organizational unit to the Selected Items panel.
4. Click *OK* to save the setting.
5. Proceed with Section 5.9.5, “Setting Inactive Users Policy Provisioning Options,” on page 58.

5.9.5 Setting Inactive Users Policy Provisioning Options

1. In the left pane, click *Provisioning Options.*
2. In the Folder Properties region of the page, deselect each of the rights check boxes.

   This assures that User objects placed in the inactive users organizational unit do not have access rights to home folders.
3. Click *OK* to save the setting.
4. Proceed with Section 5.9.6, “Setting Inactive Users Policy Target Paths,” on page 59.

5.9.6 Setting Inactive Users Policy Target Paths

1. In the left pane, click *Target Paths*.
2. Click the + button, then browse to and select the inactive users folder that your created in Step 2 on page 57.
3. Click the + button to add the inactive users folder to the Selected Items panel.
4. Click *OK* to save the setting.
5. Proceed with Section 5.9.7, "Setting Inactive Users Policy Cleanup Options," on page 59.

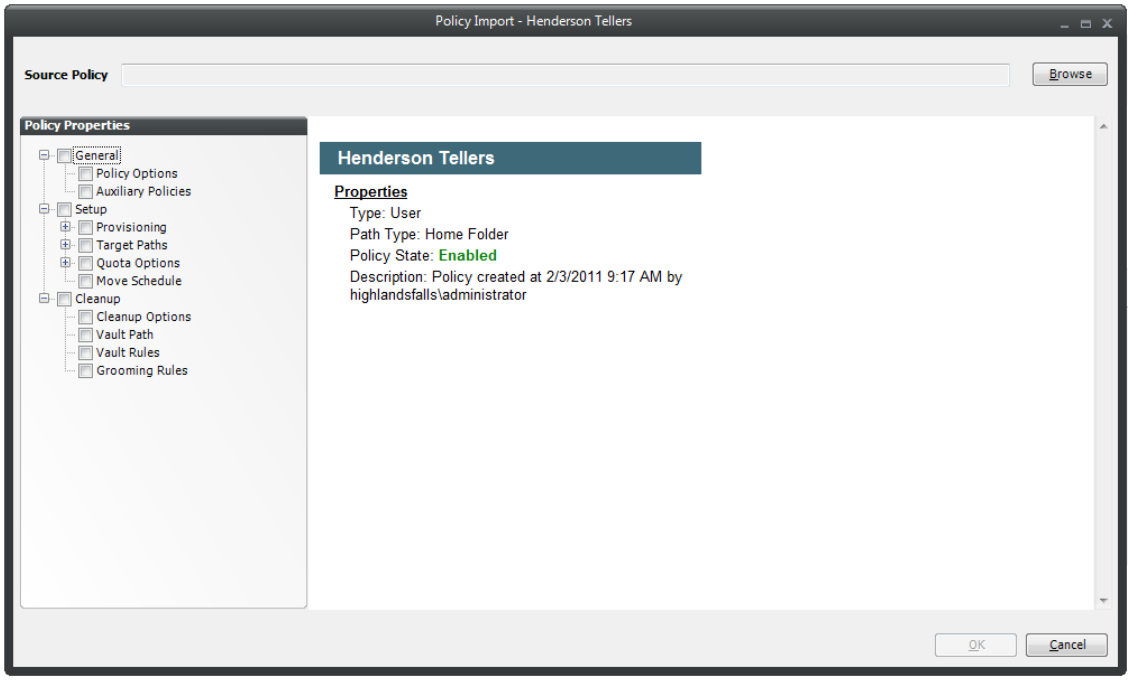
5.9.7 Setting Inactive Users Policy Cleanup Options

1. In the left pane, click *Cleanup Options.*
2. In the Storage Cleanup region, select the *Enable* check box.
3. In the *Cleanup storage* field, specify the number of days you want an inactive user's home folder to remain before it is removed from the target path for this policy.
4. Click *Apply* to save the settings.

5.10 Copying Policy Data

Copy Policy Data allows you to copy all or a portion of the policy settings of one policy into another policy.

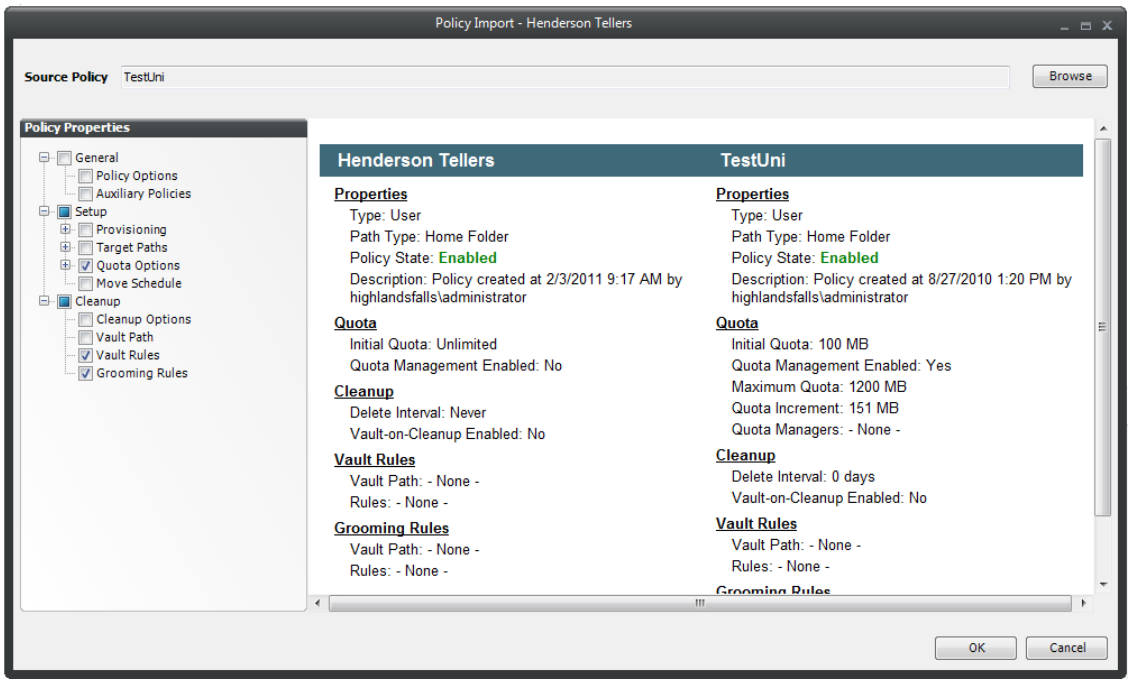
1. In NSMAdmin, click the *Main* tab.
2. Click *Policy Management*.
3. While creating a new policy or editing an existing policy, click *Copy Policy Data* in the left pane of the Policy Editor dialog box.



4 Click the *Browse* button. In the Policy Selector dialog box, select the policy from which you want to copy policy settings, then click *OK*.

The dialog box is updated to list the name of the policy from which you are copying settings.

5 In the Policy Properties region, click the settings from the policy you want to copy.



6 When you are finished selecting settings to copy, click *OK*.

5.11 Using a Policy to Manage Auxiliary Storage

Auxiliary storage allows administrators to create a policy in Active Directory that creates auxiliary storage folders when a new user is created. This auxiliary storage can even be invisible to the user for whom it was created.

For example, an organization's HR department might keep an individual folder for each user in the organization. With auxiliary user storage enabled, this folder can be created when the user joins the company and Novell Storage Manager creates and provisions his or her home folder. The user never sees the auxiliary storage, because as the policy gives Read and Write rights only to the HR department.

Additionally, the auxiliary storage can be as large as the policy specifies. This means that even though the user's home directory might have 500 MB, the auxiliary storage could be as small as the HR department needed it to be for storing HR-specific documents about the user. In fact, the policy can dictate that the auxiliary storage is provisioned with needed HR documents at the time the auxiliary storage is created.

Of course, you can configure auxiliary user storage so that a user can access it. For example, you might want to have a separate storage folder for application-specific files. It is important to remember that auxiliary storage is simply another home folder for a user. To provide access to this storage, you need to provide some sort of mapping for the user to get automated access to it.

There is no limit to the number of auxiliary folders that can be created. Auxiliary folders can be created in shares that differ from the location of the user's home folder.

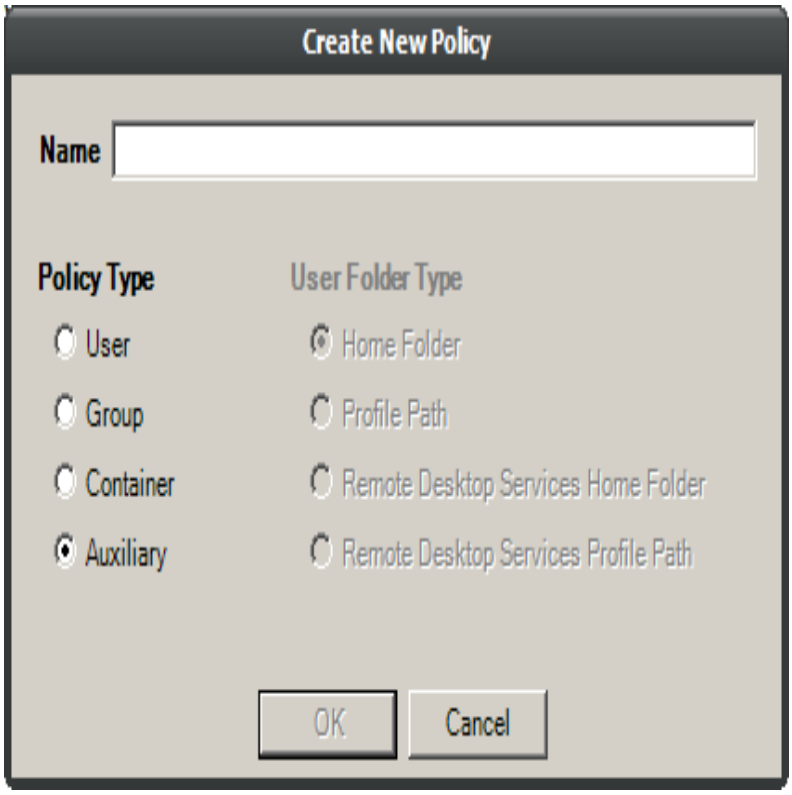
Novell Storage Manager's life cycle management capabilities easily manage auxiliary storage to the specific needs of the organization. For example, if a user transfers from one city to another and the user home directory is moved to a new Organizational Unit object as a result, the policy can dictate what becomes of the auxiliary storage including moving it, moving it and expanding it, moving it and reprovisioning it, deleting it, or leaving it where it currently is.

- Section 5.11.1, "Creating an Auxiliary Storage Policy," on page 61
- Section 5.11.2, "Linking a User Home Folder Policy to an Auxiliary Storage Policy," on page 63
- Section 5.11.3, "Provisioning Auxiliary Storage for Existing Users," on page 64

5.11.1 Creating an Auxiliary Storage Policy

1. In NSMAdmin, click *Policy Management*.
2. In the *Manage Policies* menu, select *Create Policy* > *Create Auxiliary Policy*.

   The following screen appears:



3. Specify a descriptive name in the *Name* field, such as "HR-AUX," and click *OK*.

   The Policy Options page appears.
4. Proceed with "Setting Auxiliary Storage Policy Options" on page 61.

Setting Auxiliary Storage Policy Options

1. Leave the *Process Events for Associated Managed Storage* check box selected.

If you want the settings in this policy to be inherited for all organizational units that reside within the domain or organizational unit where this policy is assigned, leave the *Policy applies to subcontainers* check box selected.

2 Proceed with "Enabling Auxiliary Storage Extended Options" on page 62.

Enabling Auxiliary Storage Extended Options

Auxiliary storage extended options help other tools, such as the AuxMap utility, identify the auxiliary storage policy through additional attributes. For information on the AuxMap utility, see Appendix D, "AuxMap," on page 259.

1 In the left pane, click *Extended Options*.

2 Click the *Enable* check box.

3 In the *Tag* field, enter a descriptive string for the auxiliary storage.

This field is used by the AuxMap utility to make auxiliary storage associations.

Novell recommends that once you have made an entry in the *Tag* field, that you do not change it. If the value of the *Tag* field is changed after some users have already had their auxiliary storage provisioned via that policy, the new tag value does not automatically get propagated to those users. Only users who get storage provisioned after the change in the tag value will get the new tag value.

4 In the *Description* field, specify a description of the auxiliary storage policy.

5 Click *Apply* to save your settings.

6 Proceed with "Setting Auxiliary Storage Provisioning Options" on page 62.

Setting Auxiliary Storage Provisioning Options

Before setting the provisioning options, you need to decide whether the user should have rights to auxiliary storage.

Additionally, if you are going to provision auxiliary storage folders with a certain structure or with specific documents, you need to place them somewhere in the file system so you can use them as a template. For example, if the HR department wants the auxiliary storage folder to have an Annual Reviews folder and an Insurance Forms folder, you need to set these up in the file system before proceeding.

1 In the left pane, click *Provisioning Options*.

2 Do one of the following:

- If you do not want the associated user to have access to the auxiliary storage folder, deselect all of the Default Rights check boxes.
- If you want the associated user to have access to the auxiliary storage folder, select the appropriate rights from the Default Rights check boxes.

3 In the Template Folder region, click the Browse button, and then specify the template path in the Path Browser dialog box.

4 Click *Apply* to save your settings.

Setting Additional Auxiliary Storage Options

1 Select the additional options that you want to use in the Auxiliary Storage policy.

Auxiliary Storage Target Paths: You need to specify the location where the auxiliary storage folders are to be located. For example, if these were HR Department folders, they would probably be located on a network share specific to the HR Department.

The fields presented on the Target Paths page are identical to those presented when you create a User Home Folder policy. For an explanation of the page along with procedures for setting target paths, see Section 5.5.4, "Setting Target Paths," on page 46.

Auxiliary Storage Quota Options: You need to specify the quota for the auxiliary storage folder associated with a user. In many cases, such as the HR Department example, this folder can be much smaller that the home folder.

The fields presented on the Quota Options page are identical to those presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting quota options, see Section 5.5.5, "Setting Quota Options," on page 47.

Auxiliary Storage Move Schedule: The fields presented on the Move Schedule page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 5.5.6, "Setting the Move Schedule," on page 49.

Auxiliary Storage Cleanup Options: The fields presented on the Cleanup Options page are identical to those presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 5.5.7, "Setting Cleanup Options," on page 49.

Auxiliary Storage Vault Rules: The fields presented on the Vault Rules page are identical to those presented when you create a User Home Folder policy. For an explanation of the page, along with procedures for setting vault rules, see Section 5.5.8, "Setting Vault Rules," on page 49.

Auxiliary Storage Grooming Rules: The fields presented on the Grooming Rules page are identical to those presented when you create a user home folder policy. For an explanation of the page, along with procedures for setting grooming rules, see Section 5.5.9, "Setting Grooming Rules," on page 51.

2 Proceed with Section 5.11.2, "Linking a User Home Folder Policy to an Auxiliary Storage Policy," on page 63.

5.11.2 Linking a User Home Folder Policy to an Auxiliary Storage Policy

This procedure connects the Auxiliary Storage policy with an existing User Home Folder policy. All new users that are added to a group or organizational unit associated with the linked user home folder policy will also have auxiliary storage created. To provide existing users with auxiliary storage, see Section 5.11.3, "Provisioning Auxiliary Storage for Existing Users," on page 64.

1 In NSMAdmin, click the *Main* tab.

2 Click *Policy Management*.

3 In the list of policies, double-click the policy you want to link to the auxiliary storage policy.

4 In the left pane of the Policy Editor, click *Auxiliary Policies*.

5 Click the + button. In the Policy Selector dialog box, select the Auxiliary Storage policy, then click *OK*.

6 Click *OK* to exit the Policy Editor.

5.11.3 Provisioning Auxiliary Storage for Existing Users

This procedure lets Novell Storage Manager manage an existing second user home folder by classifying the second home folder as an auxiliary storage folder and managing it through an auxiliary storage policy. In the process, Novell Storage Manager corrects any potential problems.

1. In NSMAdmin, click the *Main* tab.
2. Click *Policy Management*.
3. Select the auxiliary storage policy linked to the user home folder policy of the users for whom you want to create auxiliary storage.
4. In the *Policy Action* drop-down menu, select *Assign Auxiliary Attributes*.
5. Verify that the *Assign using value in policy is Auxiliary Attribute is not set* option is selected.

   This option uses the defined auxiliary storage policy path and looks for a folder that matches the common name of all users defined within the policy. If a match is found, the Auxiliary Storage Attribute is set and the users are cataloged and managed by the Auxiliary Storage policy.
6. Verify that the *Run in Check Mode* check box is selected and click *Run*.

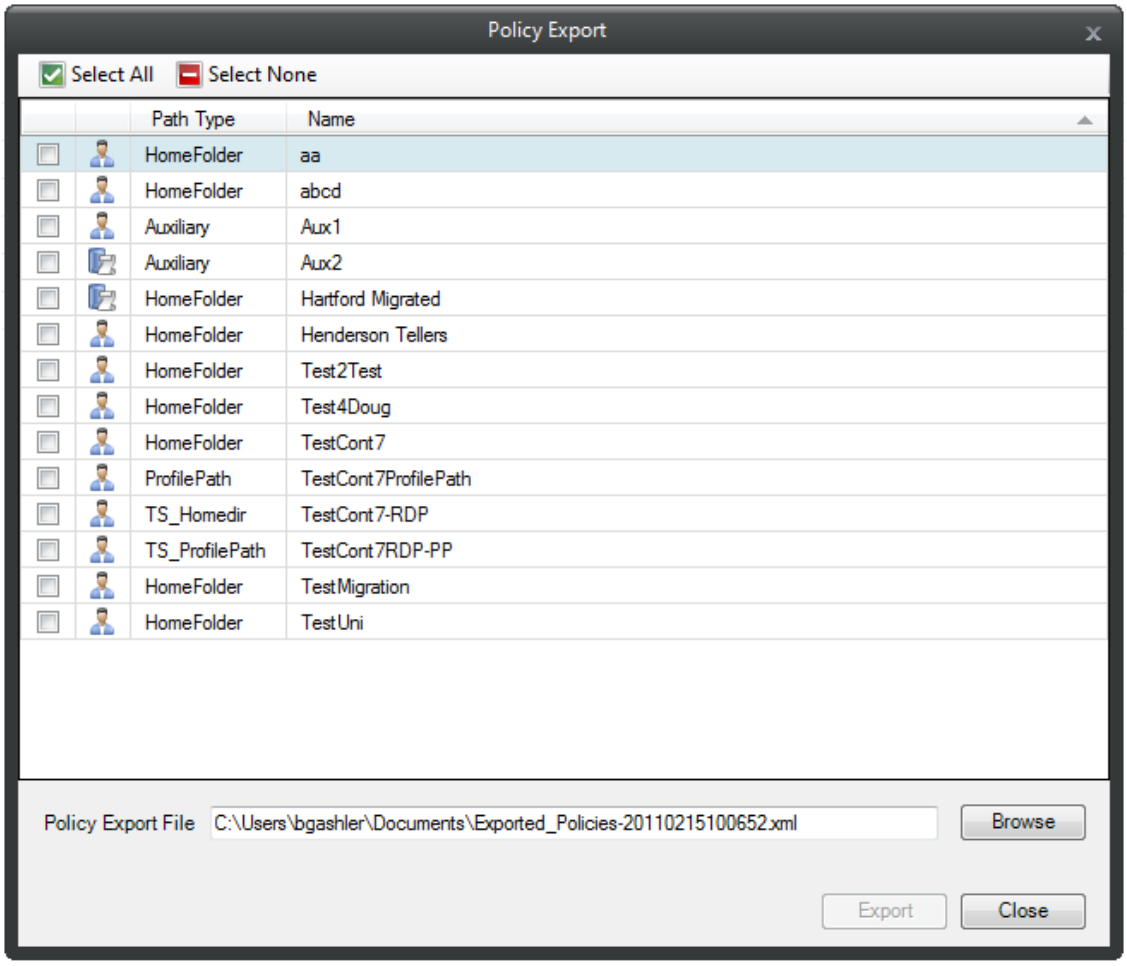
   Run in Check Mode allows you to view the results of an action without actually making changes.
7. Click *Expand* to see the results.

   Note that the Auxiliary Attribute is set for each folder that matches a User object.
8. Click *Collapse*.
9. Deselect *Run in Check Mode* and click *Run* to set the Auxiliary Attribute.
10. From the *Policy Action* drop-down menu, select *Apply Quota*.
11. Select *Set quota for all directories. Overwrite any existing quota assignments except where the existing quota is larger than the quota defined in the policy.*
12. Select *Run in Check Mode* and click *Run* to view the results.
13. Deselect *Run in Check Mode*, then click *Run* to put auxiliary storage into effect for existing users.

5.12 Exporting Policies

Novell Storage Manager provides the ability to export policies so that they can be imported later. For example, many customers first evaluate Novell Storage Manager in a lab environment and create a large number of policies in the process. You can export these policies and later import them into the production environment. All exported policies are saved in a single XML file.

1. In NSMAdmin, click the *Main* tab.
2. Click *Policy Management*.
3. From the *Manage Policies* drop-down menu, select *Export Policies*.



4 Select the check boxes of those policies you want to export.

5 Accept the default export filename or indicate a new one in the *Policy Export File* field.

6 Accept the default path of the file or browse to select a new path.

7 Click *Export*.

8 After you are notified that the policies have been exported, click *Close*.

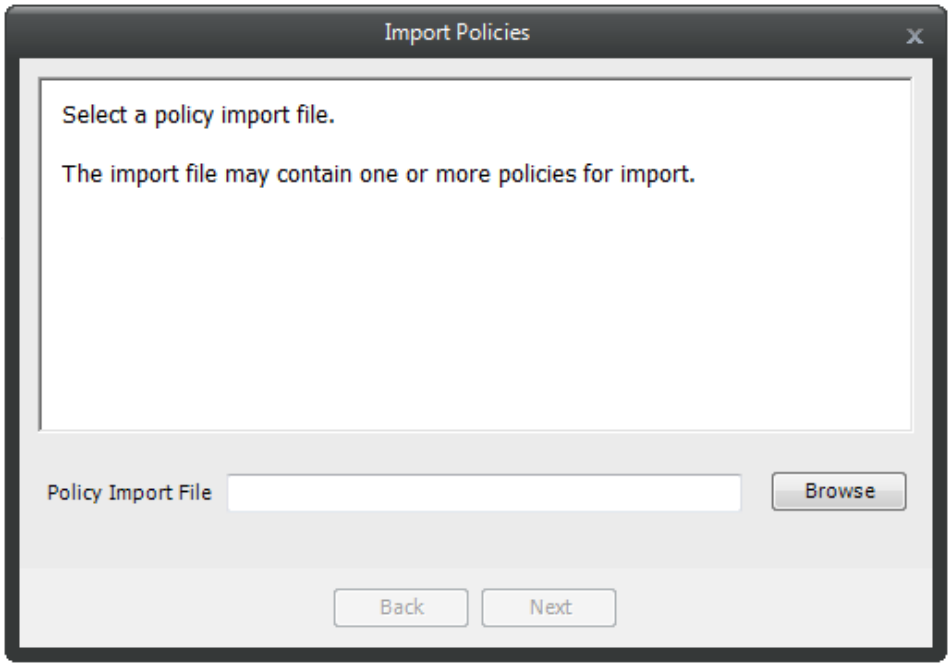
5.13 Importing Policies

Previously exported policies are imported by using the Import Policies feature.

1 In NSMAdmin, click the *Main* tab.

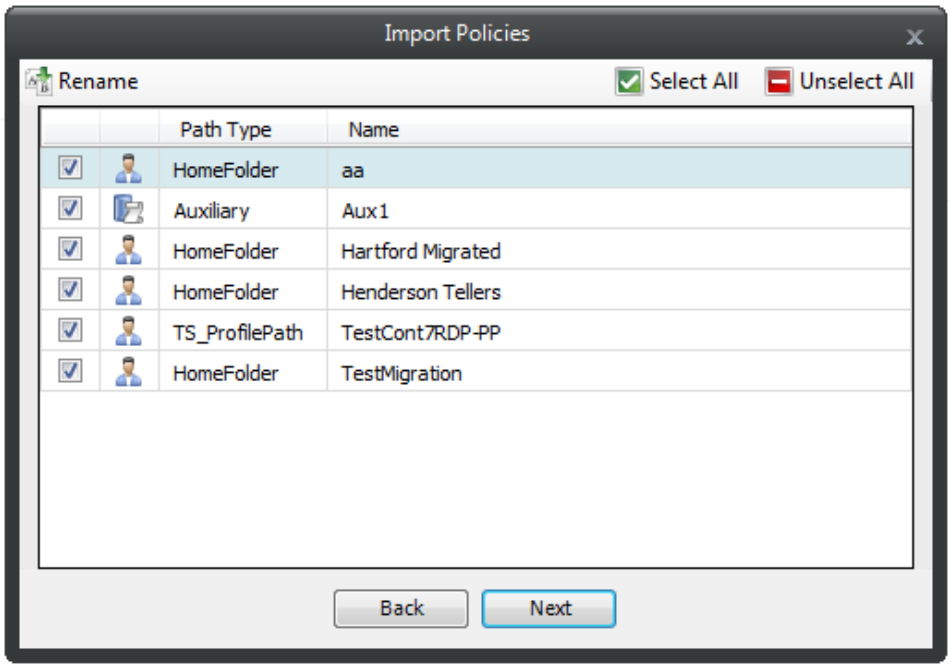
2 Click *Policy Management*.

3 From the *Manage Policies* drop-down menu, select *Import Policies*.



4 Browse to select the saved export file.

5 Click *Next*.



6 Verify that the check box for each policy you want to import is selected.

7 Click *Next*.

A status page appears indicating what policies were imported and when the import process is complete.

8 Click *Close*.

6 Managing Existing Collaborative Storage

This section includes the procedures for using Novell Storage Manager to manage the home folders that are assigned to Group objects or containers in Active Directory.

In a Novell Storage Manager environment, group-based or container-based storage is referred to as "collaborative storage," because Novell Storage Manager, through its collaborative policies, provides the means of creating storage folders where members can easily collaborate through a single project folder, or even through a structured project folder where all members have personal subfolders.

Similar to Chapter 4, "Managing Existing User Storage," on page 23, this section provides the basic procedures for managing collaborative storage, which includes associating groups and containers with shared storage, and setting the target path, quota rules, and grooming rules.

This section does not provide procedures for establishing a structured project folder with personal subfolders, which are enabled through template creation and Dynamic Template Processing. For a comprehensive discussion on managing collaborative storage, including Dynamic Template Processing, see Chapter 7, "Managing Collaborative Storage," on page 77.

The process for managing existing storage and creating personal subfolders involves several tasks:

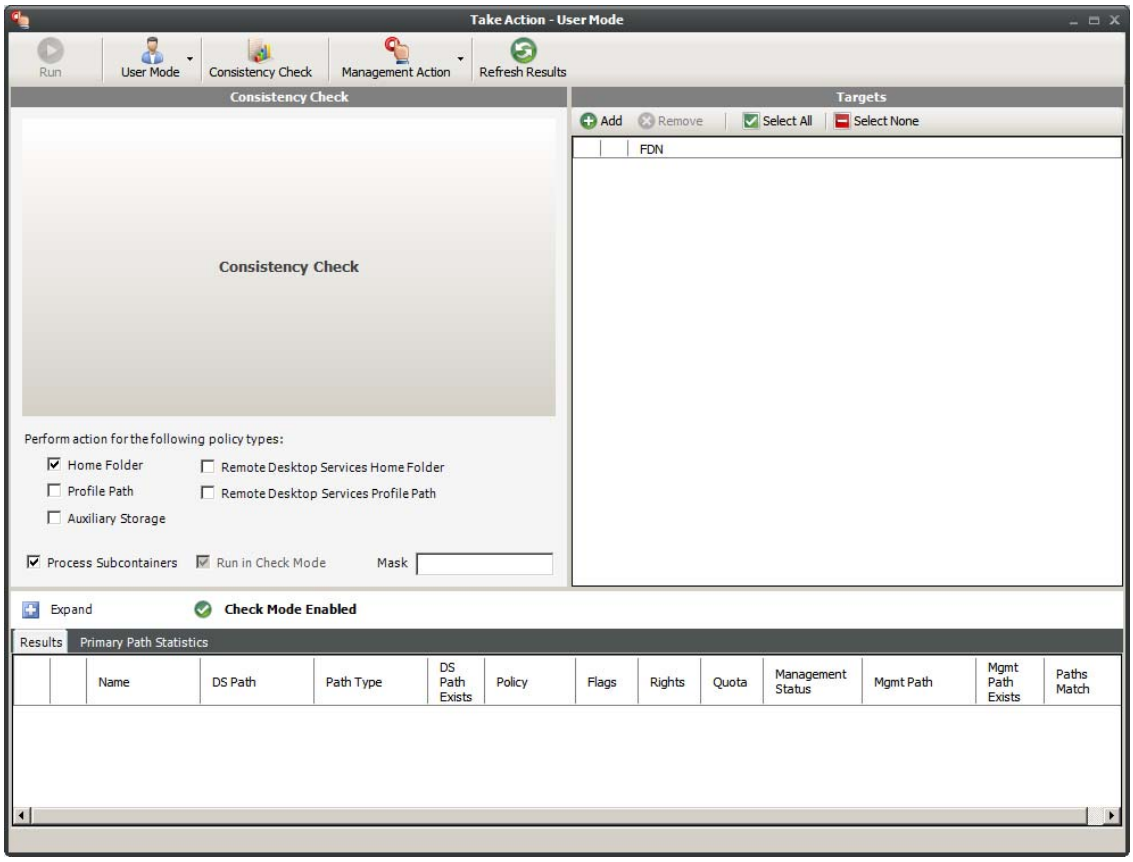
- Section 6.1, "Assigning a Managed Path to Existing Group-based or Container-based Storage," on page 67
- Section 6.2, "Creating a Collaborative Storage Policy," on page 70
- Section 6.3, "Performing Management Actions," on page 73
- Section 6.4, "Editing Collaborative Storage Policies," on page 75

6.1 Assigning a Managed Path to Existing Group-based or Container-based Storage

A managed path group home folder attribute is a folder attribute that is created by Novell Storage Manager when the Active Directory schema is extended. It is needed to associate a Group or container object with a managed path.

In this procedure, you assign a managed path group home folder attribute to a Group or container object that has existing collaborative storage and then assign the storage path. This path is then used in the collaborative storage policy that you create later.

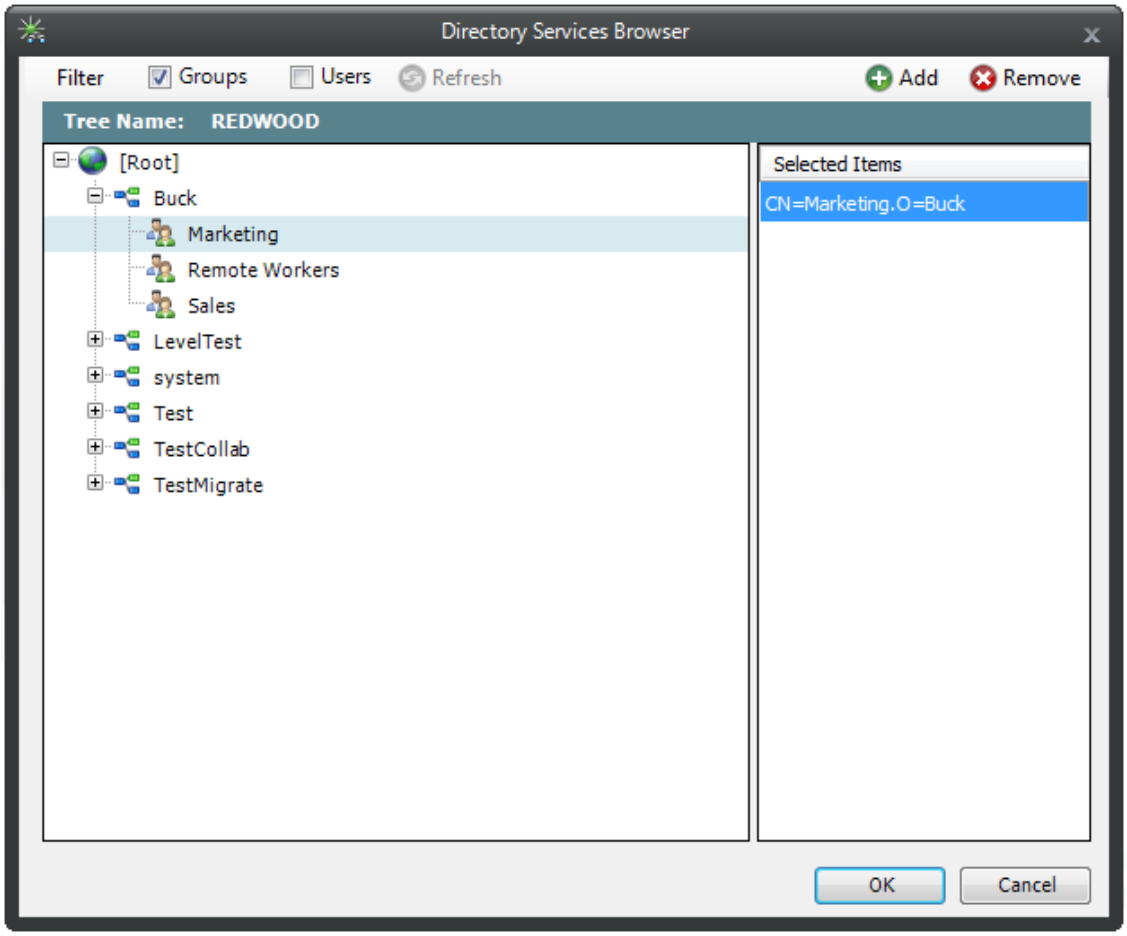
1. In NSMAdmin, click the *Main* tab.
2. Click *Management Action*.



3 Use the menu to replace *User Mode* with *Group Mode* or *Container Mode*.

4 In the Targets region, click *Add*.

5 Browse to locate and select the container or group you want to associate to a group storage area, then click *Add*.



6 Click *OK*.

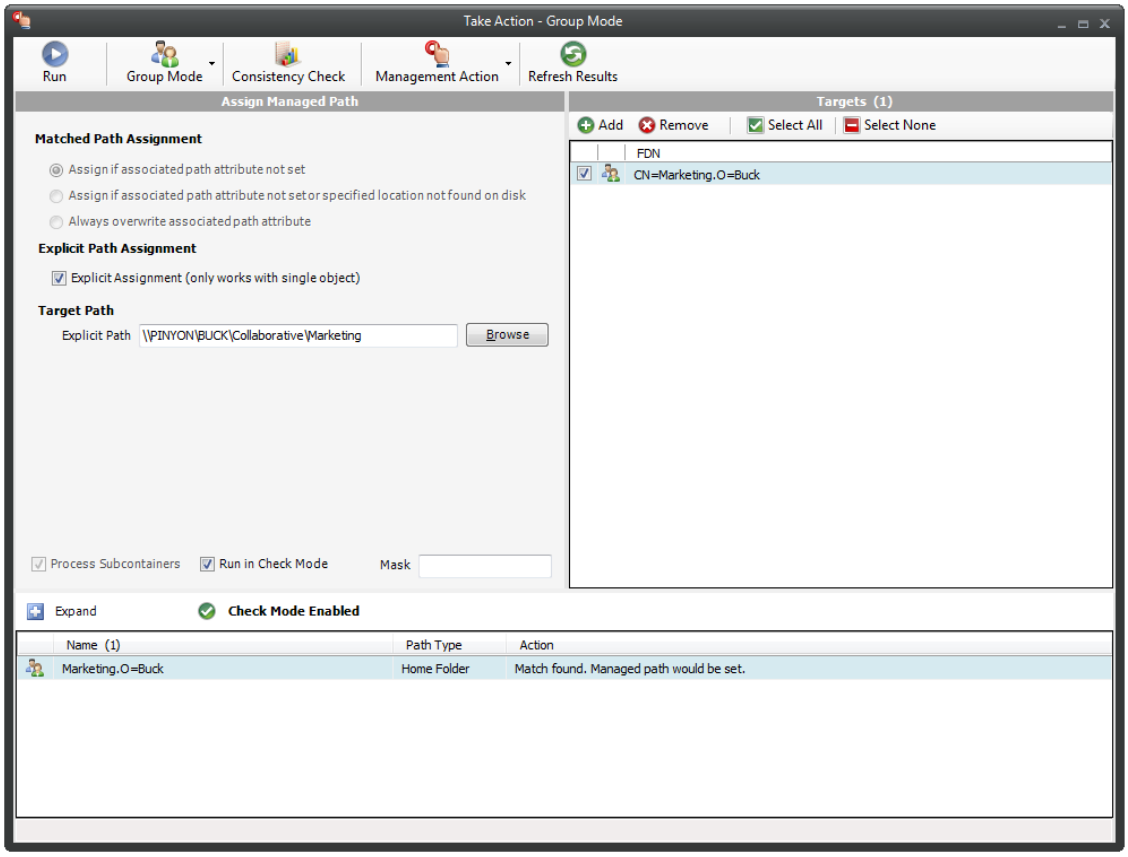
7 Click *Management Action* > *Assign Managed Path*.

8 Select the *Explicit Assignment* check box.

9 Click *Browse*, then locate and select the group storage folder you want to manage through Novell Storage Manager.

10 Verify that the *Run in Check Mode* check box is selected.

11 Click *Run*.



12 Deselect *Run in Check Mode*, then click *Run*.

13 Observe in the bottom portion of the page that the managed path has been set.

14 Continue with Section 6.2, "Creating a Collaborative Storage Policy," on page 70.

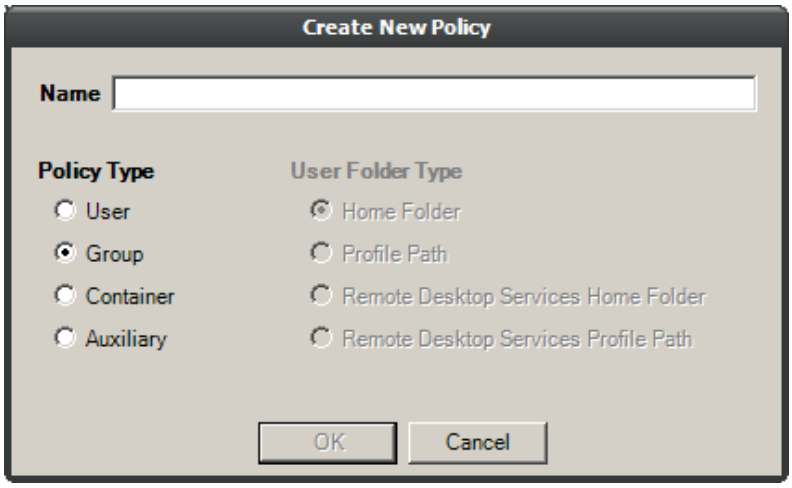
6.2 Creating a Collaborative Storage Policy

After you assign a managed path, the next step is to create a collaborative storage policy for the group or container you selected in Step 5 on page 68. The collaborative storage policy will apply to all existing users of the group or container, as well as any that are added at a later time.

1 In NSMAdmin, click the *Main* tab.

2 Click *Policy Management*.

3 Select *Manage Policies* > *Create Policy* > *Create Group Policy*.

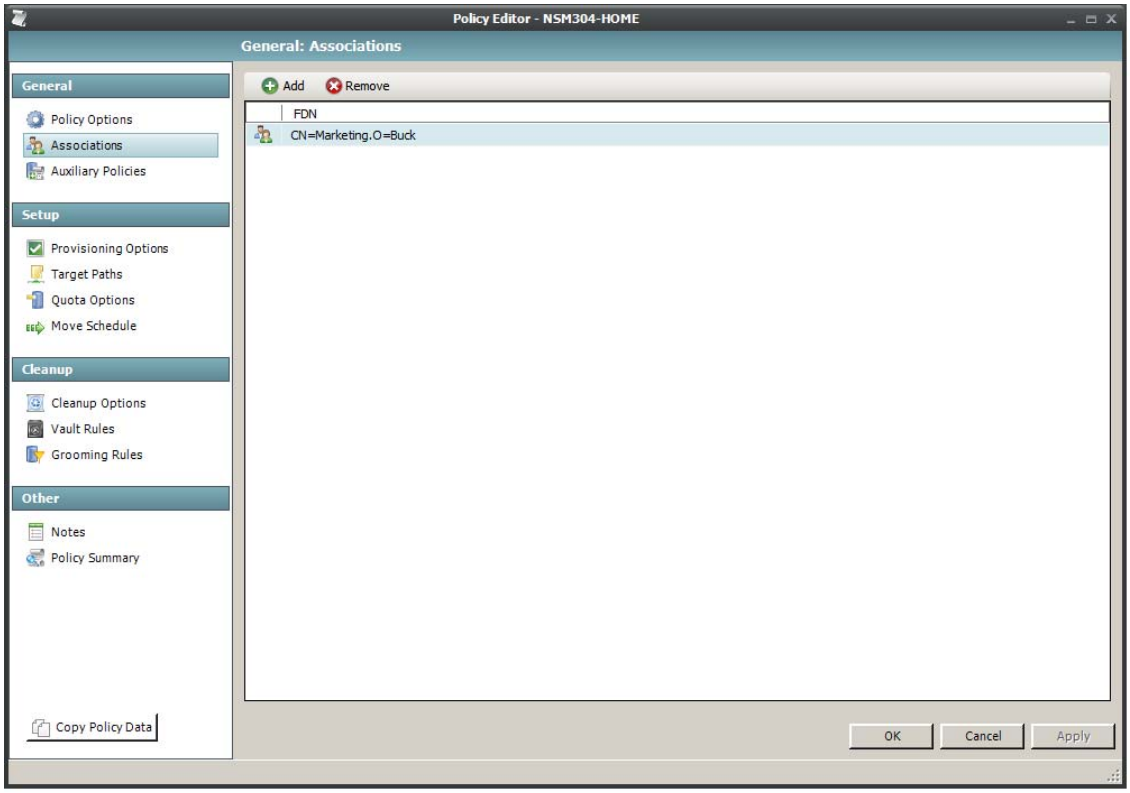


4 Specify a descriptive name for the new policy and click *OK*.

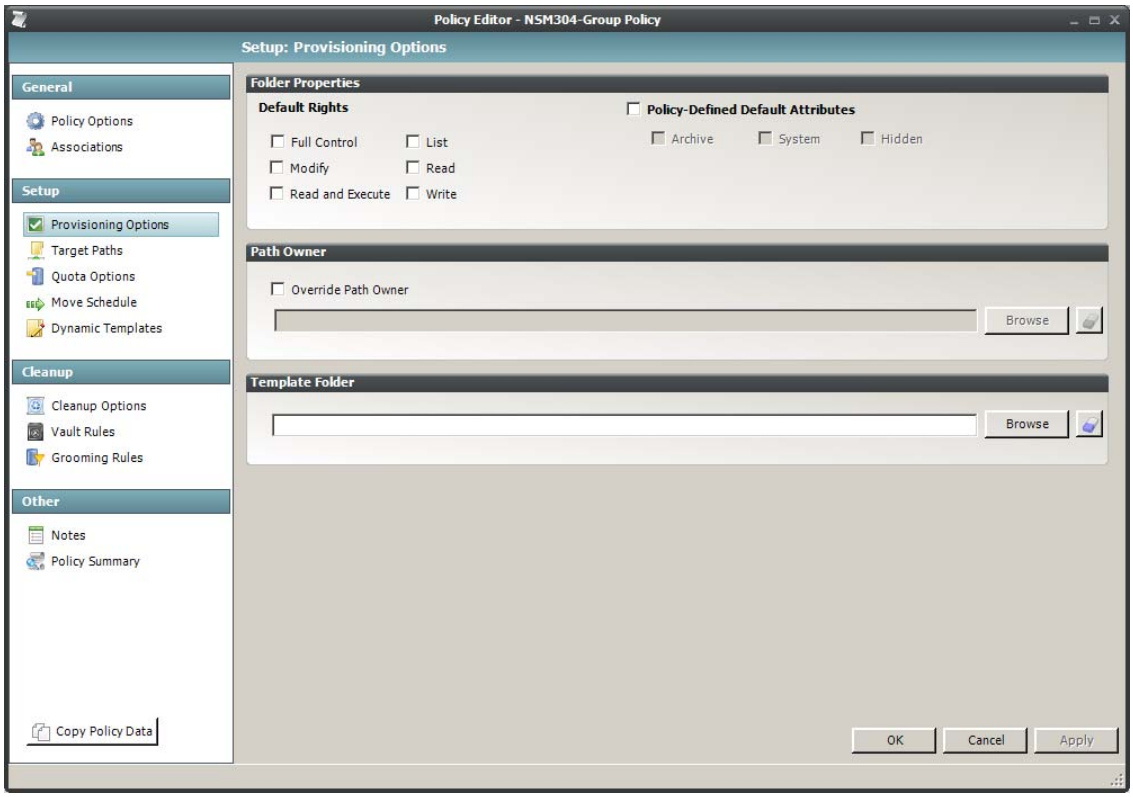
5 In the left panel, click *Associations*.

6 At the top of the right pane, click *Add* and browse to select the group or container that you selected in Step 5 on page 68.

7 Click *Add*, then click *OK*.



8 In the left panel, click *Provisioning Options*.



9 In the Default Rights region, specify the rights that you want users in the specified group or container to have to the collaborative storage home folder.

   These rights are those that all members of the group or container will have to the folder.

10 In the Policy-Defined Default Attributes region, select the *Policy-Defined Default Attributes* check box.

   This enables the Rename Inhibit and Delete Inhibit attributes, which in most cases you should leave selected.

11 (Conditional) From the other attributes in this region, select any additional attributes you want to apply.

12 In the left panel, select *Target Paths*, then click *Add*.

13 Browse to select the folder you selected in Step 9 on page 69.

14 Click *Add*, then click *OK*.

15 In the left panel, select *Quota Options*.

16 In the Initial Quota region, select the *Enabled* check box and specify the amount of initial quota you want assigned to the collaborative storage folder.

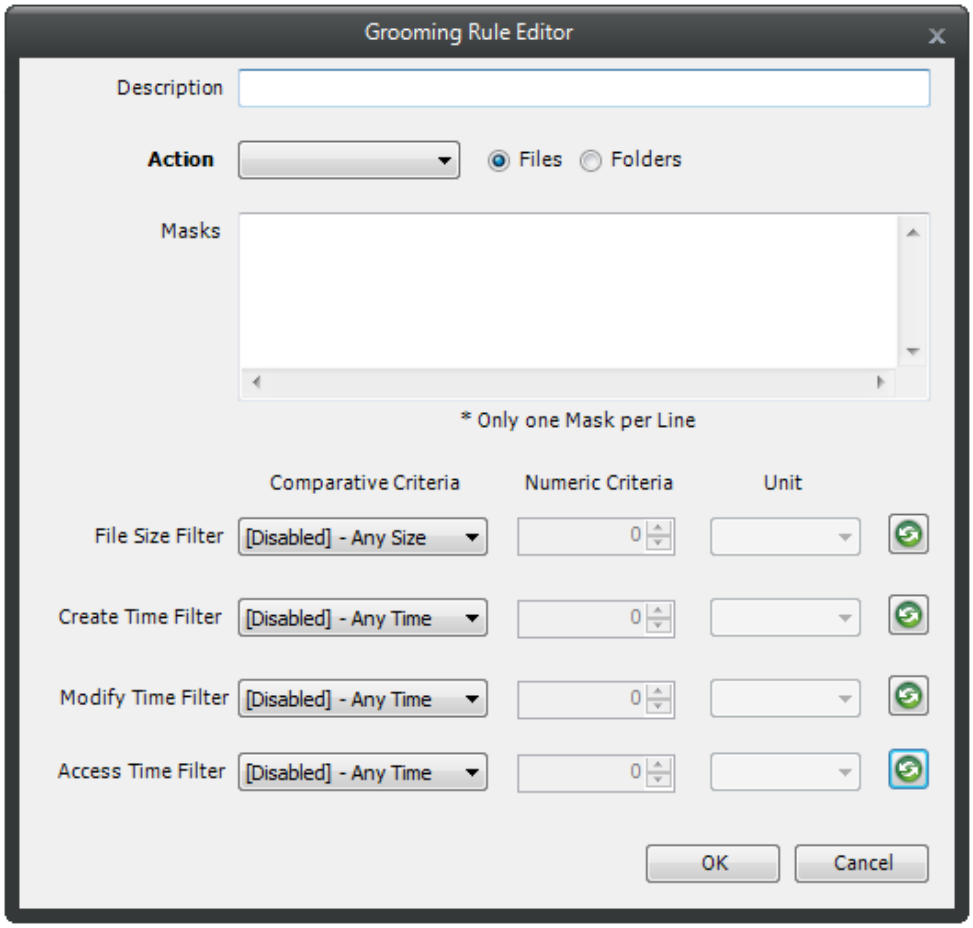
17 (Conditional) If you want to set specifications for a quota manager, select *Enable Quota Manager / Quota Preservation for this policy* and set quota maximums, increments, and managers.

18 In the left pane, select *Grooming Rules*.

19 Browse to select the folder where you want to vault the files that will be groomed.

   If the folder does not exist, you can right-click to create the folder.

20 Click *OK* to save the vault path, then click *Add*.



21 In the Grooming Rule Editor dialog box, indicate the files that Novell Storage Manager will groom from the collaborative storage pertaining to this policy.

For information on each of the fields in this dialog box, refer to Section 5.5.9, "Setting Grooming Rules," on page 51.

22 Click *OK* to save the grooming rule.

23 Continue with Section 6.3, "Performing Management Actions," on page 73.

6.3 Performing Management Actions

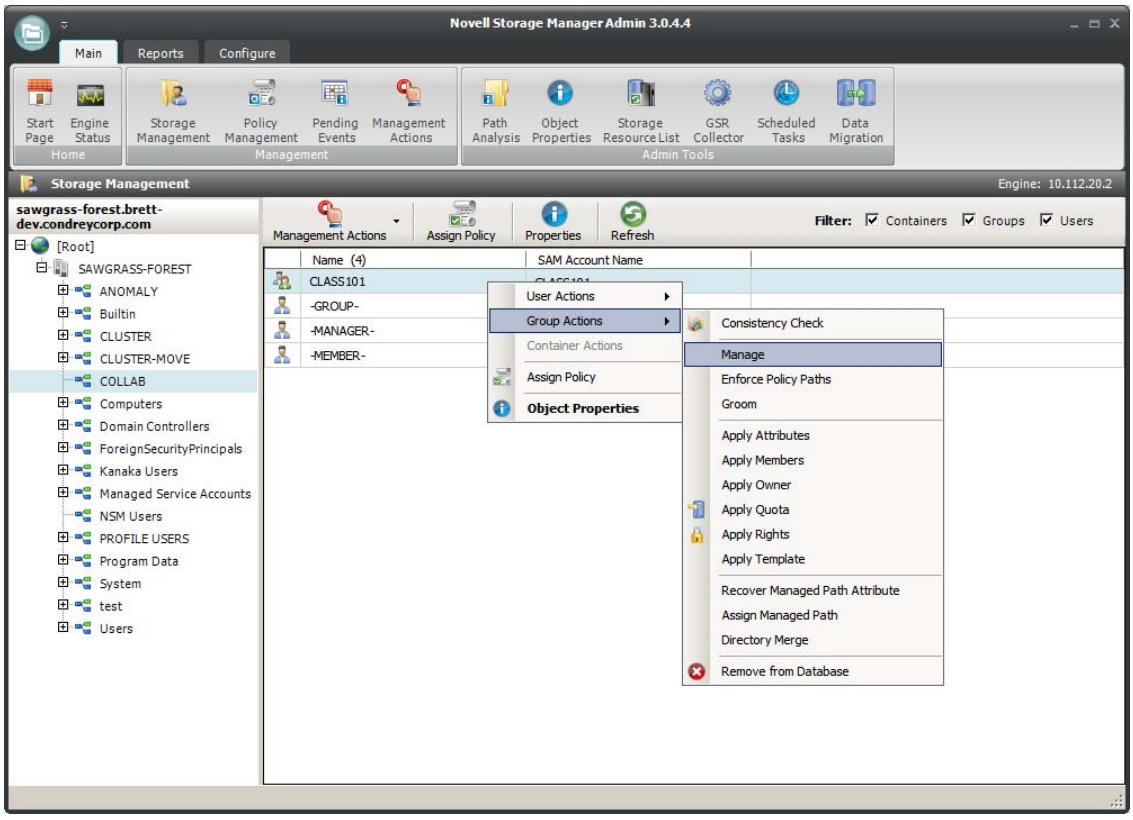
This procedure enforces the policy for all members of the group or container to which the collaborative storage policy is applied.

1 In NSMAdmin, click the *Main* tab.

2 Click *Storage Management*.

3 Browse to and select the group or container that you specified in Step 5 on page 68.

4 Right-click the group or container and select *Group Actions* > *Manage*.



5 Verify that *Run in Check Mode* is selected, then click *Run*.

6 Verify that the following message appears in the lower panel of the window:

```
Catalog Existing Managed Path Location.
```

7 Deselect the *Run in Check Mode* check box, then click *Run*.

8 From the *Management Action* menu, select *Apply Attributes*.

9 Select the *Use policy definitions* check box.

10 Select the *Run in Check Mode* check box, then click *Run*.

11 Verify that the following message appears in the lower panel of the window:

```
Apply attributes will be applied for object.
```

12 Deselect the *Run in Check Mode* check box, then click *Run*.

13 From the *Management Action* menu, select *Apply Quota.*

14 Verify that the *Set quota for directories that do not have quota defined* option is selected.

15 Select the *Run in Check Mode* check box, then click *Run*.

16 Verify that the following message appears in the lower panel of the window:

```
Apply quota will be scheduled for object.
```

17 Deselect the *Run in Check Mode* check box, then click *Run*.

18 From the *Management Action* menu, select *Apply Rights.*

19 Select the *Run in Check Mode* check box, then click *Run*.

20 Verify that the following message appears in the lower panel of the window:

```
Apply rights will be scheduled for object.
```

21 Deselect the *Run in Check Mode* check box, then click *Run*.

22 From the *Management Action* menu, select *Groom*.

23 Select the *Run in Check Mode* check box, then click *Run*.

24 Verify that the following message appears in the lower panel of the window:

```
Groom scheduled for object.
```

25 Deselect the *Run in Check Mode* check box, then click *Run*.

6.4 Editing Collaborative Storage Policies

In this section, you created a basic collaborative storage policy designed to manage a non-structured storage folder. If you decide later that you want to edit the policy to adjust the quota, modify the target path, or even structure the group or container home folder with personal folders for each group or container member, you can easily do so.

For more comprehensive information on collaborative storage policies, including their ability to create structured group-based or container-based storage folders through Dynamic Template Processing, see Chapter 7, “Managing Collaborative Storage,” on page 77.

7 Managing Collaborative Storage

Collaborative storage is a shared storage area where a group of people in an organization can collaborate by sharing files. For example, a cross-functional project team in an organization might need a collaborative storage area where all members could access and submit project files.

Novell Storage Manager lets you easily create collaborative storage areas through collaborative storage policies that you can assign to Group objects or to an organizational unit (also known as a container). You can structure the collaborative storage in one of two ways:

- Creating a single project folder where all project members have access and have the same rights.
- Creating a project folder with a specified owner. The project folder has subfolders for each of the members of the group. This configuration is done through Dynamic Template Processing. For more information on Dynamic Template Processing, see Setting Group Policy Dynamic Template Processing.

Novell Storage Manager works with Active Directory to ensure that only members of the Group object have access to collaborative storage. As new members are added to the group, they are automatically granted access to the collaborative storage. As members are removed, they are denied access, but the files that they submitted to the collaborative storage folder remain.

In this chapter, you will learn how to create collaborative storage policies. These include:

- Group-based collaborative policies
- Container-based collaborative policies

- Section 7.1, “Creating Collaborative Storage Objects in Active Directory,” on page 77
- Section 7.2, “Understanding Collaborative Storage Template Folders,” on page 78
- Section 7.3, “Determining How You Want to Structure Your Collaborative Storage,” on page 78
- Section 7.4, “Creating a Collaborative Storage Template,” on page 79
- Section 7.5, “Setting Up Security for a Collaborative Storage Template,” on page 80
- Section 7.6, “Understanding Collaborative Storage Policies,” on page 85
- Section 7.7, “Creating a Group Collaborative Storage Policy,” on page 85
- Section 7.8, “Creating a Container Collaborative Storage Policy,” on page 95

7.1 Creating Collaborative Storage Objects in Active Directory

For Novell Storage Manager to manage collaborative storage, it must have the following Group or User objects located in an organizational unit in Active Directory:

- -MEMBER-
- -MANAGER-
- -GROUP-

These objects are needed for assigning rights to the collaborative storage template folders (that you will create later) for the group members, the manager, and the group itself.

IMPORTANT: You only need to create these objects in one organizational unit.

1. At a Windows workstation, click *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
2. Right-click an organizational unit and select *New* > *Group*.
3. Give the Group object the name -MEMBER- and leave the Group Scope setting as *Global* and the Group Type setting as *Security*.
4. Repeat Step 2 to create a -MANAGER- group and a -GROUP- group.

   These three objects are used to automatically set rights for the collaborative storage. Make sure you name the objects exactly as indicated. The object names can either be uppercase or lowercase.

7.2 Understanding Collaborative Storage Template Folders

When you created user home folder policies in Chapter 5, "Managing User Home Folders," on page 39, a field in the Provisioning Options page let you indicate the path to a template for provisioning folder structure and content in the home folder.

For collaborative storage management, you can also indicate a template path for provisioning and folder structure within the collaborative storage folder. When Novell Storage Manager creates a collaborative folder for a group, Novell Storage Manager examines the policy to determine if a template has been defined and, if so, it copies the contents of the template directory along with all attributes, trustee assignments, and quotas.

If you want to enable quota management for collaborative storage folders, the folders must have the following characteristics:

- Be located on servers running either Windows Server 2008 or above
- Have a firewall exception for the Remote File Server Resource Manager
- Have a quota assignment set through the Windows Server Manager tool for any of the following folders: -MEMBER-, -GROUP-, -MANAGER-

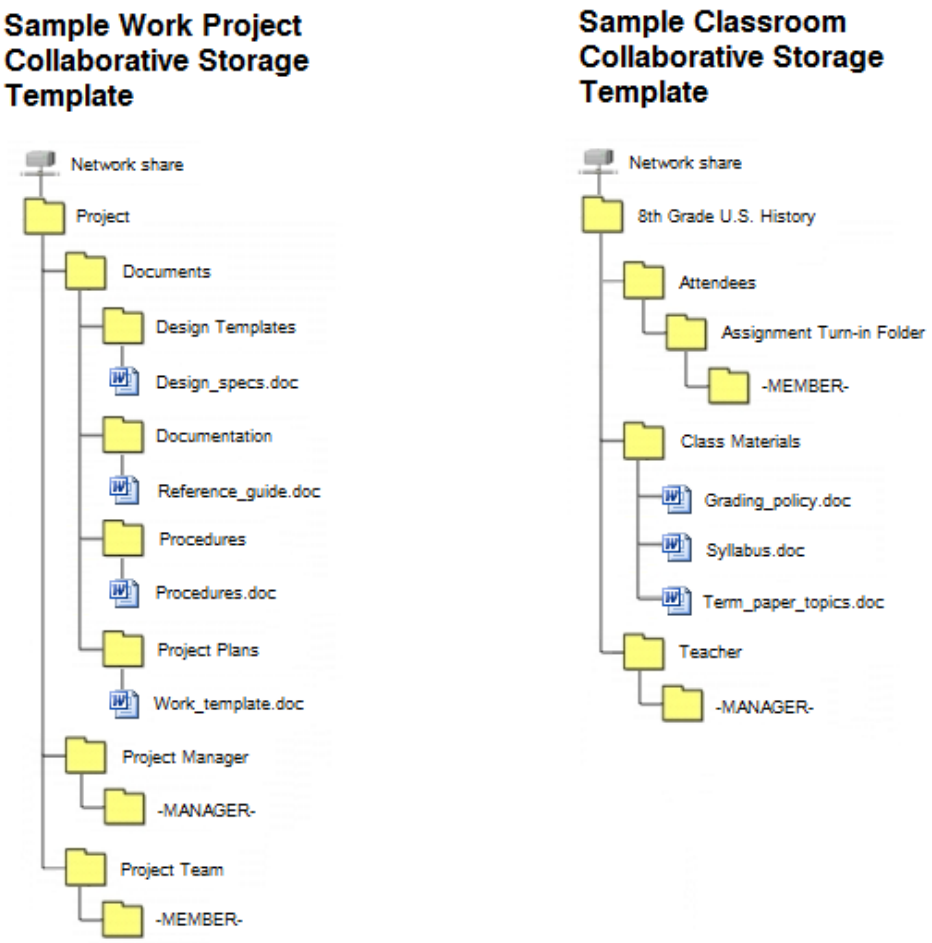
Unlike user home folders, collaborative disk space managed by Novell Storage Manager is dynamic in that the member attributes of Group objects are monitored so that the addition and deletion of members can have a direct impact on the structure of the individual file system of a group as well as the rights given within the structure.

7.3 Determining How You Want to Structure Your Collaborative Storage

Your collaborative storage area should be structured so that it optimally serves the needs of your collaborative users. The collaborative storage needs of a cross-functional team at an architectural firm would be quite different from a junior high school history class.

Two sample designs are shown below.

Figure 7-1 *Sample Collaborative Storage Templates*



In the template structures above, both have -MANAGER- and -MEMBER- folders. This means that there is a personal folder created for the designated manager of the group, along with personal folders created for each member of the group.

In order for those folders to be created and managed properly, the -MANAGER- and -MEMBER- folders must not exist in the same folder.

In the project collaborative storage template, all members can see the contents of each member's folder—except for the designated manager's folder. In the classroom template, class members cannot see the contents of other classmate's folders because members have rights only to their personal folders.

7.4 Creating a Collaborative Storage Template

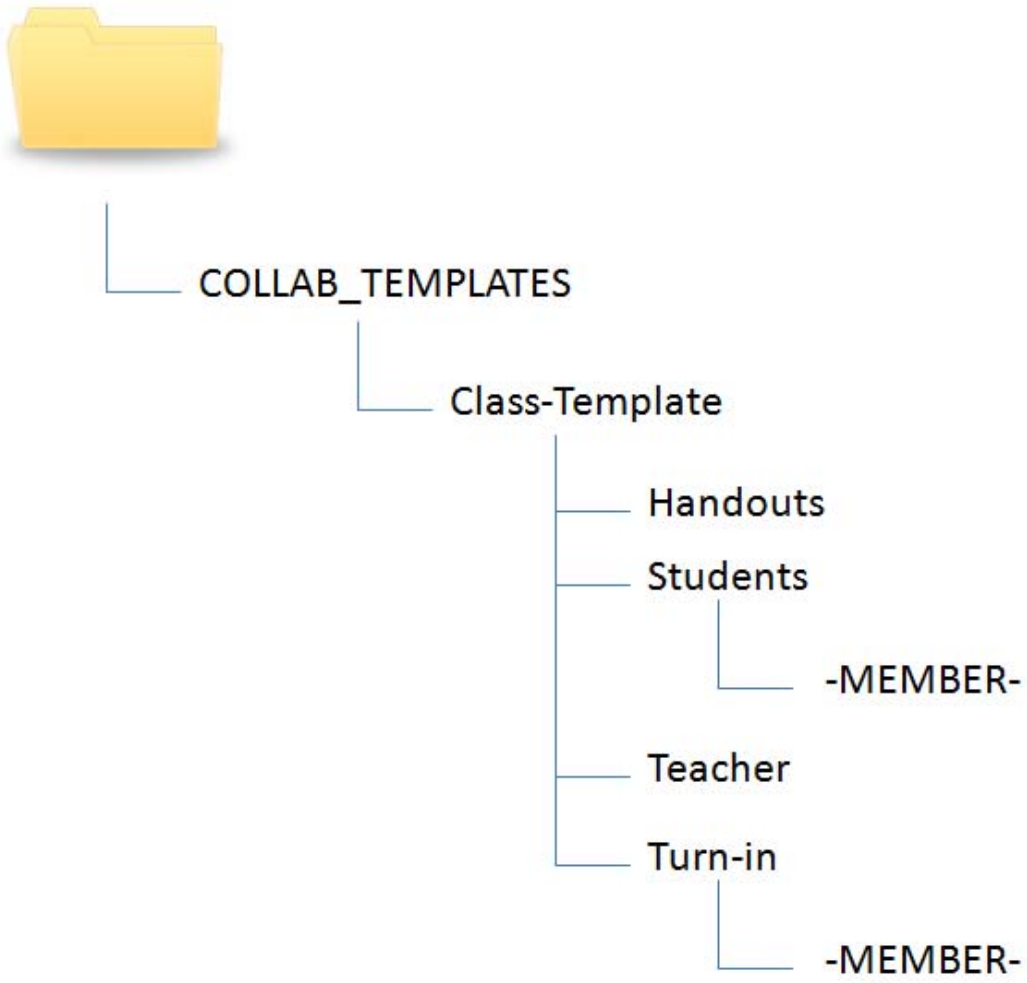
1. Launch Windows Explorer.
2. On a network share, create a file structure for a group for which you will provide collaborative storage.
3. Place any documents you want available to the group in the appropriate folders.

7.5 Setting Up Security for a Collaborative Storage Template

Properly setting security and rights for collaborative storage in Active Directory can be potentially confusing. For this reason, we are providing an example of the correct way to set up security for a collaborative storage template.

The example provided is for a school class where the instructor is using a collaborative storage folder as the means of distributing assignments to students, as well as the means of retrieving assignments that the students turn in. The students cannot see the personal folders of the other students.

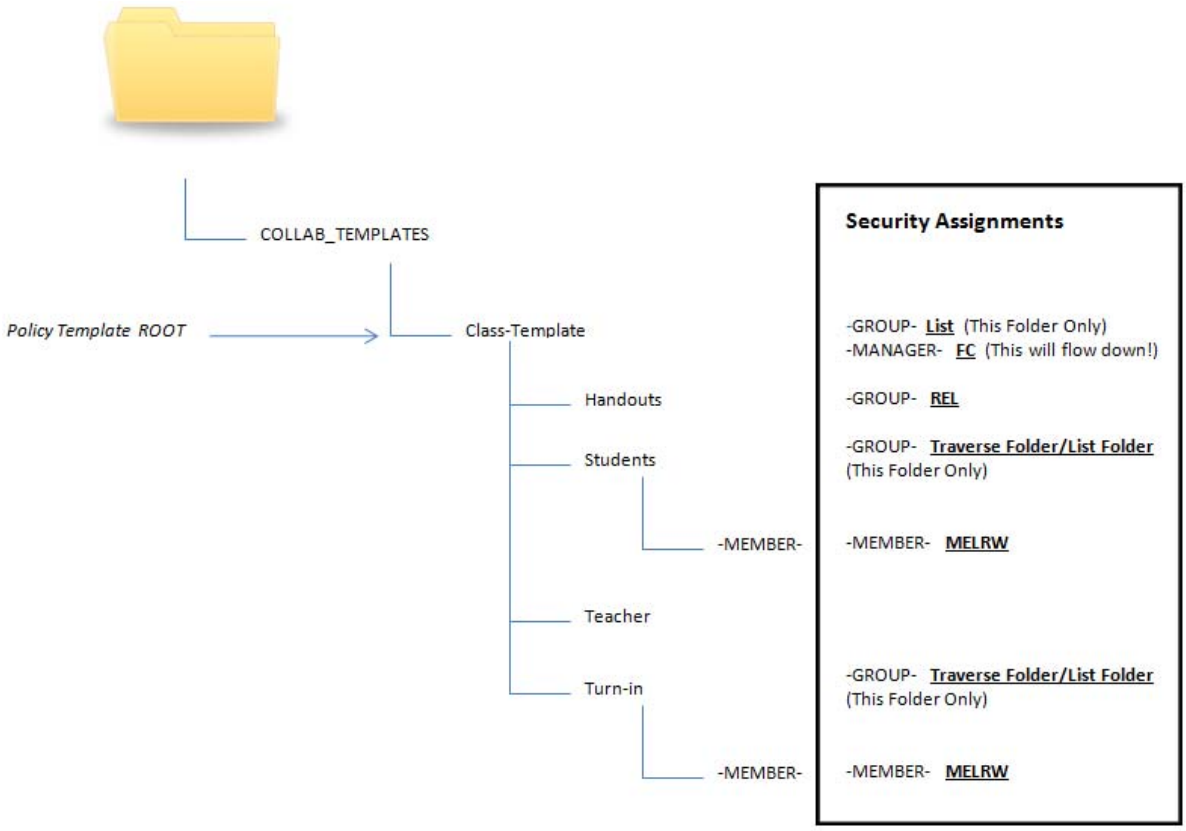
Figure 7-2 *Common Academic Setting Collaborative Storage Template Structure*



The file structure above is a common structure that can be used as a template for collaborative storage in an academic setting. By establishing the correct permissions, the course instructor can be established as the owner with full control of the collaborative storage area. Students can be provided with personal folders for retrieving and turning in assignments.

The diagram below shows the security permissions that must be established.

Figure 7-3 *Security Permissions for Each Folder in the Sample Template*

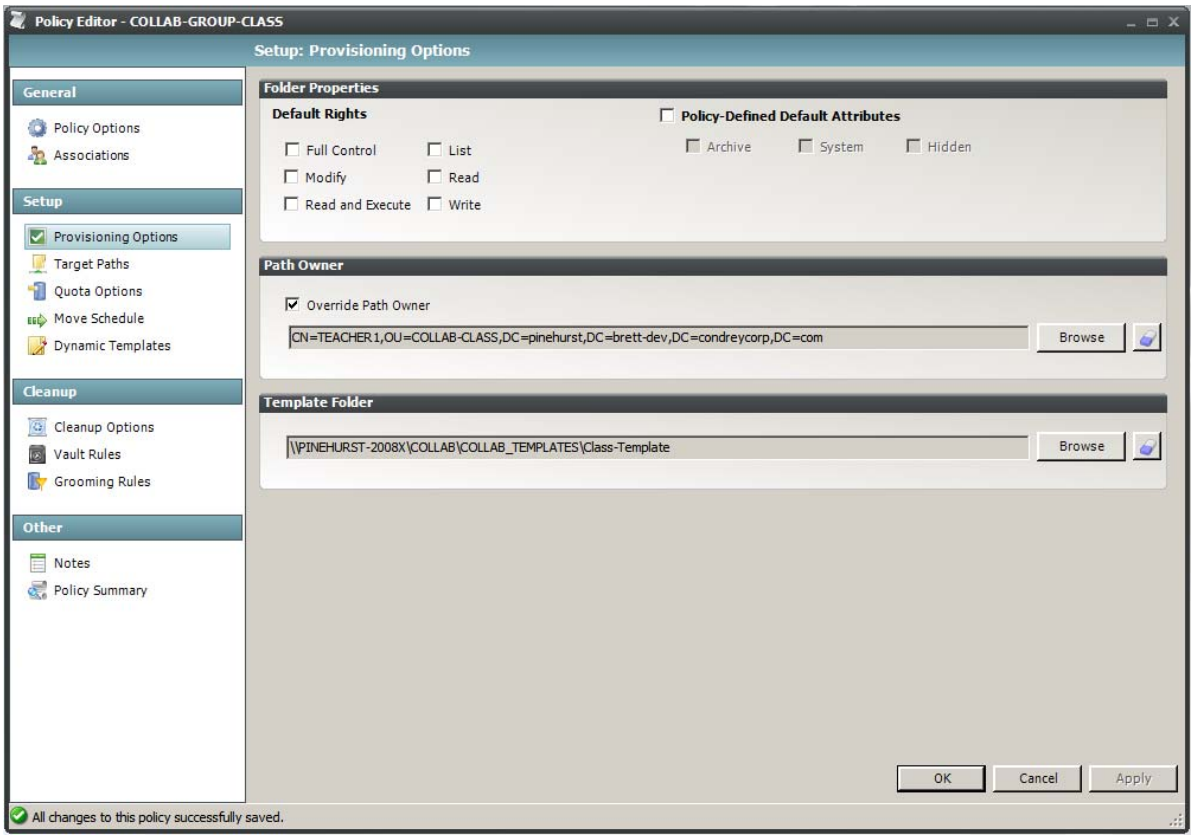


The diagram above shows the security permissions that must be established for each of the folders in the template structure. For example, the -GROUP- object must be given the List permission to the Class-Template folder and the -MANAGER- object must be given Full Control. List, Traverse Folder, and List Folder are all advanced permissions.

IMPORTANT: When you set the provisioning options for the collaborative storage policy, you must override the path owner and indicate an owner, unless you want all users in the group to have all rights to the collaborative storage area.

In the example in Figure 7-3, Teacher1 is specified as the owner.

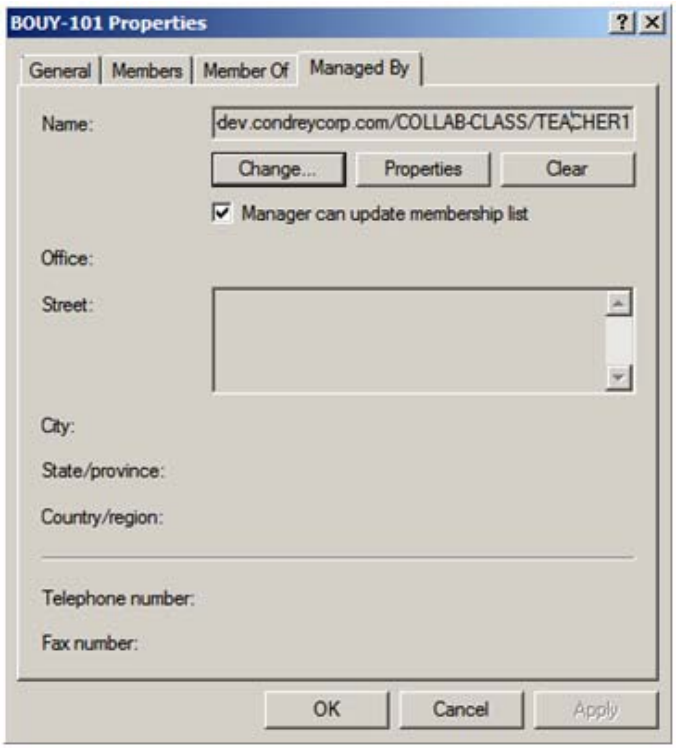
Figure 7-4 *Owner of a Collaborative Storage Folder*



The *Override Path Owner* check box is selected and the owner of the folder is set to TEACHER1. The template is indicated in the Template Folder region.

You use the Group properties of Active Directory Users and Computers to indicate the group owner in the Managed By screen. In this example, the owner is TEACHER1.

Figure 7-5 *An Owner in the Name Field Enables -MANAGER- to Function Properly*



7.5.1 Establishing Permissions

You establish the permissions specified for each of the folders in Figure 7-3 through the Windows Explorer *Security* tab. Permissions such as Traverse Folder are special permissions.

To set special permissions:

1. In Windows Explorer, right-click the desired folder and select *Properties*.
2. Click the *Security* tab.
3. Click *Advanced*.
4. Click *Change Permissions*.
5. Click *Add*.
6. In the *Enter the object name to select* field, specify the name of the desired user or group and click *OK*.
7. In the new dialog box, use the *Apply to* drop-down menu to select the desired application level, select the check boxes for all special permissions for the user or group, and click *OK*.

7.5.2 Configuring Rights for the Group Manager

This procedure grants Manager rights to the group's designated manager, meaning that he or she is given all rights needed to view and modify any document within the structure of the collaborative storage area.

1. Launch Windows Explorer.
2. In the file structure that you created earlier, browse to and right-click the topmost folder, then select *Properties*.

   For example, in the sample work project collaborative storage template example in Figure 7-1 on page 79, the topmost folder would be the Project folder.
3. Click the *Security* tab.
4. Click *Edit*.
5. Click *Add*.
6. In the *Enter the object names to select* field, specify `-MANAGER-`.
7. Click *Check Names*.
8. Click *OK*.
9. In the Permissions dialog box, select the *Modify* check box and click *OK* to save the settings.
10. Click *OK* to close the Properties dialog box.

7.5.3 Configuring Rights for the Group Members' Personal Folders

This procedure grants the rights needed for group members to work in their personal folders within the collaborative storage area.

1. Launch Windows Explorer.
2. In the structure that you created in Section 7.4, "Creating a Collaborative Storage Template," on page 79, browse to and right-click the -MEMBER- folder, then select *Properties*.
3. Click the *Security* tab.
4. Click *Edit*.
5. Click *Add*.
6. In the *Enter the object names to select* field, specify `-MEMBER-`.
7. Click *Check Names*.
8. Click *OK*.
9. In the Permissions dialog box, select the *Modify* check box and click *OK* to save the settings.
10. Click *OK* to close the Properties dialog box.

7.5.4 Configuring Group Member Rights to Other Folders

This procedure grants List and Read rights to other areas of the collaborative storage area.

1. Launch Windows Explorer.
2. In the structure that you created in Section 7.4, "Creating a Collaborative Storage Template," on page 79, browse to and right-click one of the subfolders, then click *Properties*.

   For example, in the sample work project collaborative storage template example in Figure 7-1 on page 79, a subfolder would be the Documents folder.

3 Click the *Security* tab.

4 Click *Edit*.

5 Click *Add*.

6 In the *Enter the object names to select* field, specify `-MEMBER-`.

7 Click *Check Names*.

8 Click *OK*.

9 Click *OK* to close the Properties dialog box.

10 Repeat Step 1 through Step 9 for each additional folder where you want to grant users List and Read rights.

7.6 Understanding Collaborative Storage Policies

Before setting up collaborative storage policies, you need to understand the two types of collaborative storage policies and the differences between the two.

- A Group collaborative storage policy is triggered when a new Group object is created in an organizational unit where the policy is associated. For example, if a cross-functional team named HEALTHFAIR2011 is created in an organizational unit associated with the Group collaborative storage policy, the collaborative storage area is be created when the group is created.
- A Container collaborative storage policy is triggered when a new User object is added to an organizational unit where the policy is associated. For example, if user BSMITH is added to an organizational unit that had an associated Container policy, BSMITH is granted access to the collaborative storage area. Furthermore, if the template associated with the policy is structured with a -MEMBER- Group object, the user is given a personal storage area within the collaborative storage area.

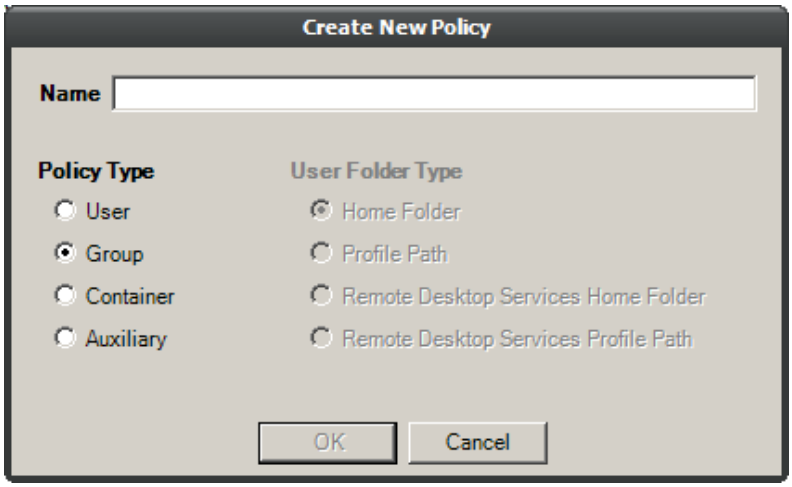
7.7 Creating a Group Collaborative Storage Policy

1 Launch NSMAdmin.

2 In the *Main* menu, click *Policy Management*.

3 In the *Manage Policies* menu, select *Create Policy* > *Create Group Policy*.

The following screen appears:



4 Specify a name in the *Name* field.

The Policy Options page appears.

5 Continue with Section 7.7.1, "Setting Group Policy Options," on page 86.

7.7.1 Setting Group Policy Options

Settings within Policy Options let you indicate how the policy is applied, set policy inheritance, and write an expanded policy description.

NOTE: Group policies in Novell Storage Manager are completely independent of Microsoft Group policies.

---

1 Leave the *Process Events for Associated Managed Storage* check box selected.

This indicates that you want the settings in this policy to be applied to all users within the Domain or Organizational Unit where this policy is assigned. Deselecting this check box indicates that you want to create a blocking policy that can be applied to a specific user or group. For more information on blocking policies, see Section 4.6, "Creating a Blocking Policy," on page 27.

2 Do one of the following:

- If you are assigning this policy to a container rather than a group, and you want the settings to apply to subcontainers, leave the *Policy applies to subcontainers* check box selected.
- If you are assigning this policy to a container, and you do not want the settings to apply to subcontainers, deselect the *Policy applies to subcontainers* check box.
- If you are assigning this policy to a group rather than a container, deselect the *Policy applies to subcontainers* check box.

3 In the Description region, use the text field to specify a description of the policy you are creating.

4 Click *OK* to save your settings.

5 Proceed with Section 7.7.2, "Setting Group Policy Associations," on page 86.

7.7.2 Setting Group Policy Associations

The Associations page is where you assign the collaborative policy you are creating to a domain, organizational unit, Group object, or (if you are creating a blocking policy) a User object.

1 In the left pane, click *Associations*.

2 Click the + button to bring up the Object Browser.

3 Browse through the directory structure and select the domain, organizational unit or Group object you want to associate the policy to.

4 Drag the object to the Selected Items pane and click *OK*.

The Object Browser is closed and the path is displayed in fully qualified name format in the right pane of the window. For example, OU=Las Vegas,DC=NVB,DC=local.

5 Click *OK* to close the Object Browser.

6 Click *Apply* to save your settings.

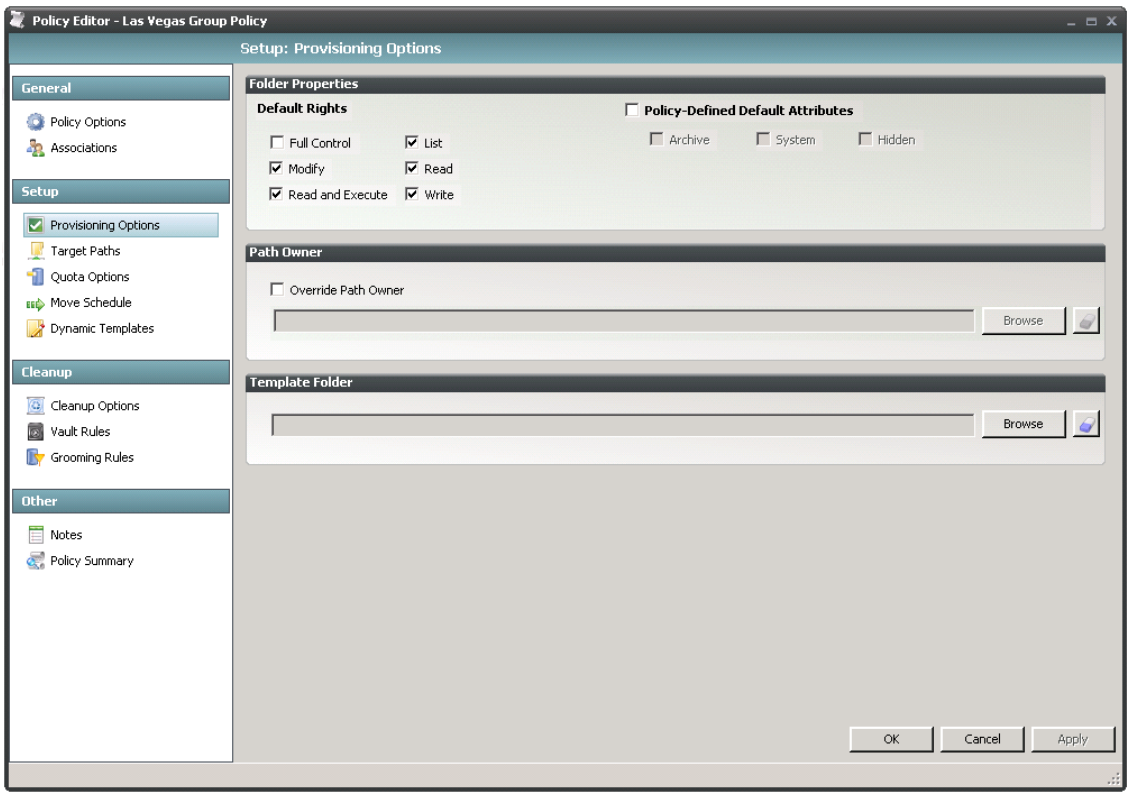
7 Proceed with Section 7.7.3, "Setting Group Policy Provisioning Options," on page 87.

7.7.3 Setting Group Policy Provisioning Options

The Provisioning Options page is where you indicate collaborative storage rights, the location of a template for provisioning the collaborative storage folder structure and content in a home folder when it is created, and more.

1 In the left pane, click *Provisioning Options*.

The following page appears:



2 In the Folder Properties region, deselect all rights.

If you chose to create a collaborative storage template, the rights will be applied from the template that you created earlier under Section 7.5.3, “Configuring Rights for the Group Members’ Personal Folders,” on page 84 and Section 7.5.4, “Configuring Group Member Rights to Other Folders,” on page 84.

3 Select the *Override Path Owner* check box.

When you create collaborative storage policies, it's very important to override the path owner. By default, each group owns the entire group home folder, so all members of the group inherit Full Control of all subdirectories in the group folder, including other users' personal folders.

4 In the field below the *Override Path Owner* check box, browse to indicate a path owner (that is, the owner of the group folder).

5 In the Template Folder region, click the *Browse* button and locate the file structure that you created in Section 7.4, “Creating a Collaborative Storage Template,” on page 79.

6 Select the topmost folder in the file structure and click *OK*.

For example, if you had a structure similar to the Sample Classroom Collaborative Storage Template in Figure 7-1 on page 79, you would select “8th Grade U.S. History.”

7 Click *Apply* to save your settings.

8 Proceed with Section 7.7.4, "Setting Group Policy Target Paths," on page 88.

7.7.4 Setting Group Policy Target Paths

The Target Paths page is where you set the paths to the shares where the collaborative storage area for this policy will be hosted.

1 In the left pane, click *Target Paths*.

2 In the Target Placement region, fill in the following fields:

Random: Distributes storage in an ordered sequence. For example, if you have two target paths listed on this page, Group A's collaborative storage folder is created using the first path, Group B's collaborative storage folder is created using the second path, and Group C's home collaborative storage folder is created using the first path.

Actual Free Space: Distributes the creation of collaborative storage folders according to shares with the largest amount of absolute free space. For example, if you have two target paths listed, target path 1 has 15 GB of free space, and target path 2 has 10 GB, the collaborative storage folders are created using target path 1.

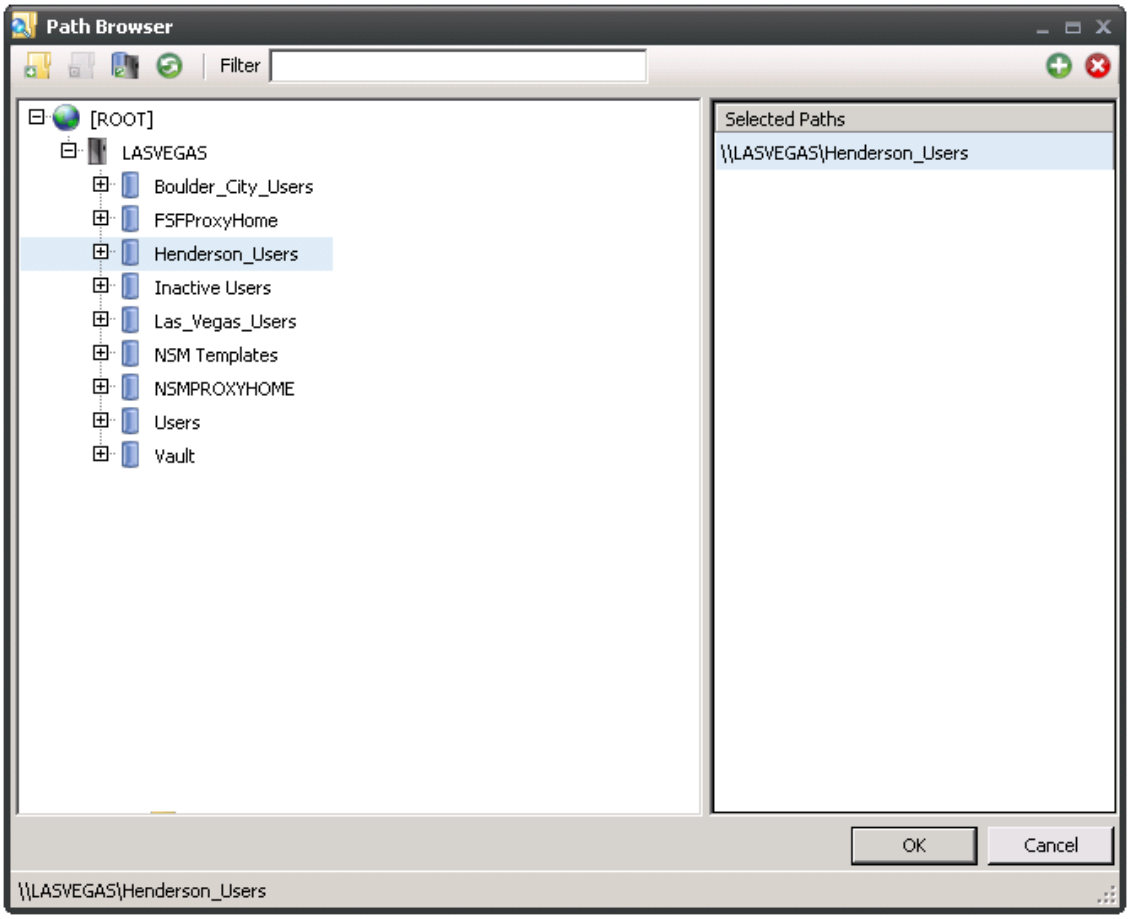
Percentage Free Space: Distributes the creation of collaborative storage folders to shares with the largest percentage of free space. For example, if you have two target paths listed and target path 1 is to a 10 TB drive that has 30 percent free space, and target path 2 is to a 500 GB drive with 40 percent free space, the collaborative storage folders are created using target path 2, even though target path 1 has more absolute available disk space. You should be cautious when using this option with target paths to shares of different sizes.

Leveling Algorithm: Use this option to structure the collaborative storage folders so that they are categorized by the Group object's first or last name through a subordinate folder. For example, if you choose *First Letter*, all collaborative storage folders are grouped by first name, with individual folders for each first letter.

Maximum Unreachable Paths: If you have a substantial number of target paths listed on this page, this field lets you indicate the number of target paths Novell Storage Manager accesses to attempt to create a collaborative storage folder before it suspends the attempt.

3 For each target path that you want to establish, click the + button to access the Path Browser.

4 Browse to the location of the target path you want and click the + button to add the target path to the Selected Paths pane.



5 Click *Apply* to save your settings.

6 Proceed to Section 7.7.5, "Setting Group Policy Quota Options," on page 89.

7.7.5 Setting Group Policy Quota Options

This page lets you establish storage quota for the collaborative storage folder. Until quota management is enabled, a collaborative storage area has unlimited storage. Quota management for collaborative storage applies to:

- The quota for the entire storage folder
- Quotas for personal folders in the collaborative storage folder

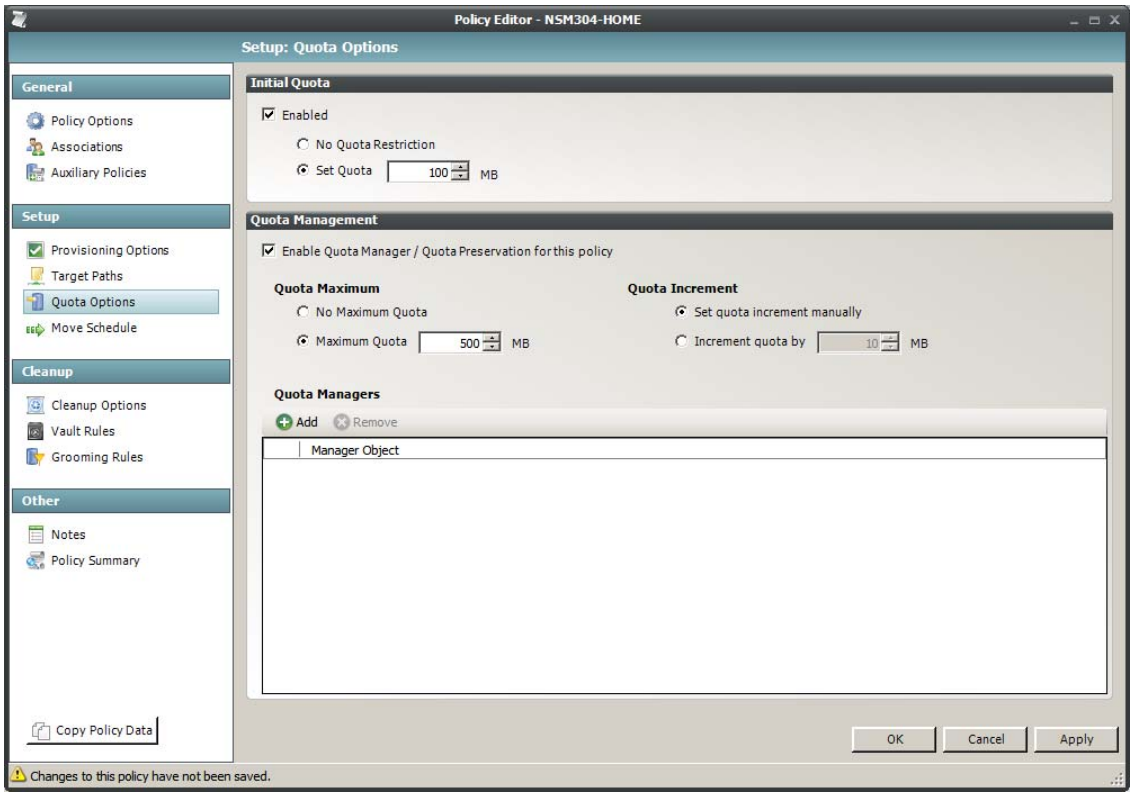
---

NOTE: In order for the quota to be managed on a personal folder, you must also manage the quota on the -MANAGER- or -MEMBER- folder. You can set this in the template through the Windows Server Manager in the same way you set the folder options.

The Quota Options page is also where you establish quota management settings for quota managers. A quota manager is a specified user or group—for example, a help desk administrator or technical support rep, who is granted the ability to increase quotas without having rights to the file system. Quota management actions are performed through Quota Manager, which is a separate Web browser-based management interface. For more information on Quota Manager, see Chapter 8, "Using Quota Manager," on page 97.

1 In the left pane, click *Quota Options*.

The following page appears:



2 Select the *Enabled* check box to enable an initial storage quota for the group to whom this policy will apply.

3 In the *MB* field, specify the initial storage quota for the collaborative storage folders.

4 Set up quota managers and enable the Quota Manager Web interface for this policy by filling in the following fields:

Enable Quota Manager / Quota Preservation for this Policy: Select this check box to enable the Quota Management region of the page.

Quota Maximum: Indicate whether the folders associated with this policy will have a maximum quota setting. If so, indicate the maximum quota.

Quota Increment: Indicate whether quota managers will set quotas manually or in set increments. If you select manual increments, the quota manager can increase the quota in any increment until it meets the maximum quota setting. If you select set increments, the quota manager can only increase the quota by the increment setting.

Quota Managers: Click the + button and use the Object Browser to browse to and select a user or group you want to be a quota manager, then drag the User or Group object to the right pane. Repeat this for each user or group you want to be a quota manager.

If you do not specify a user or group as a quota manager, only members of the NSMAdmins group will be able to use the Quota Manager Web interface.

5 Click *Apply* to save your settings.

6 Proceed with Section 7.7.6, “Setting the Group Policy Move Schedule,” on page 91.

7.7.6 Setting the Group Policy Move Schedule

This page lets you use a grid to specify when collaborative storage data can be moved during data migration operations.

By default, all days and times are available for data movement. You might decide that data movement during regular business hours creates unacceptable network performance, and choose to move data after regular business hours.

NOTE: The collaborative storage folder will not move if someone is accessing the folder or there are any open files. Until the folder can be moved, the Move event will be listed as a pending event.

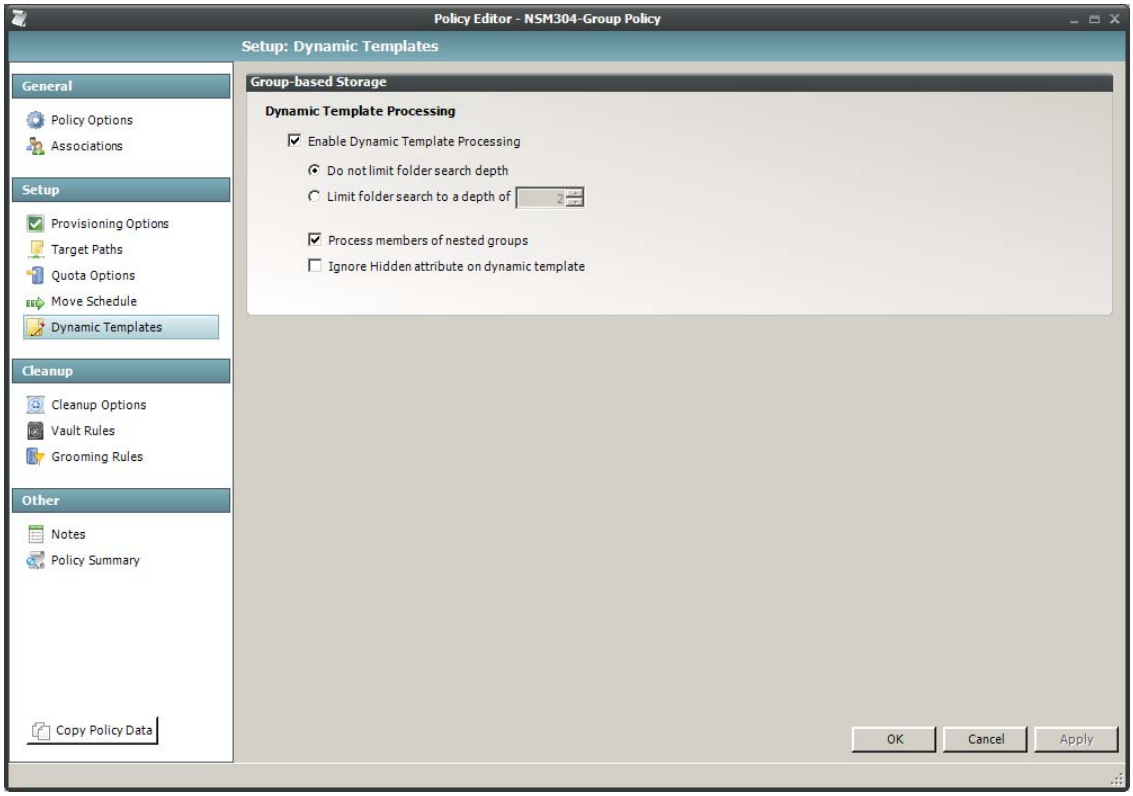
1. In the left pane, click *Move Schedule*.
2. In the Data Move Schedule grid, click the squares for the day and hour you want to disable for data movement.
3. Click *Apply* to save your settings.
4. Proceed with Section 7.7.7, "Setting Group Policy Dynamic Template Processing," on page 91.

7.7.7 Setting Group Policy Dynamic Template Processing

Dynamic Template Processing is the term used in Novell Storage Manager for creating personal folders in a collaborative storage folder. If Dynamic Template Processing is enabled, creating a -MEMBER- Group object in the collaborative storage file structure automates the creation of a new user's personal folder when he or she is added to the group.

1. In the left pane, click *Dynamic File Processing*.

   The following screen appears:



2 Do one of the following:

- If the file structure in your collaborative storage template includes a -MEMBER- folder, Novell Storage Manager automatically creates personal folders within the collaborative storage folder. Leave the *Enable Dynamic Template Processing* check box selected and proceed with Step 3.
- If your collaborative storage template does not include a -MEMBER- folder, Novell Storage Manager does not create personal folders within the collaborative storage folder. Deselect the *Enable Dynamic Template Processing* check box and proceed with Section 7.7.8, "Setting Group Policy Cleanup Options," on page 92.

3 Choose one of the following options:

- **Do not limit folder search depth:** The NSM Engine searches through the collaborative storage folder looking for -GROUP-, -MANAGER-, and -MEMBER- folders. Depending on the number of folders in the collaborative storage folder, this can take significant time. It is therefore best to not select this option.
- **Limit folder search to a depth of:** If you know the level where the -MEMBER- folder is structured in your collaborative storage template, you can select this option and indicate the level.

  For example, in the Sample Classroom Collaborative Storage Template in Figure 7-1 on page 79, the -MEMBER- folder is located four levels down.

4 Select the applicable check boxes:

Process members of nested groups: If you have nested groups in your Active Directory deployment, selecting this check box creates personal storage for group members that are part of a group via group nesting.

Ignore hidden attribute on dynamic template: Selecting this check box ignores the HIDDEN flag on the -MEMBER, -MANAGER-, and –GROUP- folders in the collaborative home folder when provisioning the corresponding folder for the user or group.

5 Click *Apply* to save your settings.

6 Proceed with Section 7.7.8, "Setting Group Policy Cleanup Options," on page 92.

7.7.8 Setting Group Policy Cleanup Options

This page lets you enable and specify cleanup rules for the Group policy. Options for cleanup include deleting a collaborative storage folder after a set number of days following the removal of the associated Group object from Active Directory, or vaulting (rather than deleting) the collaborative storage folder.

1 In the left pane, click *Cleanup Options.*

2 Enable storage cleanup by filling in the following fields:

Enable: Select this check box to enable storage cleanup rules.

Cleanup storage: Specify the number of days a collaborative storage folder remains after the associated Group object is removed from Active Directory.

3 Enable vaulting on cleanup by filling in the following fields:

Enable: Select this check box to enable vaulting on cleanup rules.

Vault Path: Click *Browse* to browse and select the share where you want the collaborative storage folders vaulted after cleanup.

When you indicate this path, it also appears in the *Vault Path* field of the Grooming Rules page, because grooming rules and vault on cleanup rules share the same vault path.

4 Click *Apply* to save the settings.

5 Proceed with Section 7.7.9, "Setting Group Policy Vault Rules," on page 93.

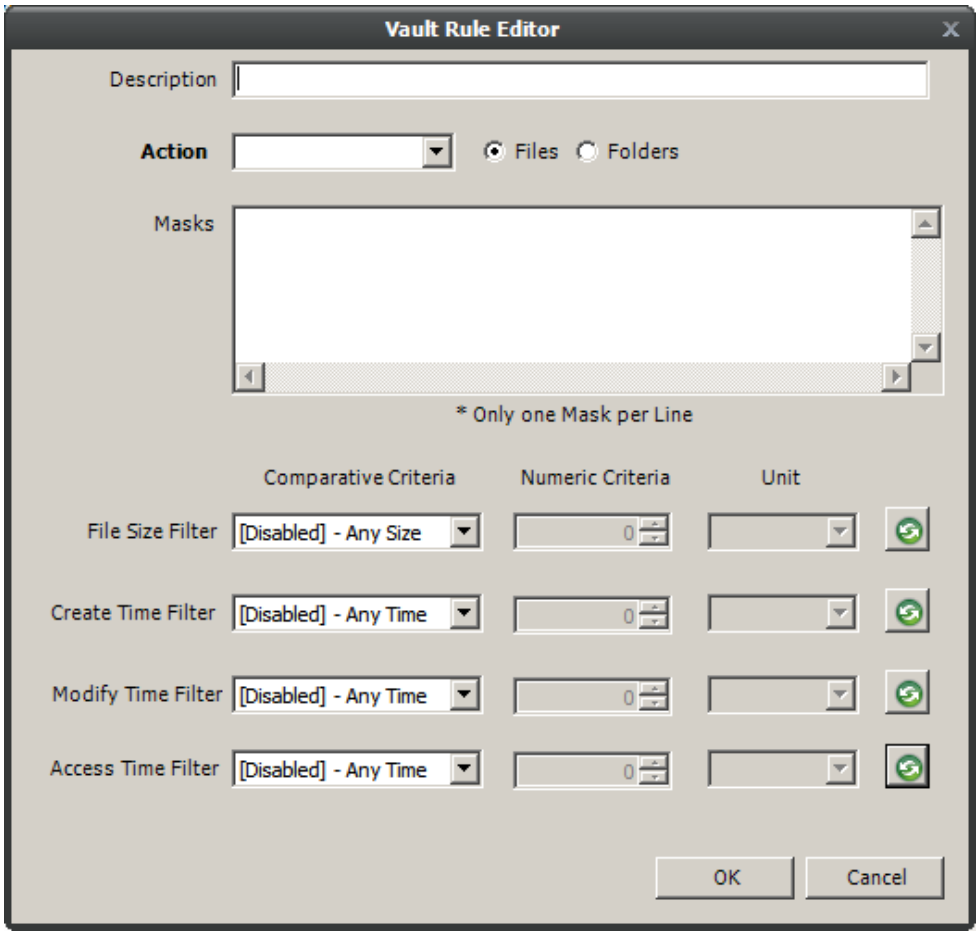
7.7.9 Setting Group Policy Vault Rules

When a Group object is removed from Active Directory, you can have Novell Storage Manager vault the contents of the associated collaborative storage folder from a primary storage device to a less expensive secondary storage device. Novell Storage Manager lets you specify what to vault or delete by using vault rules. For example, you might want to remove all TMP files before vaulting the collaborative storage folder. Or, you might want to vault only a single folder, such as Final Proposal and nothing else in the other folders. You accomplish all of this through settings in the Vault Rules Editor.

1 In the left pane, click *Vault Rules*.

The *Vault Path* field displays the vault path that you established when you set up collaborative storage cleanup rules.

2 Click the + button to bring up the Vault Rules Editor.



3 In the *Description* field, specify a description of the vault rule.

For example, "Files to delete before vaulting," or "Files to vault."

4 Fill in the following fields:

Action: Select whether this vault rule deletes or vaults.

Be aware that if you select *Vault*, only the files or folders that you list in the *Masks* text box are vaulted and the remainder of the home folder content is deleted. Conversely, if you select *Delete*, only the files or folders that you list in the *Masks* text box are deleted, and everything else is vaulted.

Files: If the vault rule you are creating will vault or delete content at the file level, leave the *File* option selected.

Folders: If the vault rule you are creating will vault or delete content at the folder level, select the *Folders* option.

Selecting *Folders* disables the filter settings in the lower portion of the Vault Rules Editor.

Masks: List the files or folders you want to be vaulted or deleted, according to what is indicated in the *Action* drop-down menu.

File or folder names can contain an asterisk.

5 (Conditional) If the vault rule you are creating is specific to files, complete the applicable filter settings.

Leaving the setting as *[Disabled]-Any Size* vaults or deletes all file types listed in the *Mask* text box, according to what is indicated in the *Action* drop-down menu. Choosing any of the other options from the drop-down menu lets you indicate files to delete or vault according to size, when created, when last modified, and when last accessed.

6 Click *OK* to save the vault rule.

7 If necessary, create any needed additional vault rules by repeating the procedures above.

8 Proceed with Section 7.7.10, “Setting Group Policy Grooming Rules,” on page 94.

7.7.10 Setting Group Policy Grooming Rules

Grooming rules in Novell Storage Manager specify the file types that you do not want network users storing in their home folders or collaborative storage areas. Examples of these might be MP3 and MP4 files, MOV files, and many others. You use the Grooming rule to specify whether to delete or vault a groomed file.

Grooming takes place as a Management Action that is run by the administrator. A Management Action is a manual action that is enacted through NSMAdmin. For more information, see Section 12.1.4, “Management Actions,” on page 209.

1 In the left pane, click *Grooming Rules*.

The *Vault Path* field displays the vault path that you established when you set up cleanup rules.

2 Click the + button to bring up the Grooming Rules Editor.

3 In the *Description* field, specify a description of the grooming rule.

For example, “Files to groom in Community Outreach Group.”

4 Fill in the following fields:

Action: Select whether this grooming rule will delete or vault groomed files.

Files: If the grooming rule you are creating will vault or delete content at the file level, leave the *File* option selected.

Folders: If the grooming rule you are creating will vault or delete content at the folder level, select the *Folders* option.

Selecting Folders disables the filter settings in the lower portion of the Grooming Rules Editor.

Masks: List the files or folders you want to be vaulted or deleted, according to what is indicated in the *Action* drop-down menu.

File or folder names can contain an asterisk.

5 (Conditional) If the grooming rule you are creating is specific to files, complete the applicable filter settings.

Leaving the setting as *[Disabled]-Any Size* vaults or deletes all file types listed in the *Mask* text box, according to what is indicated in the *Action* drop-down menu. Choosing any of the other options from the drop-down menu lets you indicate files to delete or vault according to size, when created, when last modified, and when last accessed.

6 Click *Apply* to save the grooming rule.

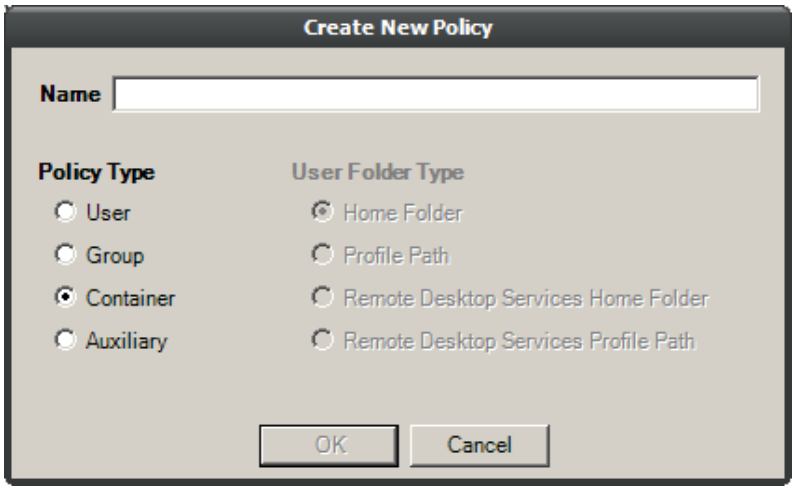
7.8 Creating a Container Collaborative Storage Policy

1 In NSMAdmin, click the *Main* tab.

2 Click *Policy Management*.

3 In the *Manage Policies* menu, select *Create Policy* > *Create Container Policy*.

The following screen appears:



4 Specify a name in the *Name* field.

The Policy Options page appears.

5 Continue with Section 7.8.1, "Setting Container Policy Options," on page 95.

7.8.1 Setting Container Policy Options

Settings within Policy Options let you indicate how the policy is applied and lets you write an expanded policy description.

1 Leave the *Process Events for Associated Managed Storage* check box selected.

This indicates that you want the settings in this policy to be applied to all users within the domain or organizational unit where this policy is assigned. Deselecting this check box indicates that you want to create a blocking policy that can be applied to a specific user or group. For more information on blocking policies, see Section 4.6, "Creating a Blocking Policy," on page 27.

2 In the Description region, specify a description of the policy you are creating in the text field.

3 Click *Apply* to save your settings.

4 Select the options and setting that you want to policy to use:

Container Policy Associations: The Associations page is identical to the Association page presented when you create a Group policy. For an explanation of the page, along with procedures for setting associations, see Section 7.7.2, "Setting Group Policy Associations," on page 86.

Container Policy Provisioning Options: The fields presented on the Provisioning Options page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting provisioning options, see Section 7.7.3, "Setting Group Policy Provisioning Options," on page 87.

Container Policy Target Paths: The fields presented on the Target Paths page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting target paths, see Section 7.7.4, "Setting Group Policy Target Paths," on page 88.

Container Policy Quota Options: The fields presented on the Quota Options page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting quota options, see Section 7.7.5, "Setting Group Policy Quota Options," on page 89.

Container Policy Move Schedule: The fields presented in the Move Schedule page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 7.7.6, "Setting the Group Policy Move Schedule," on page 91.

Container Policy Dynamic Template Processing: The fields presented on the Dynamic Templates page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting the move schedule, see Section 7.7.7, "Setting Group Policy Dynamic Template Processing," on page 91.

Container Policy Cleanup Options: The fields presented on the Cleanup Options page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting cleanup options, see Section 7.7.8, "Setting Group Policy Cleanup Options," on page 92.

Container Policy Vault Rules: The fields presented on the Vault Rules page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting vault rules, see Section 7.7.9, "Setting Group Policy Vault Rules," on page 93.

Container Policy Grooming Rules: The fields presented on the Grooming Rules page are identical to those presented when you create a Group policy. For an explanation of the page, along with procedures for setting grooming rules, see Section 7.7.10, "Setting Group Policy Grooming Rules," on page 94.

5 Click *Apply* to save your settings.

8 Using Quota Manager

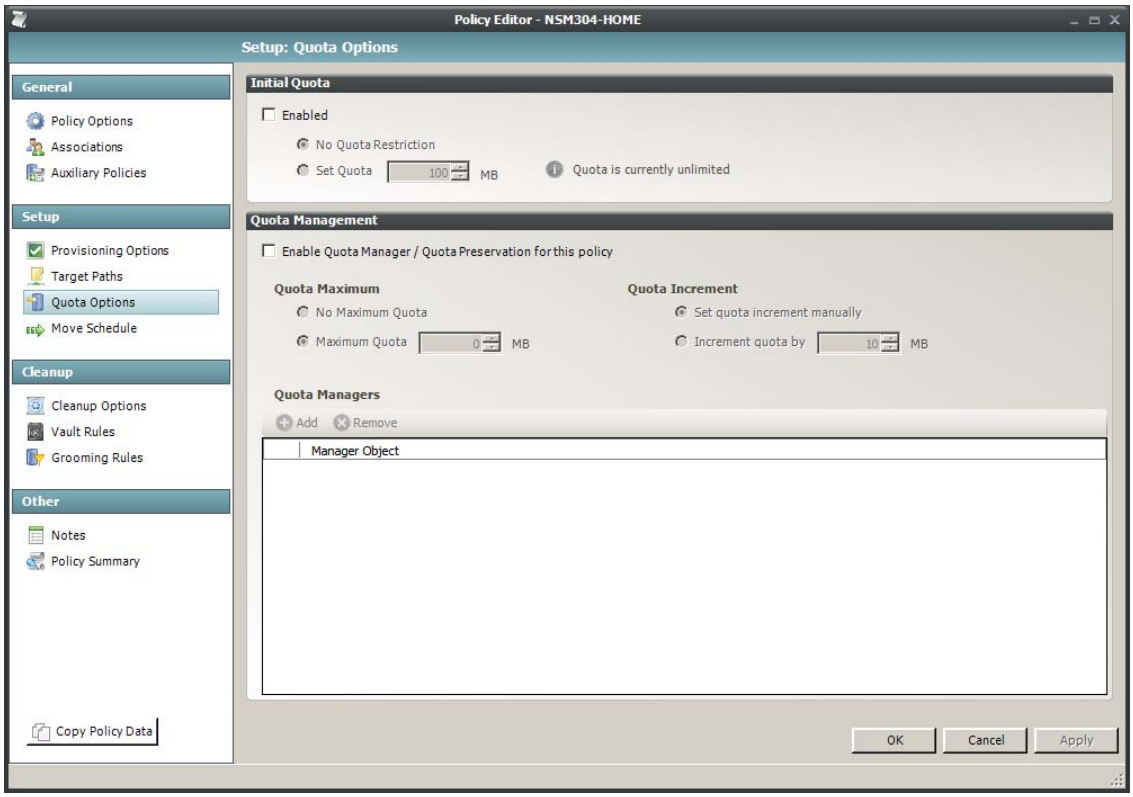
Quota Manager is a separate management interface for designated users such as help desk administrators or support personnel, to adjust user home folder or collaborative storage quota without needing rights to the file system.

Quota Manager can also provide storage information such as the total number of files and file types in a home folder. With this type of information, the help desk or support rep can make suggestions for freeing up space in the home folder rather than simply granting additional storage quota.

- Section 8.1, “Quota Management Prerequisites,” on page 97
- Section 8.2, “Managing Quotas Through Quota Manager,” on page 98
- Section 8.3, “Understanding Quota Manager Status Indicators,” on page 100

8.1 Quota Management Prerequisites

1 Using NSMAdmin, verify that all of the policies managing the users for whom you want to manage quotas through Quota Manager have the *Enable Quota Manager* check box selected, with a Quota Maximum and/or Quota Increment setting.



2 Verify that you have users or groups listed in the list box in the Quota Managers region of the page.

8.2 Managing Quotas Through Quota Manager

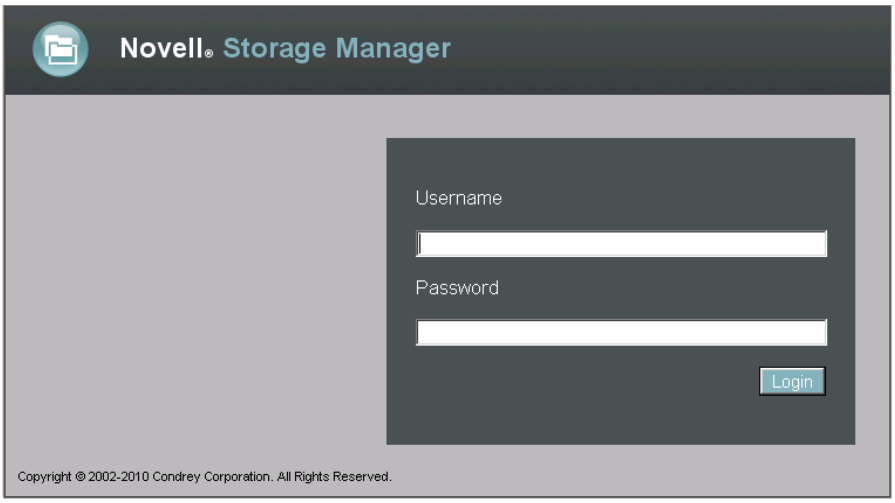
IMPORTANT: You can run Quota Manager from most modern Web browsers when JavaScript is enabled. To run it from Internet Explorer, you must enable META REFRESH. Workstation deployments of Internet Explorer come with META REFRESH enabled. If META REFRESH has been disabled, you need to enable it before proceeding.

1 Launch a Web browser.

2 Enter the following address: https://*ip-address-or-dns-name-of-nms-engine-server*:3009/qm

3 (Conditional) If a message appears informing you that the connection is not trusted, proceed by adding the security exception and downloading the certificate.

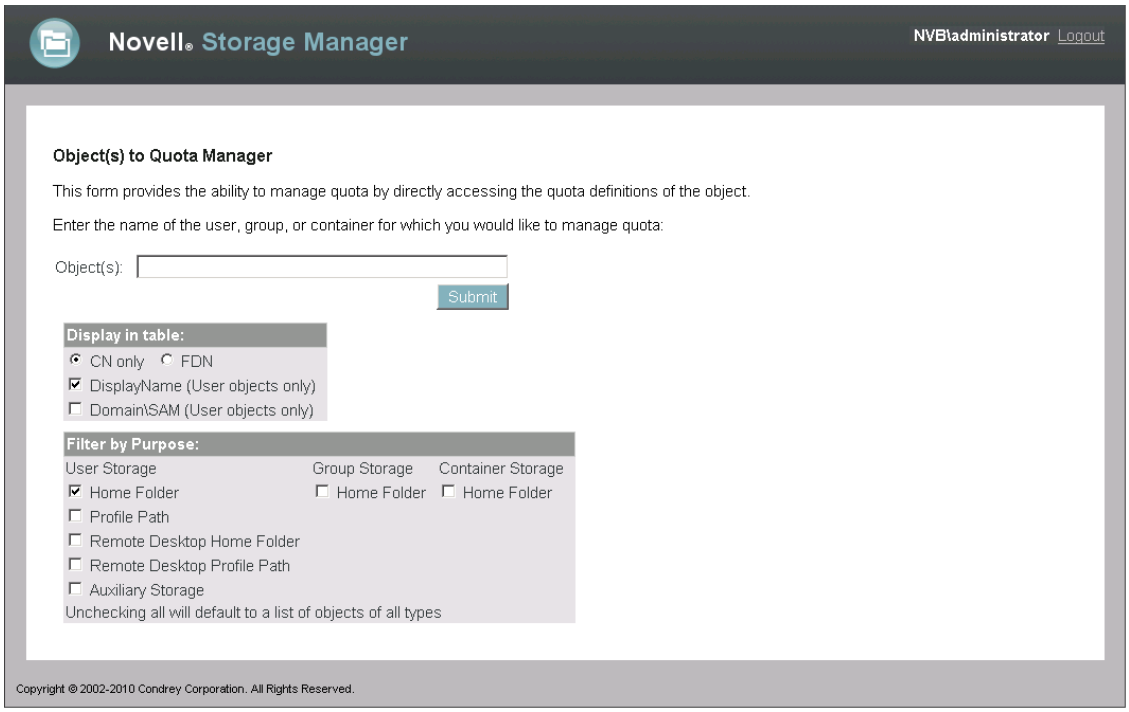
The following screen appears:



4 Enter a username and password and click *Login*.

The username and password must correspond to a user that has been designated as a quota manager either directly or through a group association.

The username must be in SAM account format such as *domain\user* or *user@full.domain.com*.

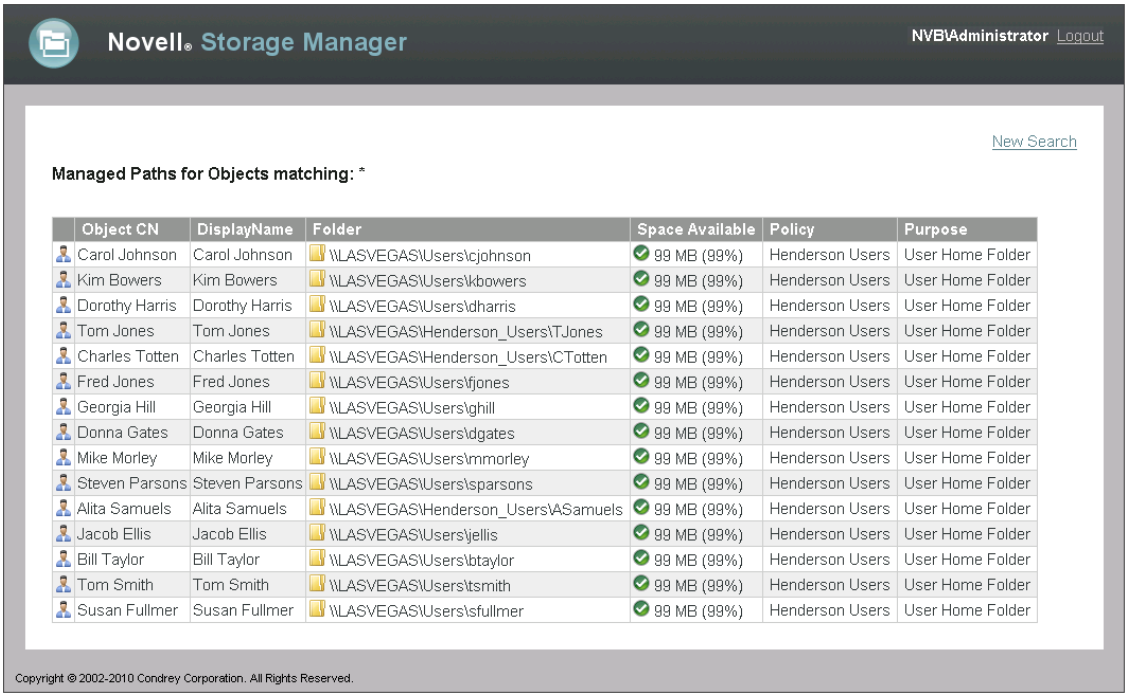


5 In the *Object(s)* field, specify a user, group, or container name, or use an asterisk (*).

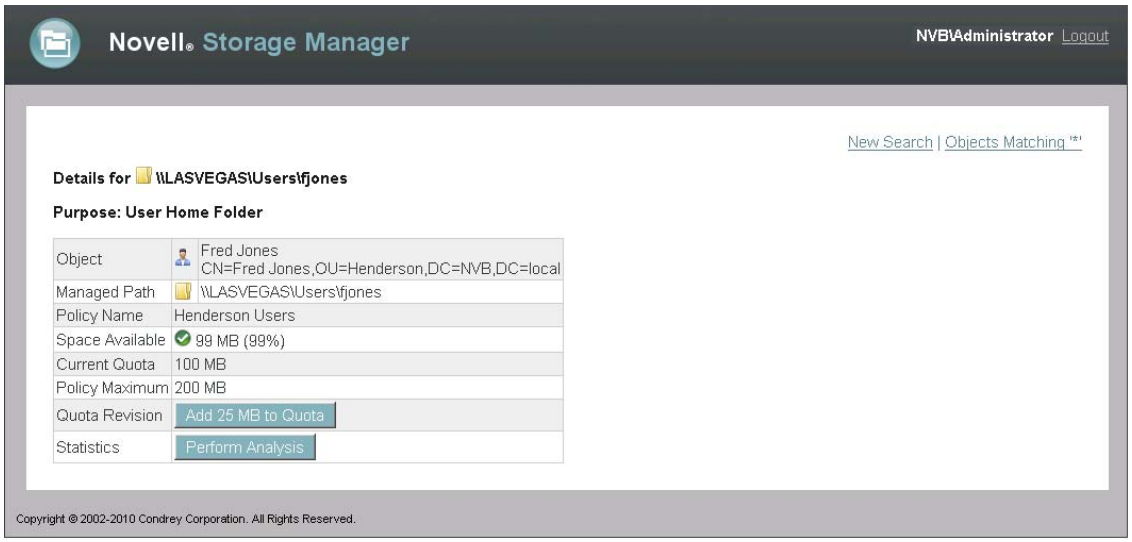
In large networks, building a list through the asterisk can be time consuming.

6 Specify your display and filter preferences in the corresponding regions.

7 Click *Submit*.



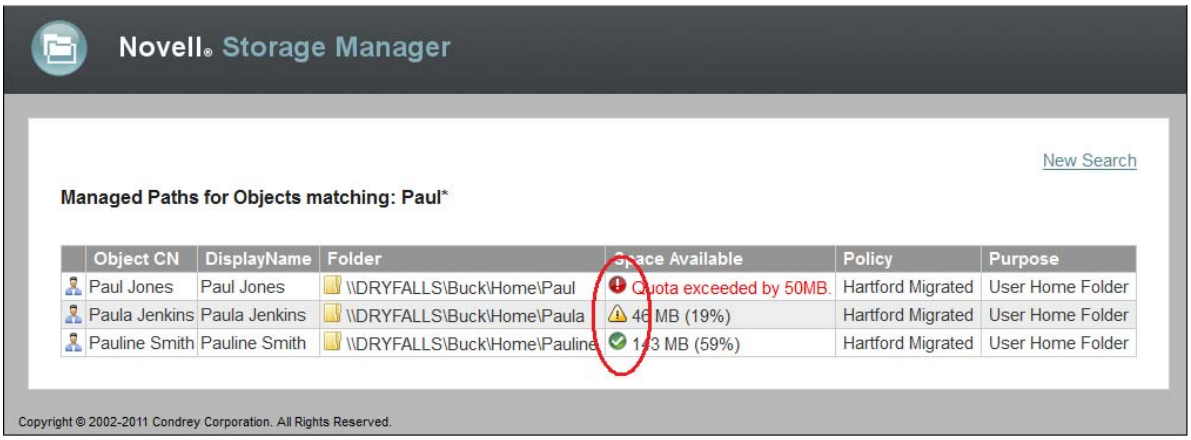
8 Click the user, group, or container you want to manage.



9 Add or remove a quota or perform a storage analysis by using the buttons provided.

8.3 Understanding Quota Manager Status Indicators

Quota Manager uses three different status indicators to show the current storage quota status for a user home folder or collaborative storage folder.



Red: Denotes one of the following conditions:

- Quota usage has exceeded 90 percent.
- The NSM Engine is unable to contact the server containing the share.
- The share does not support quota management.
- The home folder does not exist.
- The server containing the share gave an Access Denied error, indicating that either remote storage management is not configured or enabled for the NSM Engine, or that the firewall disallows remote storage management.

Yellow: Denotes that the quota usage has exceeded 75 percent.

Green: Denotes that quota usage is under 75 percent and that there are none of the problems specified above.

9 Mobile Management

As part of the release of Novell Storage Manager 3.1, Novell has introduced a new Novell Storage Manager mobile app.

Figure 9-1 *Login Screen*

The mobile app is available for download for iOS and Android devices from the Apple AppStore and Google Play respectively.

Figure 9-2 *Engine Status Screen*

An intuitive user interface allows administrators to remotely monitor NSM Agent and Event Monitor connectivity, monitor the pending event queue, change event and processing settings, view reports, and much more.

The Novell Storage Manager mobile app continues to be updated with new features and performance enhancements, so be sure to take advantage of these by keeping your app up-to-date.

10 The Network Operations Center Dashboard

The Network Operations Center Dashboard monitors and displays Novell Storage Manager activity. Its multiple monitoring regions help you to track Novell Storage Manager activity, performance, and potential problems.

- Section 10.1, “Prerequisites,” on page 105
- Section 10.2, “Installing and Configuring the Network Operations Center Dashboard,” on page 105
- Section 10.3, “Using the Network Operations Center Dashboard,” on page 108

10.1 Prerequisites

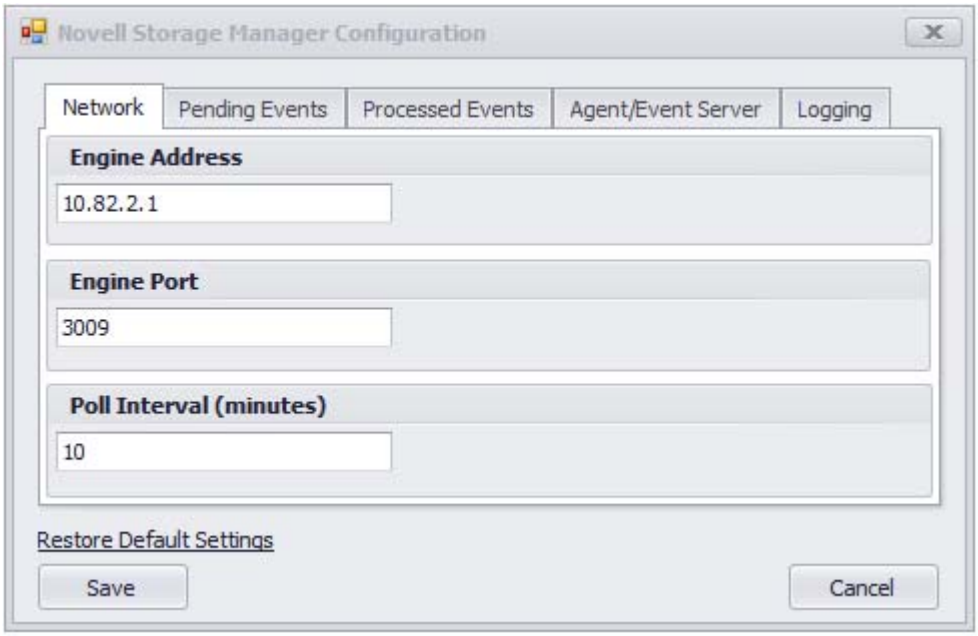
The Network Operations Center Dashboard requires the .NET 4 (Full) Framework installed on the server where it will be run.

10.2 Installing and Configuring the Network Operations Center Dashboard

Perform the following procedures on each computer where you want to run the dashboard.

1. From the Novell Storage Manager 3.1.1 ISO image, copy the `Utilities\Dashboard\NSMDashboard.zip` file to the computer.
2. Unzip the `NSMDashboard.zip` file.
3. Launch the `NSMDashboard.exe` file.

   The configuration screen appears.



Engine Address: The IP address of the server hosting the NSM Engine.

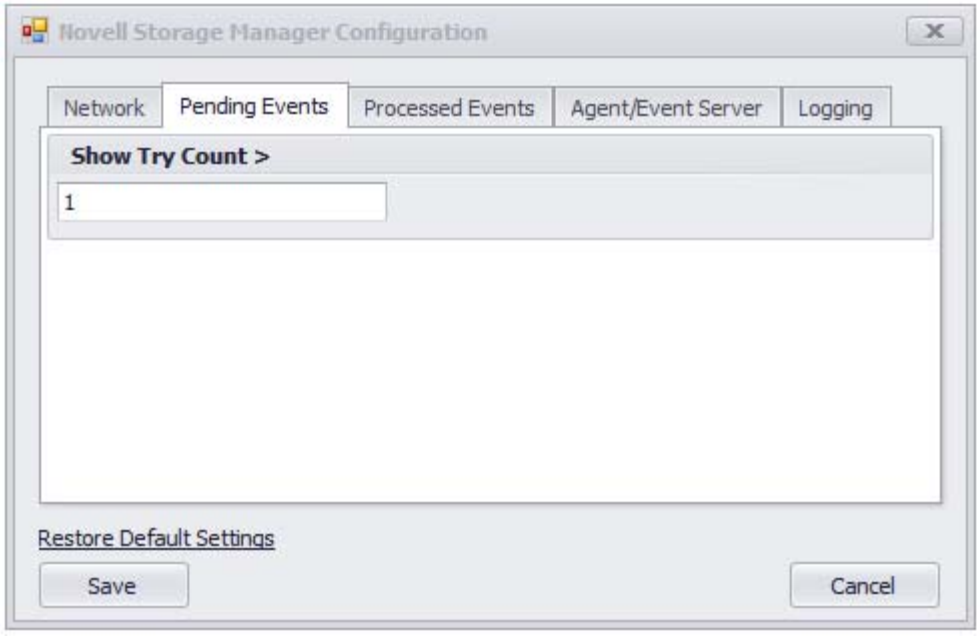
Engine Port: The port number used by Novell Storage Manager.

The default port number for Novell Storage Manager is 3009.

Poll Interval (minutes): The number of minutes before an update.

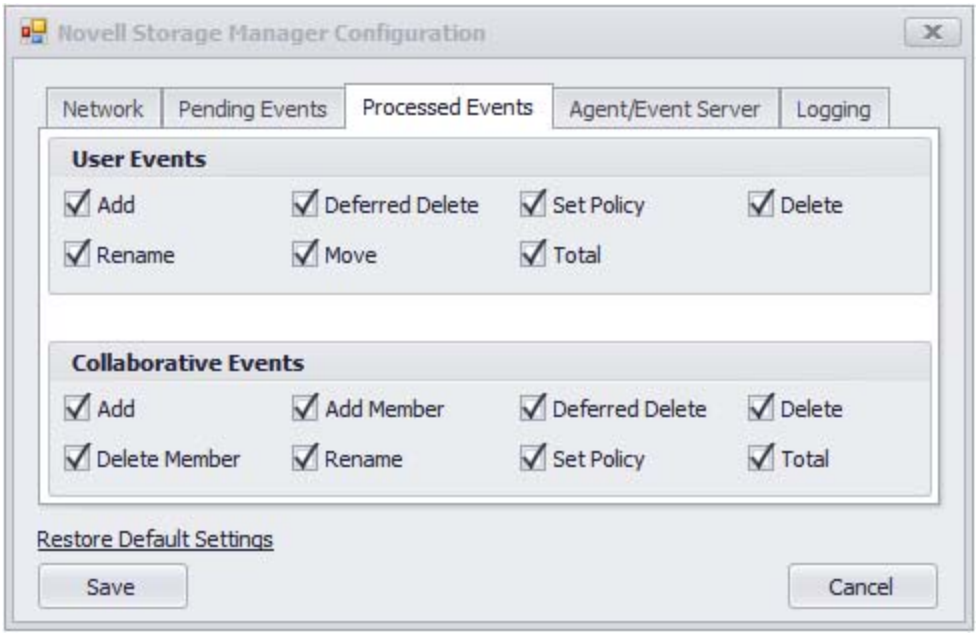
Because each update utilizes the database, it can affect Novell Storage Manager performance. We recommend using a higher number of minutes.

4 Specify your settings and click *Pending Events*.



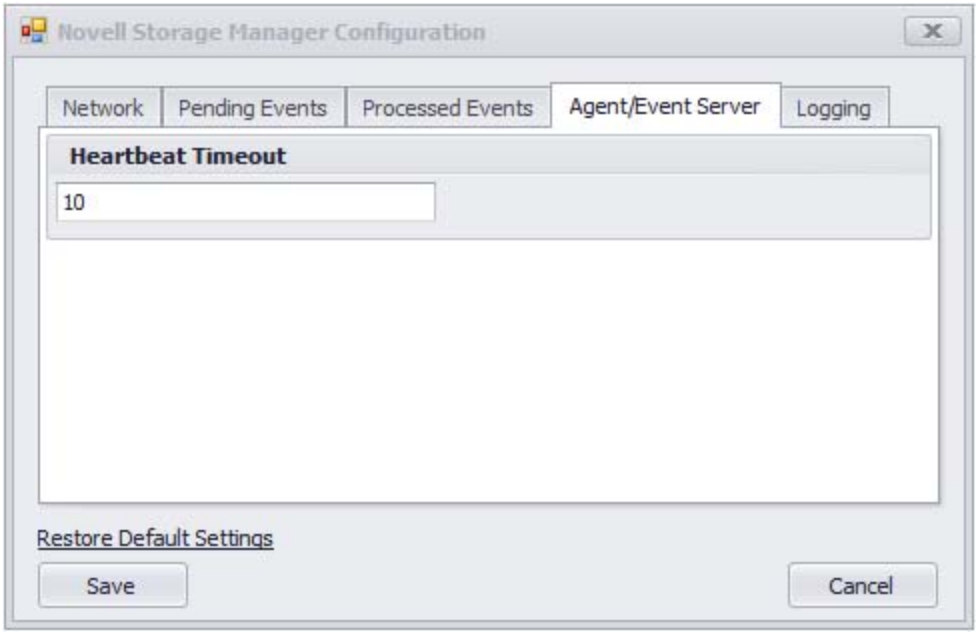
The dashboard displays the number of pending events with try counts greater than the number in the *Show Try Count* > field.

5 Specify your preferred number and click *Processed Events*.



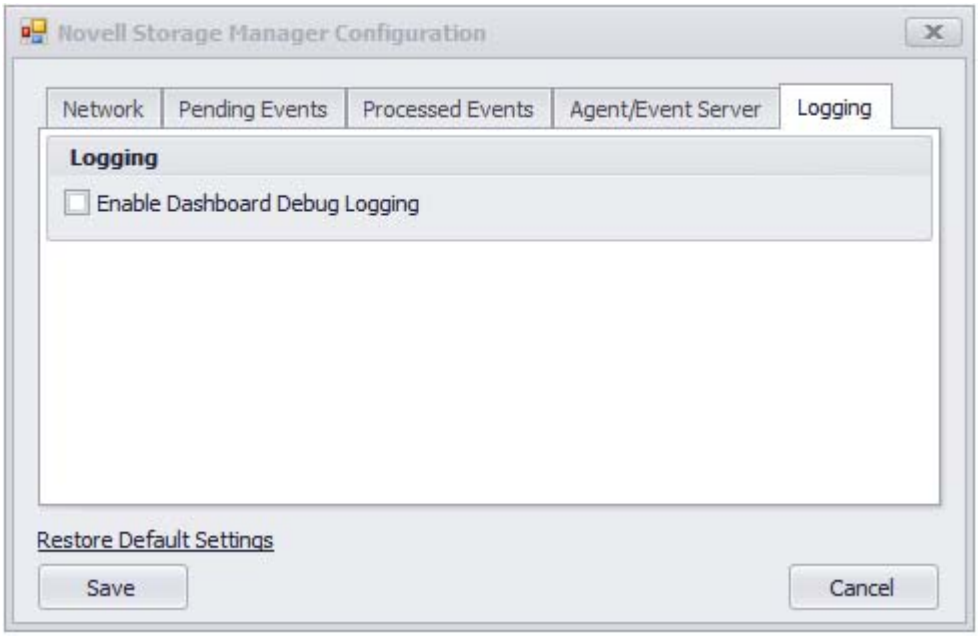
The information displayed on the dashboard depends on events that are being processed. You specify which events to process in this page.

6 Specify which events to process and click *Agent/Event Server*.



The dashboard displays NSM Agents and Event Monitors that have not generated a heartbeat after the number of minutes set in the *Heartbeat Timeout* field.

7 Set the heartbeat timeout number and click *Logging*.



Because logging can quickly fill up disk space, this option is turned off. During a call with a Novell Support representative, you might be asked to turn this on.

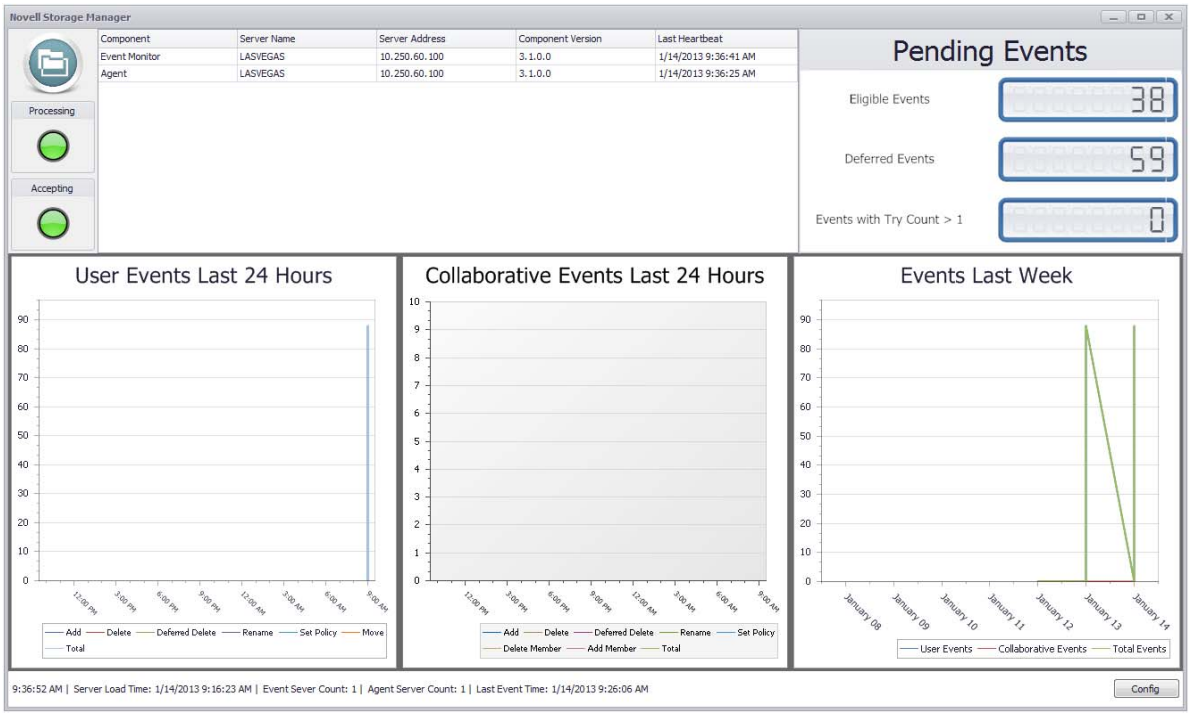
8 Click *Save* to save the configuration settings.

If you want to change the configuration settings, you can do so by clicking the *Config* button.

10.3 Using the Network Operations Center Dashboard

The Network Operations Center Dashboard presents the following information:

Figure 10-1 *The Network Operations Center Dashboard*



Processing: Displays a green light if the NSM Engine is processing events. A red light indicates that the NSM Engine is not processing events.

Accepting: Displays a green light if the NSM Engine is accepting events from the Event Monitor. A red light indicates the NSM Engine is not accepting events for processing.

Components: Displays all Event Monitors and NSM Agents and relevant data for each.

Pending Events: Displays the eligible events, deferred events, and the number of events that are greater than the try count setting you established in Step 5 on page 107.

User Events Last 24 Hours: Graphs the user storage events that have taken place in the last 24 hours. Each user event is graphed with a different colored line. You can mouse over a given hour on the graph to see how many events in each category took place at that hour.

Collaborative Events Last 24 Hours: Graphs the collaborative storage events that have taken place in the last 24 hours. Each collaborative event is graphed with a different colored line. You can mouse over a given hour on the graph to see how many events in each category took place at that hour.

Events Last Week: Graphs the total number of user storage and collaborative storage events that have taken place in the last 24 hours. Each category is graphed with a different colored line. You can mouse over a given hour on the graph to see how many events in each category took place at that hour.

11 Performing a Cross-Empire Data Migration

Cross-Empire Data Migration is a subsystem within Novell Storage Manager that allows for the movement of file system data between storage infrastructures on different platforms governed by different identity and security frameworks. Many customer initiatives can precipitate the need for such a move, including a migration to a different server operating system, a merger and acquisition by the organization, or just the consolidation of environments.

- Section 11.1, “Understanding Cross-Empire Data Migration,” on page 111
- Section 11.2, “Security and Ownership,” on page 114
- Section 11.3, “Prerequisites,” on page 115
- Section 11.4, “Creating the Migration Proxy Account,” on page 117
- Section 11.5, “Creating and Modifying an Identity Map,” on page 119
- Section 11.6, “Migration Options,” on page 137
- Section 11.7, “Viewing the Migration Log File,” on page 138
- Section 11.8, “Performing a User to User Data Migration,” on page 139
- Section 11.9, “Performing a Folder to User Data Migration,” on page 146
- Section 11.10, “Performing a Group to Group Data Migration,” on page 153
- Section 11.11, “Performing a Folder to Group Migration,” on page 159
- Section 11.12, “Performing a Folder to Folder Migration,” on page 166

11.1 Understanding Cross-Empire Data Migration

The mission of Cross-Empire Data Migration is to quickly and easily perform automated movement of data, based on a variety of scenarios, including the movement of data for multiple users and groups directly to its intended location across multiple servers or shares in a single operation, all while preserving certain file system metadata. Further, Cross-Empire Data Migration lets you leverage the policies provided in Novell Storage Manager to allow the customer to move to a managed storage environment on the target system and optionally restructure and reorganize data in the process.

An organization can use a wizard in NSMAdmin to implement a phased approach to migration by incorporating one or more migration types offered through the interface to add work onto the Novell Storage Manager event queue. In taking advantage of the dispatching and state machine architecture features of the event queue, the migration effort can be enhanced both in terms of performance through the NSM Agent subsystem and in terms of reliability in overcoming outages and other factors that occur in real-world environments. Additionally, other options involving copying rights, file ownership, filtering of the files to be copied and more, allow for greater control and flexibility during a data migration operation.

The Cross-Empire Data Migration architecture is engineered to eventually support multiple types of source platforms and targets, but the current release is limited to a Novell eDirectory source environment and a Microsoft Active Directory target environment.

Cross-Empire Data Migration generally supports three constructs for movement:

- Section 11.1.1, "User Storage Migration," on page 112
- Section 11.1.2, "Collaborative or Group Storage Migration," on page 113
- Section 11.1.3, "Direct Folder Storage Migration," on page 113

11.1.1 User Storage Migration

Cross-Empire Data Migration can be used to copy User object personal file data from the source platform to the target platform. In an eDirectory to Active Directory scenario, this would likely be a migration of the data from the Novell home directory to the Microsoft home folder. There are two options for migrating personal storage. The difference between the two is related to how Novell Storage Manager determines the path to a specific user's data on the source network. These options can be used exclusively or in combination with one another during a migration project:

- "User to User" on page 112
- "Folder to User" on page 112

User to User

This option allows you to instruct Novell Storage Manager to determine the source location for user data by using the Home Directory attribute in eDirectory. As part of the migration wizard, you specify a source eDirectory container. The user objects within that container are listed for matching with the target, and you can select one or more users for migration. For each user selected, the Home Directory attribute provides the source file system path to be used. This option is very useful when the Home Directory attribute in the source tree is populated correctly and there is a need to migrate data simultaneously from multiple locations on the source network. It is also very useful if the user directory name on the source does not match the account name on the target.

For procedures on performing a user to user data migration, see Section 11.8, "Performing a User to User Data Migration," on page 139.

Folder to User

This option allows you to specify the location of user data by providing a file system path as the source. Instead of specifying an eDirectory container, you specify a parent folder location on the file system in the source network. From this folder, all immediate subfolders are listed for matching with the target, and you can select one or more for migration. This option is useful when the Home Directory attribute in the source tree is not populated or reliable, or there is a need to migrate a set of users with folders in a single path on a single volume.

For procedures on performing a folder to user data migration, see Section 11.9, "Performing a Folder to User Data Migration," on page 146.

11.1.2 Collaborative or Group Storage Migration

File system data used by groups can also be copied by using the Cross-Empire Data Migration subsystem. The options available to the administrator are similar to those available for user storage, but are different in whether to rely on data in directory services or specify the file system paths directly.

The underlying concept behind both options is that the collaborative storage is being moved to a managed storage environment on the target network, which means that the Group Home Directory attribute is being populated and managed in directory services in the target tree. If you don't want to move some of the collaborative group directories, you should consider using Direct Folder Storage migration, which is documented at Section 11.1.3, "Direct Folder Storage Migration," on page 113.

The following options are available for moving collaborative storage:

- "Group to Group" on page 113
- "Folder to Group" on page 113

Group to Group

This option allows you to instruct Novell Storage Manager to determine the source location for user data by using the Group Home Directory attribute in eDirectory. As part of the migration wizard, you specify a source eDirectory container. The group objects within that container are listed for matching with the target, and you can select one or more groups for migration. For each group selected, the Group Home Directory attribute provides the source file system path to be used. This option is very useful when Novell Storage Manager has been used to manage collaborative storage in the source tree.

For procedures on performing a group to group data migration, see Section 11.10, "Performing a Group to Group Data Migration," on page 153.

Folder to Group

This option allows you to specify the location of group data by providing a file system path. Instead of specifying an eDirectory container, you specify a parent folder location on the file system in the source network. From this folder, all immediate subfolders are listed for matching with the target, and you can select one or more for migration. This option is useful when Novell Storage Manager has not been used in the source tree to manage collaborative group storage or when you are migrating only some of the group storage.

For procedures on performing a folder to group data migration, see Section 11.11, "Performing a Folder to Group Migration," on page 159.

11.1.3 Direct Folder Storage Migration

A major benefit in using Novell Storage Manager is that your organization can move to a managed storage environment for its file system data. Novell Storage Manager allows you to define and enforce policies on the data by driving management of it throughout the life cycle of the user or group associated with the data. The architecture of the Cross-Empire Data Migration subsystem allows organizations to move to this paradigm for both user and group storage.

However, you are not required to use this method during the migration process. You might not want to move to managed storage for all of the data, or you might want to move to it in phases. For this reason, the Cross-Empire Data Migration subsystem has provisions for direct movement of data outside of the policy construct by performing a folder to folder data migration.

Folder to Folder

A folder to folder migration allows you to move a folder and its contents directly from the source network to a designated location on the target network. Selecting this method in the wizard allows you to specify distinct file system paths on both the source and the target networks. All file system contents and metadata are copied during the operation.

For your convenience, there is a *Skip Open Files* option that allows you to migrate all of the closed files located in a folder. Open files are not migrated, but the filenames and paths of all of the open files are logged in a text file. You can then close all of the open files and do a follow-up migration of these remaining files by simply specifying the location of the text file.

With the introduction of Novell Storage Manager 3.1, you can now identify and move all files that are new or have been modified from a given date. Additionally, you can verify that all of the files you wanted to migrate from a source server have been migrated. Performing these tasks is done using four new utilities:

- **novscan.nlm:** A NetWare NLM that scans the contents of the target server and determines what files have been modified or created since you performed a preliminary file to file migration.
- **NovScanConfig.exe:** This Windows executable configures what file system data you want identified from the NetWare or Novell Open Enterprise Server source.
- **WinScan.exe:** This Windows executable lists the contents of the file system on the target Microsoft server following a file to file migration.
- **ScanCompare.exe:** This Windows executable compares the files on the NetWare or Open Enterprise Server source server and the Microsoft Server target server.

For procedures on performing a folder to folder migration, see Section 11.12, “Performing a Folder to Folder Migration,” on page 166

11.2 Security and Ownership

Moving to a managed storage environment presents an opportunity to refine the security on the data itself. By defining the security that should be on the file system as a part of the policy, you are assured that the security of the data on the target network is in line with the security and governance requirements that your organization wants to employ. This can also contribute to present and future compliance requirements for your organization. Avoiding these types of exposure is another benefit of moving to a managed storage environment.

However, in many environments, there is a desire to migrate security and ownership assignments directly from the source environment to the target. This capability is accomplished through the creation and optional usage of an Identity Map as a part of a migration operation.

- Section 11.2.1, “Defining an Identity Map for Security and Ownership Migration,” on page 114
- Section 11.2.2, “Using an Identity Map,” on page 115

11.2.1 Defining an Identity Map for Security and Ownership Migration

For security and ownership information to be migrated between environments, the Cross-Empire Data Migration subsystem requires a series of object equivalence definitions to identify an object in the source environment as equivalent to an analogous object in the target environment. In other words, if an object in the source environment is given rights to a file or folder, and you want that

trustee assignment to be migrated along with the data, then Novell Storage Manager must be told which object in the target environment is equivalent to it so that the appropriate rights assignment can be made. An identity map is a construct for creating and managing these equivalence definitions.

You can create and populate an identity map within the Cross-Empire Data Migration subsystem of the NSMAdmin interface. There are various options for automatically locating and matching objects based on a number of matching rules. There are options for creating manual assignments as well as for editing assignments.

However, some objects that are assigned rights in the source environment might not have an analogous object that already exists in the target environment. These objects need to be created before they can be defined to an identity map.

In addition, an analogous object might exist in the target environment, but might not be able to be assigned as a trustee, such as a container that is given rights in the source environment. The same container might exist in the target environment (Active Directory), but Active Directory does not support the assignment of a container as a security object. In these instances, a group representing the container is usually created for rights assignments.

You can import data into an identity map. This can be useful when you already have a data set defining equivalences, or you can easily create one using data from an external system.

In general, it is standard practice to iteratively evolve an identity map as needed to perform a migration. Within the interface, you can run a check scan against a given source file system path to check rights and ownership assignments against an identity map. This identifies which objects still need a definition within the map in order for a migration to finish with 100 percent coverage for security and ownership.

11.2.2 Using an Identity Map

When you are satisfied with the coverage within the identity map for a given file system path, you can use the identity map as a part of a migration. You can optionally use the identity map in conjunction with any migration operation type supported by the Cross-Empire Data Migration subsystem:

- User storage migration
- Collaborative or group storage migration
- Direct folder storage migration

The system supports a single identity map within the framework at any one time. When the map is created or edited, the master copy is held by the NSM Engine and is automatically distributed to NSM Agents as necessary.

IMPORTANT: Certain operations during a Cross-Empire Data Migration involve building a cache on the local workstation or the NSM Engine. If the identity map contains more than 20,000 objects, the time it takes to cache all of the objects could significantly inhibit the speed of the migration.

Once the cache has been built the first time on the workstation or NSM Engine, it does not have to be rebuilt again.

11.3 Prerequisites

The server on which the NSM Engine in Active Directory is installed must have the Novell Client installed while the migration is being performed. After the migration is complete, the client can be removed. Additionally, the NSM Engine can delegate migration operations to NSM Agents for

improved migration performance. If Agents are deployed as a part of a Novell Storage Manager installation, these agents are individually used for migration if the Novell Client is installed on them. In order for an agent to participate in a migration, the server that has the agent installed must also have the Novell Client installed. This determination is made automatically within Novell Storage Manager as a part of Agent/Engine communications and no additional configuration is required in order to use this feature.

The Novell Client installed on the NSM Engine in the Active Directory should be properly configured to use SLP (Service Location Protocol) for the Novell eDirectory that serves as the source of a data migration. For information on SLP configuration, see Section 4.0, "Setting Client Properties" in the *Novell Client 2 SP1 for Windows Administration Guide*.

11.3.1 Prerequisite Tasks

Before you proceed with a Cross-Empire Data Migration, perform the following tasks:

1. Log in with Administrative access to the Domain.
2. Install the Novell Storage Manager Engine on the Windows 2008 server.

   See "Installing the NSM Engine" in the *Novell Storage Manager 3.1.1 for Active Directory Installation Guide.*
3. Install the Novell Client with the NMAS installation default option on the NSM Engine server.

   The Novell Client can be removed after you have completed your migrations.
4. Extend the Active Directory schema.

   This is required only if you are migrating to a target share managed by a collaborative storage policy.

   See "Active Directory Schema" in the *Novell Storage Manager 3.1.1 for Active Directory Installation Guide*.
5. Install NSMAdmin, run the Setup Wizard, and complete installation steps.

   See "Installing and Configuring NSMAdmin" in the *Novell Storage Manager 3.1.1 for Active Directory Installation Guide*.
6. Install and authorize the NSM Event Monitor.

   This is required if you are creating and testing storage policies for the migration of data.

   See "Installing and Configuring the Event Monitor" and "Authorizing the Event Monitor" in the *Novell Storage Manager 3.1.1 for Active Directory Installation Guide*.
7. Assign Full Control permission to the NSMProxyRights group for shares that you will be migrating data to on the target devices.

   See "Setting Rights and Privileges on Managed Storage" in the *Novell Storage Manager 3.1.1 for Active Directory Installation Guide*.
8. Install and authorize NSM Agents and configure Proxy Agents on all servers that will be target servers for Cross-Empire Data Migrations.

   See "Installing and Configuring an NSM Agent" and "Authorizing the NSM Agents" in the *Novell Storage Manager 3.1.1 for Active Directory Installation Guide*.
9. (Conditional) If you plan to migrate data to a NAS device, make the NSMProxyRights group a member of the Local Administrators group on each NAS device.

   See "Setting Rights and Privileges on Managed Storage" in the *Novell Storage Manager 3.1.1 for Active Directory Installation Guide*.
10. Install the Novell Client and configure SLP on any NSM Agent servers that will be involved in a Cross-Empire Data Migration.

The Novell Clients can be removed after you have completed your migrations.

11. Create Novell Storage Manager policies for the migration of storage.

    These policies are needed if the Cross-Empire Data Migrations will be driven by Novell Storage Manager 3.1.1 for Active Directory policies, which we recommend for migrating user data.

12. For all objects in eDirectory that have rights assigned to the file system, create matching objects in Active Directory.

    To migrate rights assigned to containers, you must create an equivalent Group object in Active Directory for each container object in eDirectory,.

11.4 Creating the Migration Proxy Account

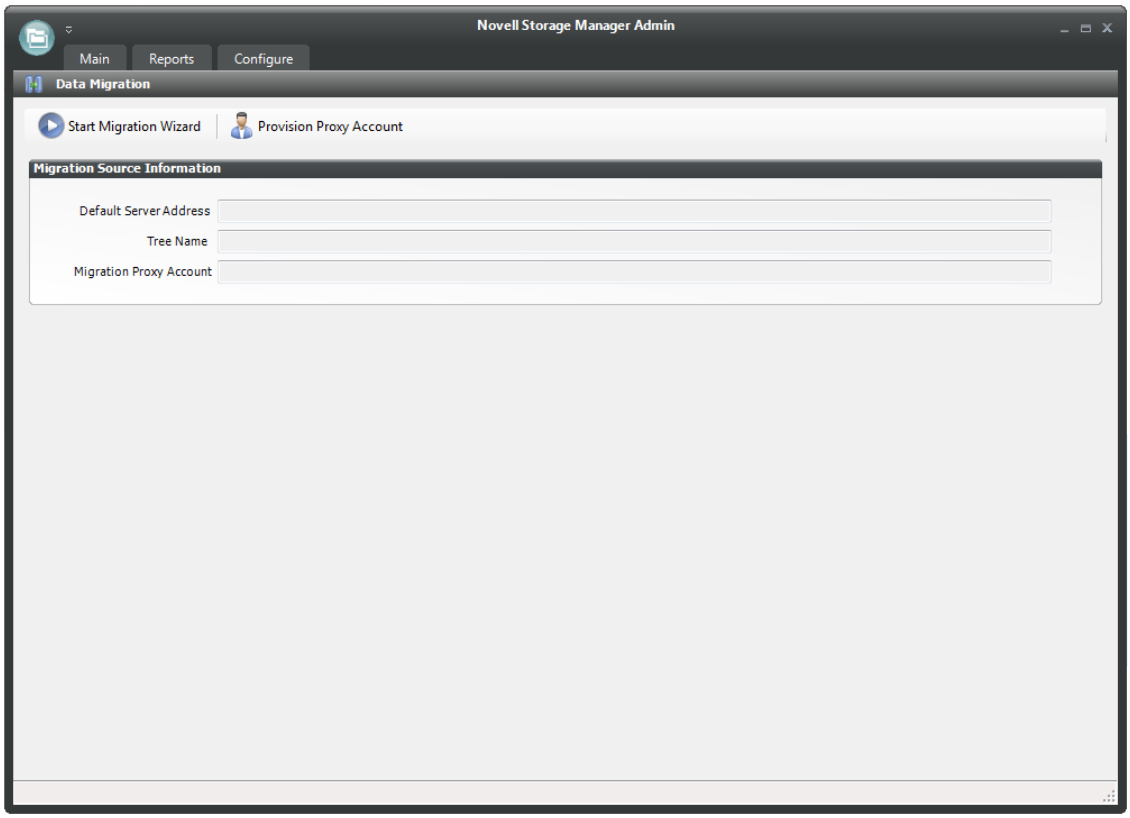
The NSM Engine running in Active Directory uses a migration proxy account to log in to the eDirectory tree. Any time you perform a migration from the eDirectory tree to the Active Directory domain, NSMAdmin uses the migration proxy account that you establish in this procedure.

IMPORTANT: This process creates a new User object in Novell eDirectory with a 32-character password that is generated automatically by Novell Storage Manager. If your Universal Password policy does not accommodate 32-character passwords, you must modify or create a new Universal Password policy before proceeding. For more information, refer to Section 3.4, "Creating Password Policies," (http://www.novell.com/documentation/password_management33/pwm_administration/data/an4bun5.html) in the *Novell Password Management 3.3.1 Administration Guide*, especially the information in Figure 3.3, "Advanced Password Rules Continued."

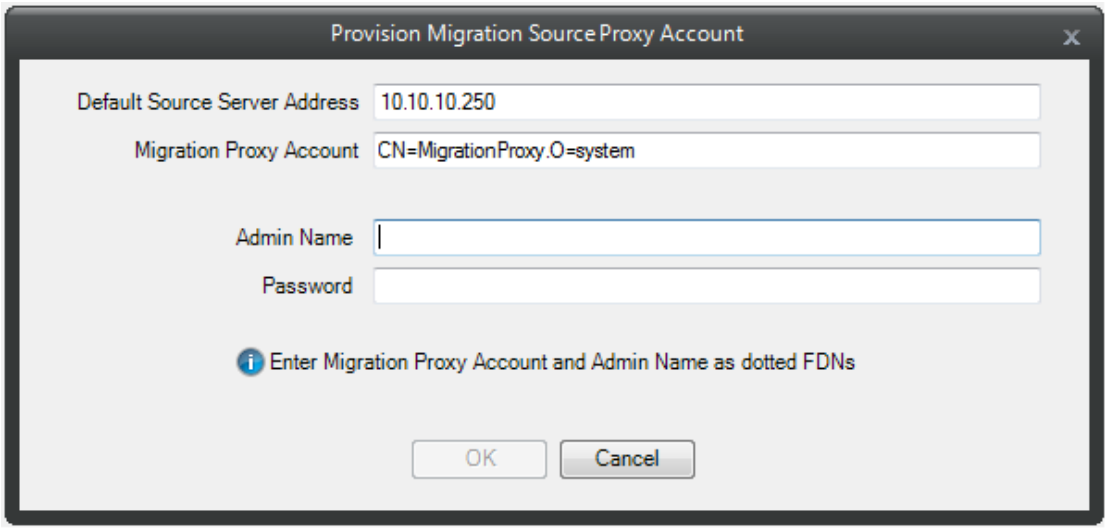
---

1. Launch NSMAdmin.
2. From the *Main* tab, click *Data Migration*.

   The following page appears:



3 Click *Provision Proxy*.



4 Fill in the following fields:

Default source Server Address: Specify the IP address or DNS name of a server in the eDirectory tree where the files you want to migrate are located. The NSM Engine in the Active Directory environment must be able to communicate with this server when performing data migrations.

Migration Proxy Account: Provision a migration proxy account by specifying the typeless fully distinguished name (FDN) of the proxy account that you want to provision.

The NSM Engine running in Active Directory uses the migration proxy account to log in to the eDirectory tree. Any time you perform a migration from the eDirectory tree to the Active Directory domain, the NSM Engine uses the migration proxy account that you establish in this step.

Admin Name: Specify the typeless FDN of an account in the source eDirectory tree that has the appropriate right to provision the Migration Proxy Account (MPA).

Password: Specify the password for the typeless FDN provided above.

5 Click *OK*.

The information entered in the Provision Migration Proxy Account dialog box is now displayed in the fields of the Data Migration page.

The NSM Engine logs in as the Admin account provided, and provisions the MPA as a User object in the source eDirectory tree. It also grants the MPA object full rights to the root of the source tree, which allows Novell Storage Manager to pull eDirectory and file system information during the course of migration operations.

11.5 Creating and Modifying an Identity Map

Novell Storage Manager for Active Directory uses an identity map to make associations between the users, groups, and containers that are the owners and trustees of the Novell network data and the corresponding data owners on the Microsoft network target.

You create a single identity map for each eDirectory tree that you are migrating.

IMPORTANT: You must create an identity map so that file and folder rights, trustee assignments, and other metadata are maintained during the migration. If you do not want to maintain these rights, trustee assignments, and other metadata, you can skip this section and migrate through using the *Migrate Data Only* option from the *Migrate Data and Trustees* menu.

- Section 11.5.1, “Creating an Identity Map,” on page 119
- Section 11.5.2, “Importing a Source Path List,” on page 127
- Section 11.5.3, “Adding Source Entries to the Identity Map,” on page 129
- Section 11.5.4, “Adding or Modifying Target Entries to the Identity Map,” on page 131
- Section 11.5.5, “Saving the Identity Map,” on page 132
- Section 11.5.6, “Exporting an Identity Map,” on page 132
- Section 11.5.7, “Importing an Identity Map,” on page 132
- Section 11.5.8, “Generating a Preview Report,” on page 133
- Section 11.5.9, “Review Rights and Trustee Assignment Mappings,” on page 135
- Section 11.5.10, “Adding Entries from Preview Reports,” on page 136

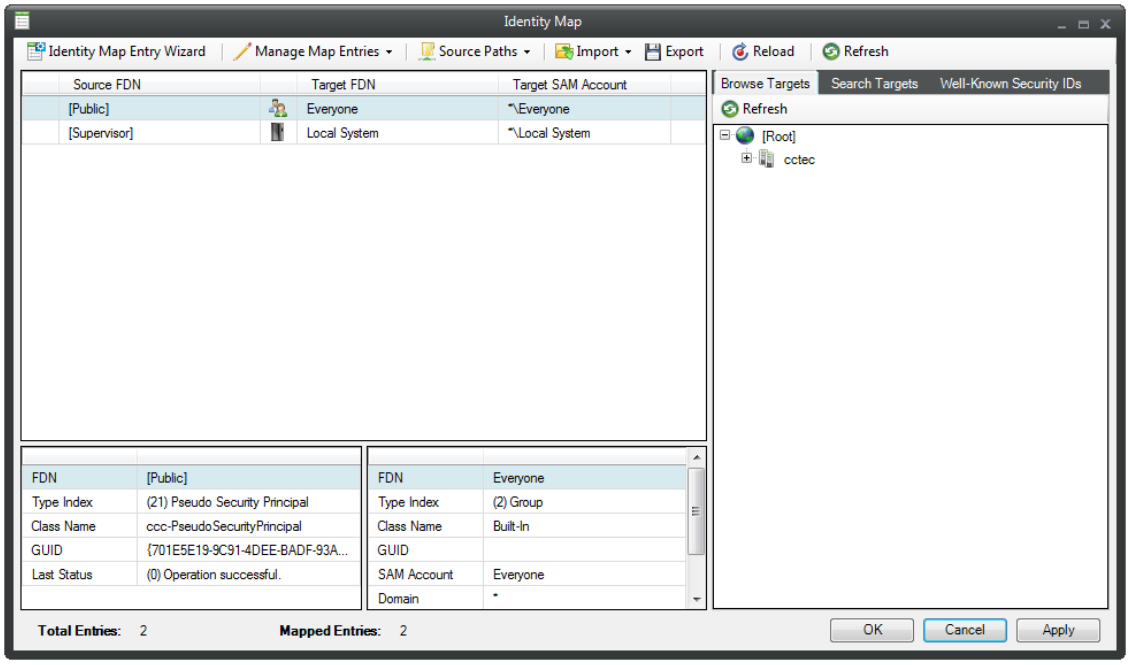
11.5.1 Creating an Identity Map

1 In NSMAdmin, click the *Main* tab.

2 Click *Data Migration*.

3 Click *Identity Map Management*.

The following page appears:



The page displays an initial identity map with a small number of suggested entries that you can append.

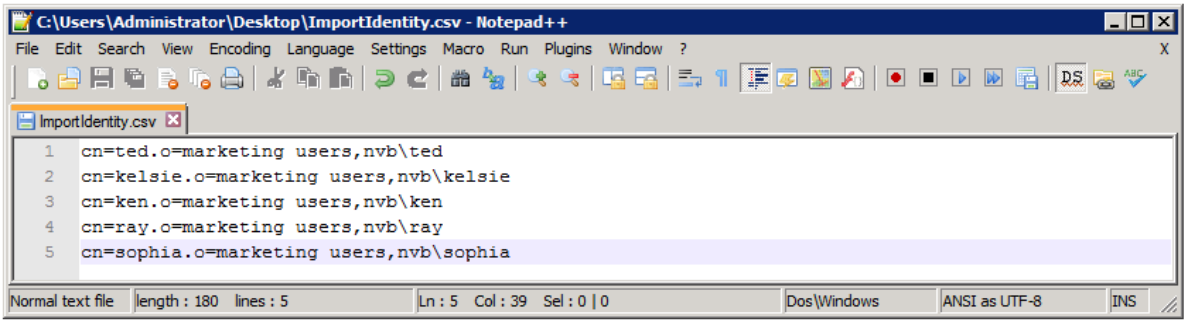
4 Do one of the following:

- To import associations between users in eDirectory and Active Directory using a delimited text CSV file, go to "Importing Identity Associations through Delimited Text" on page 120.
- To associate the users between the two directory services yourself, go to "Creating Object Associations" on page 124.

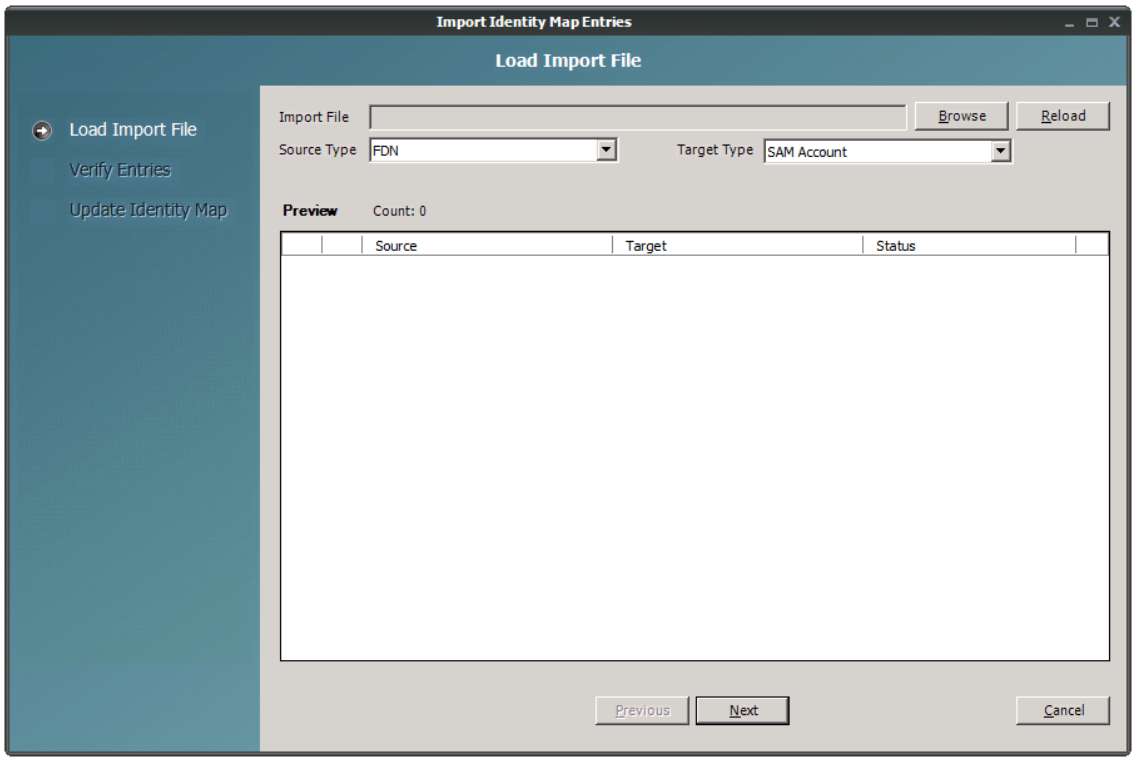
Importing Identity Associations through Delimited Text

If you have a delimited text CSV file that associates eDirectory user and group objects with Active directory user and group objects, you can import it into the identity map using the *Import Identity Map from Delimited Text* option.

The CSV file can have entries using either typeful or typless Fully Distinguished Names (FDNs).



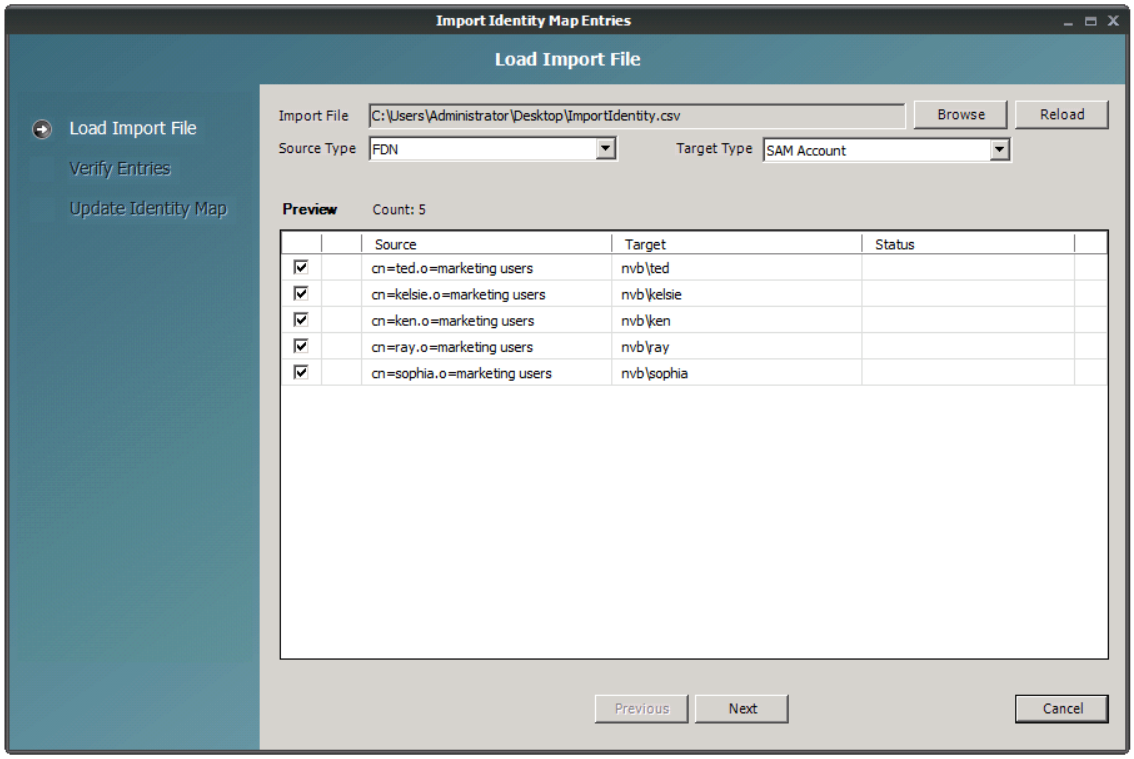
1 Select *Import* > *Import Identity Map from Delimited Text*.



2 Click *Browse*.

3 Select the file, then click *Open*.

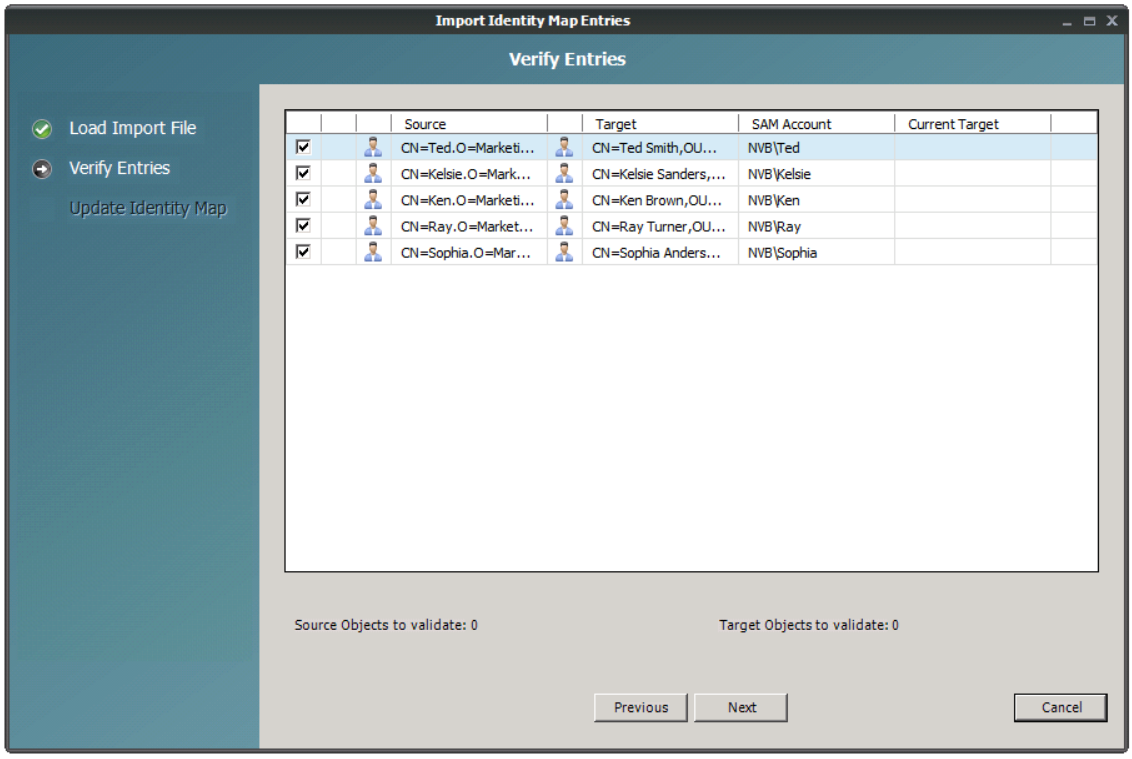
The following page appears and specifies whether the names in the CSV file are formatted properly.



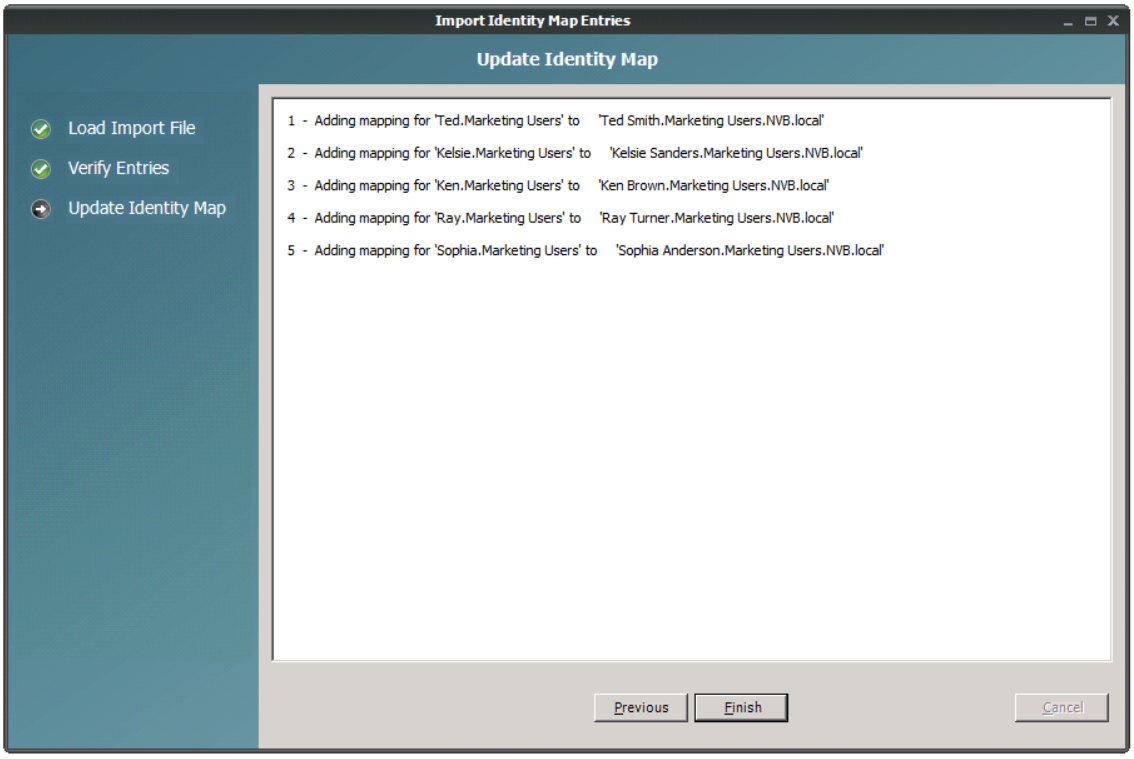
4 (Conditional) If incorrect options in the *Source Type* or *Target Type* fields are displayed, select the correct options.

5 Click *Next*.

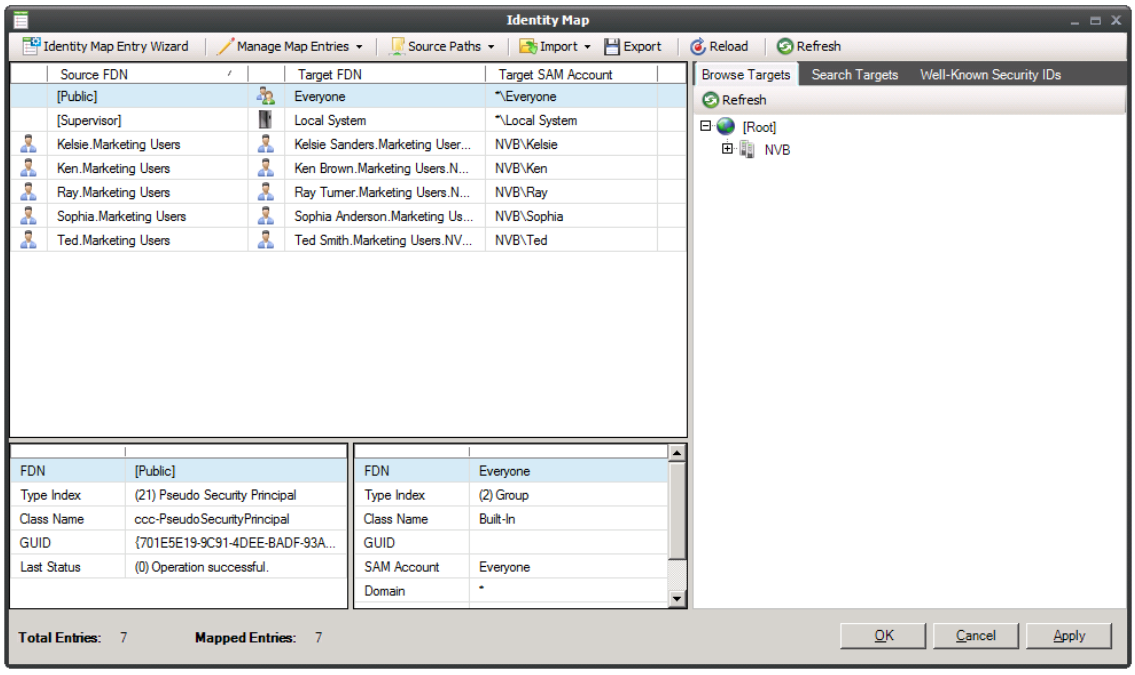
The following page appears and specifies whether the user and group objects exist in eDirectory and Active Directory.



6 Click *Next*.



7 Click *Finish*.



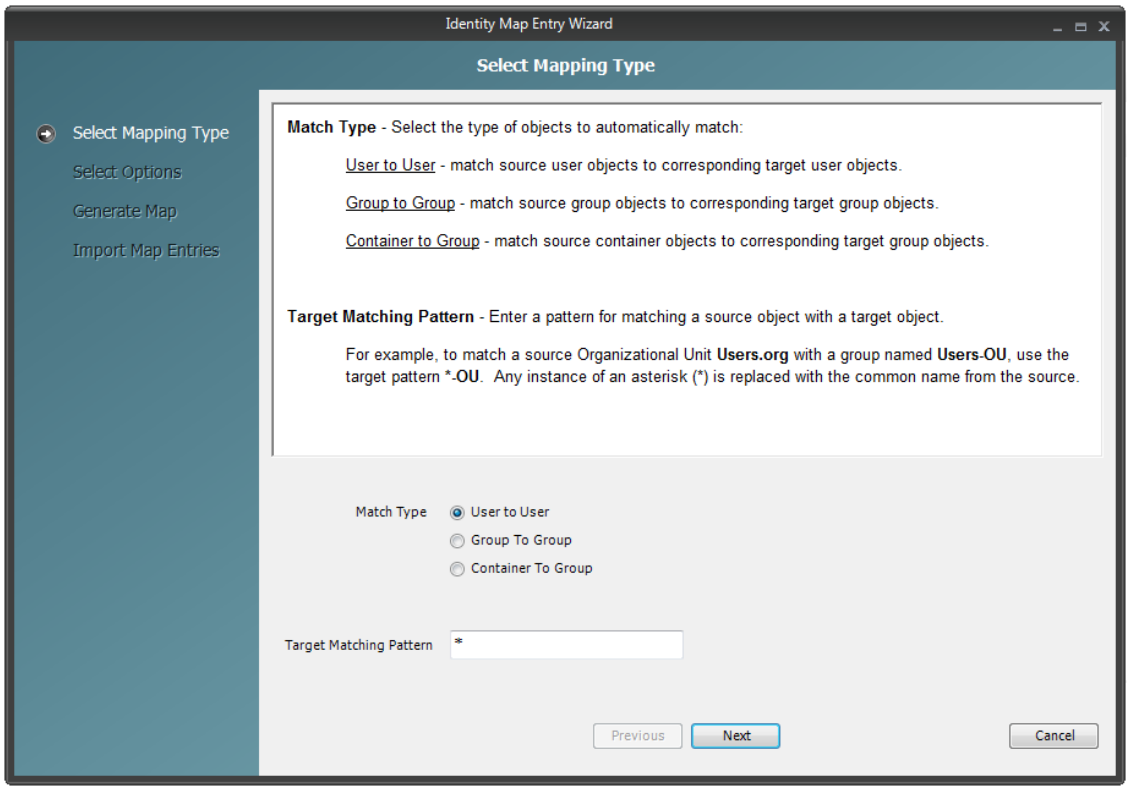
8 Click *Apply* to save the updated identity map.

9 (Conditional) If you have additional users to import from another delimited text CSV file, select the new CSV file and repeat the procedures in this section.

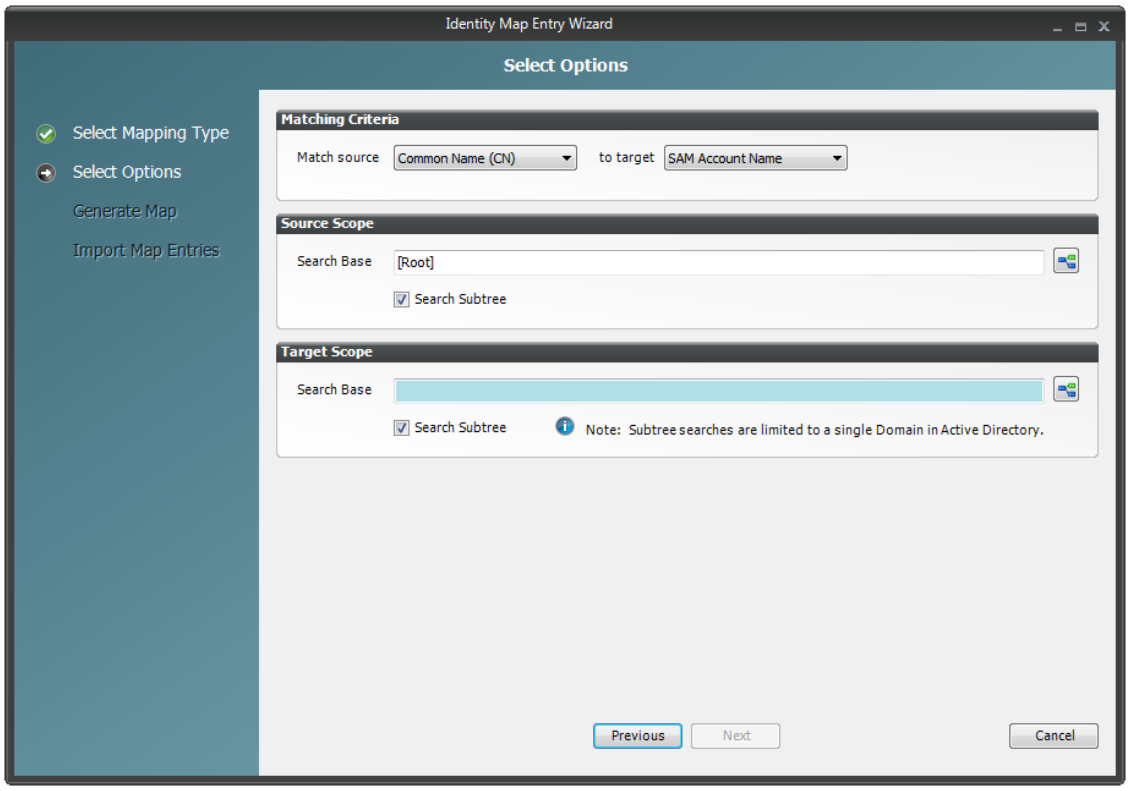
10 (Conditional) If you need to add additional users that were not listed in the CSV file, proceed to "Creating Object Associations" on page 124.

Creating Object Associations

1 Click *Identity Map Entry Wizard*.



2 Leave the *User to User* option selected and click *Next*.



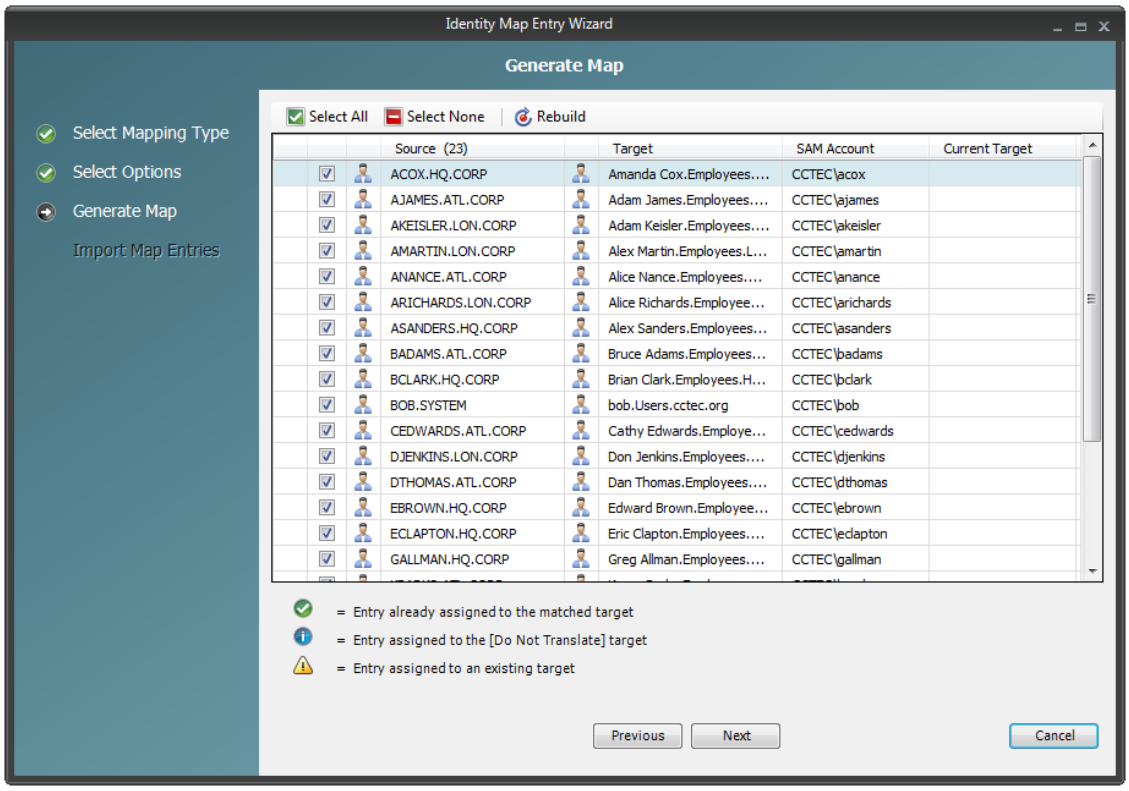
3 In the Matching Criteria region of the page, use the *to target* drop-down menu to specify if the target accounts to locate are SAM accounts or Common Name (CN) accounts.

   If you need to match using both account types on your target server, you can choose one option now and then run the wizard again and choose the other option. You might need to run the wizard multiple times in order to add all of the users, groups, and containers to the identity map.

4 In the Source Scope region, browse to and select the source container with the users you want included in the identity map.

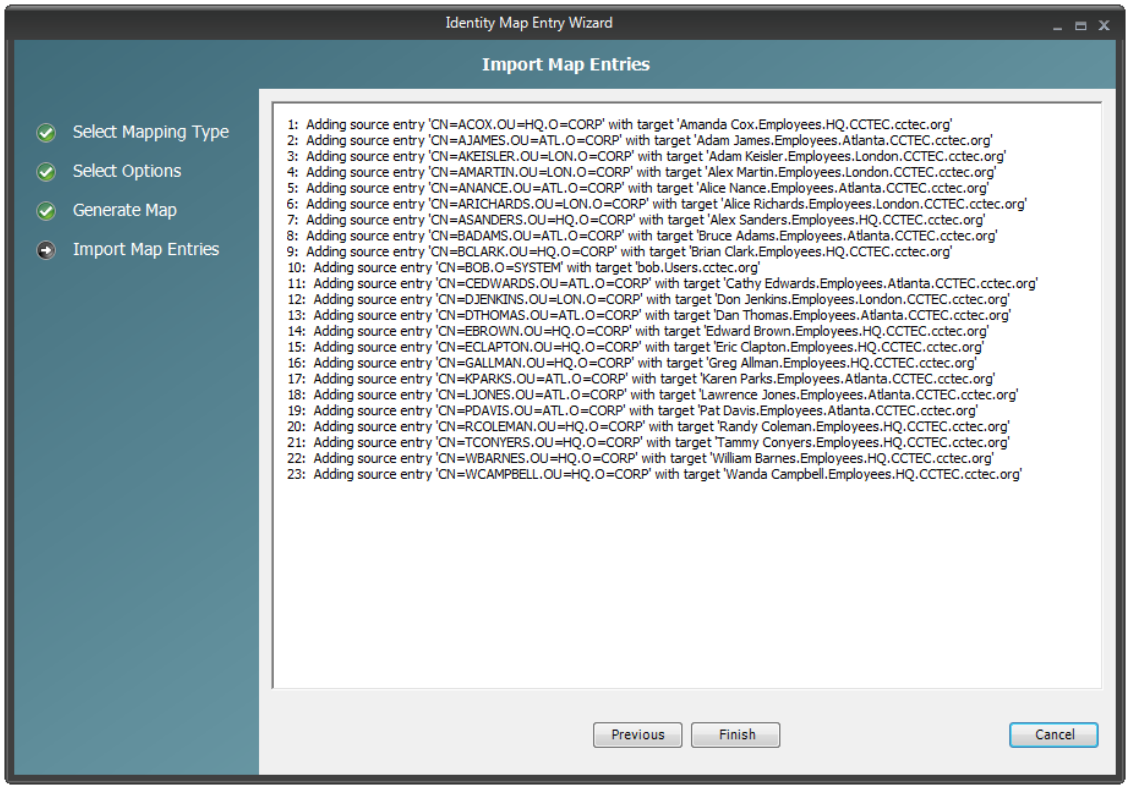
5 In the Target Scope region, browse to and select the target container with the users you want included in the identity map.

6 Click *Next*.



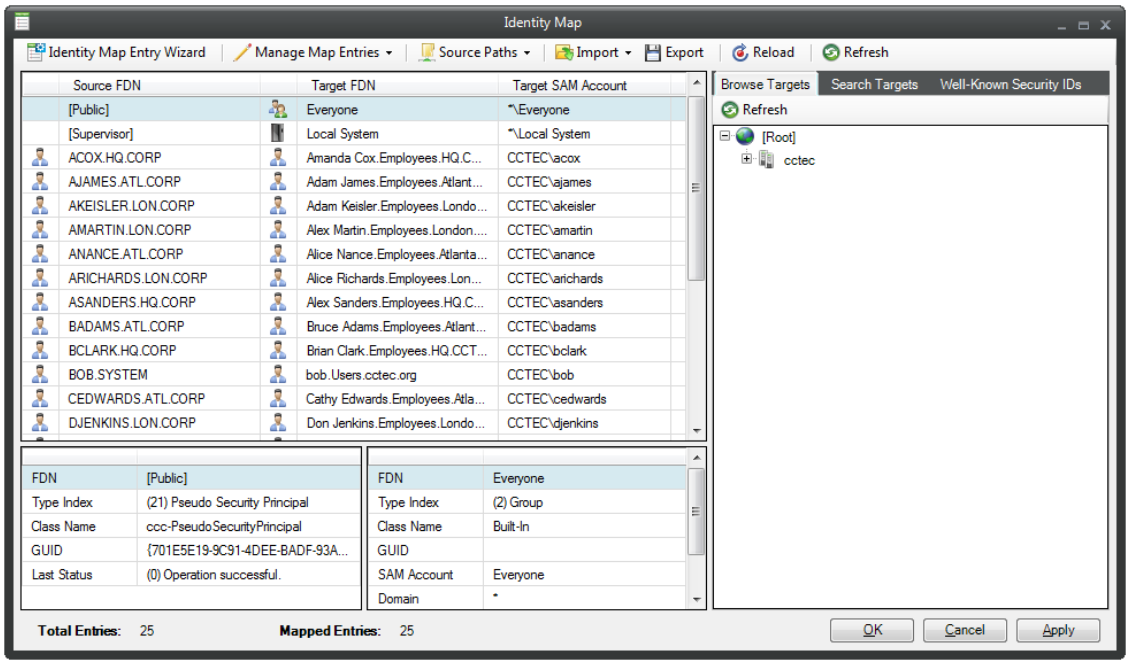
7 (Conditional) Deselect any names you do not want appended to the identity map file.

8 Click *Next*.



9 Click *Finish*.

The identity map is appended with the new entries.



10 Click *Apply* to save the updated identity map.

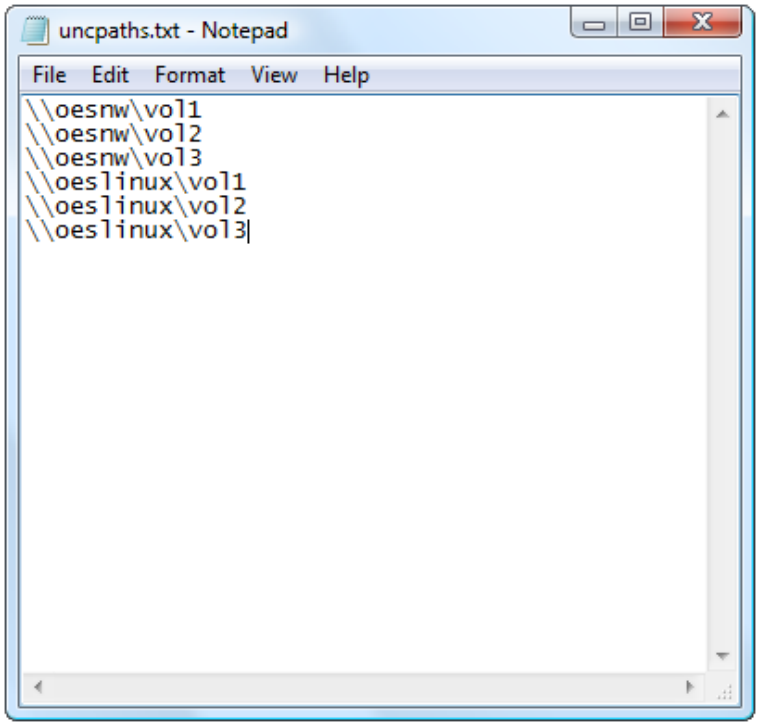
11 Repeat Step 1 and Step 2 and select the account type you did not select previously.

12 Repeat Step 3 through Step 10.

11.5.2 Importing a Source Path List

Depending on the size of your network, you might need to specify a significant number of different source paths as you build your identity map. You can easily import a list of your UNC paths from a text file so that these paths are accessible from drop-down menu. Additionally, the search is filtered so that it can locate the specific UNC path as you type.

1 Using a text editor, create a file with UNC paths for each server and volume that you want to import, then save the file.

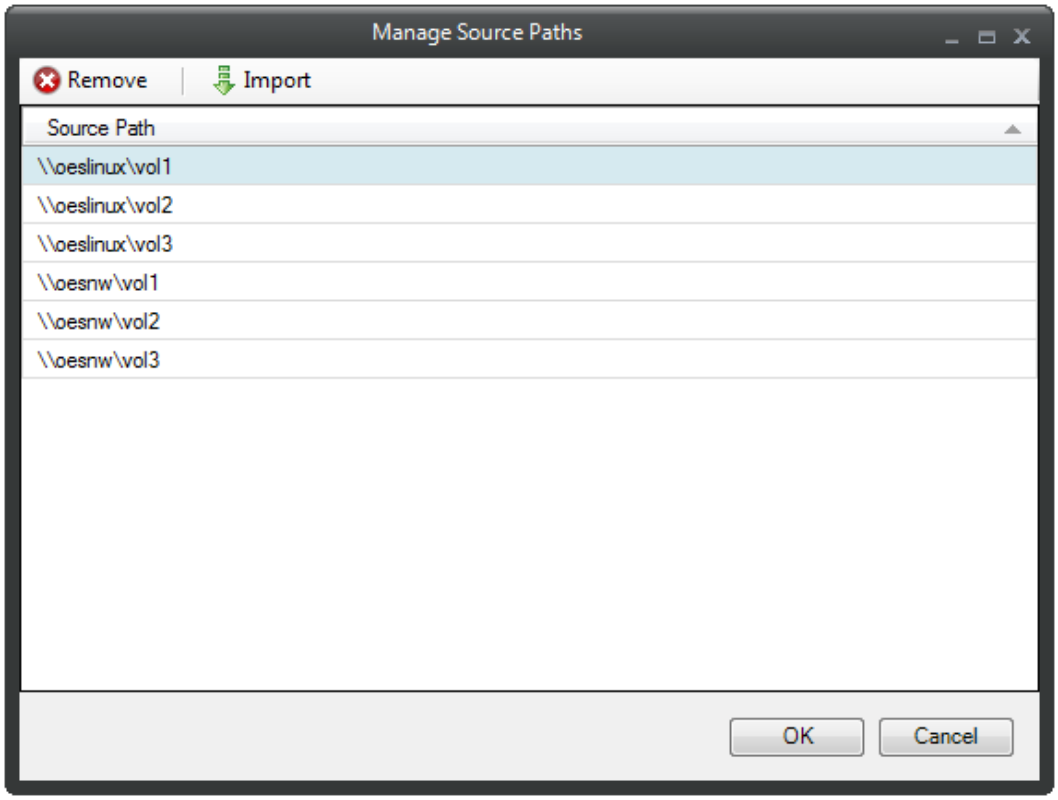


2 In NSMAdmin, click the *Main* tab.

3 Click *Data Migration*.

4 Select *Source Management* > *Source Path Cache*.

5 Click *Import*, browse to and select the text file, then click *Open*.



6 Click *OK*.

11.5.3 Adding Source Entries to the Identity Map

To append additional users or groups to the identity map from the Novell eDirectory source:

1 In NSMAdmin, click the *Main* tab.

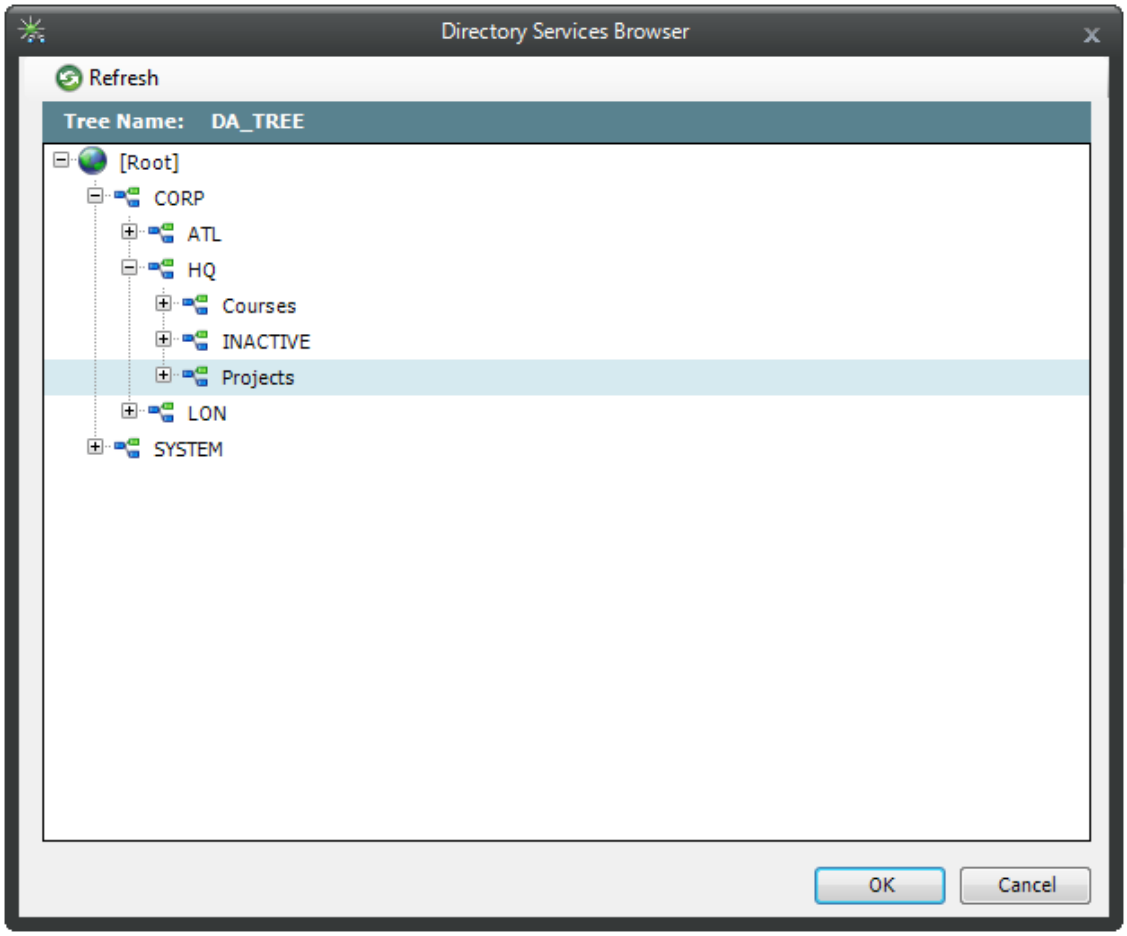
2 Click *Data Migration*.

3 Click *Identity Map Management*.

4 Select *Manage Map Entries* > *Add Source Entries*.

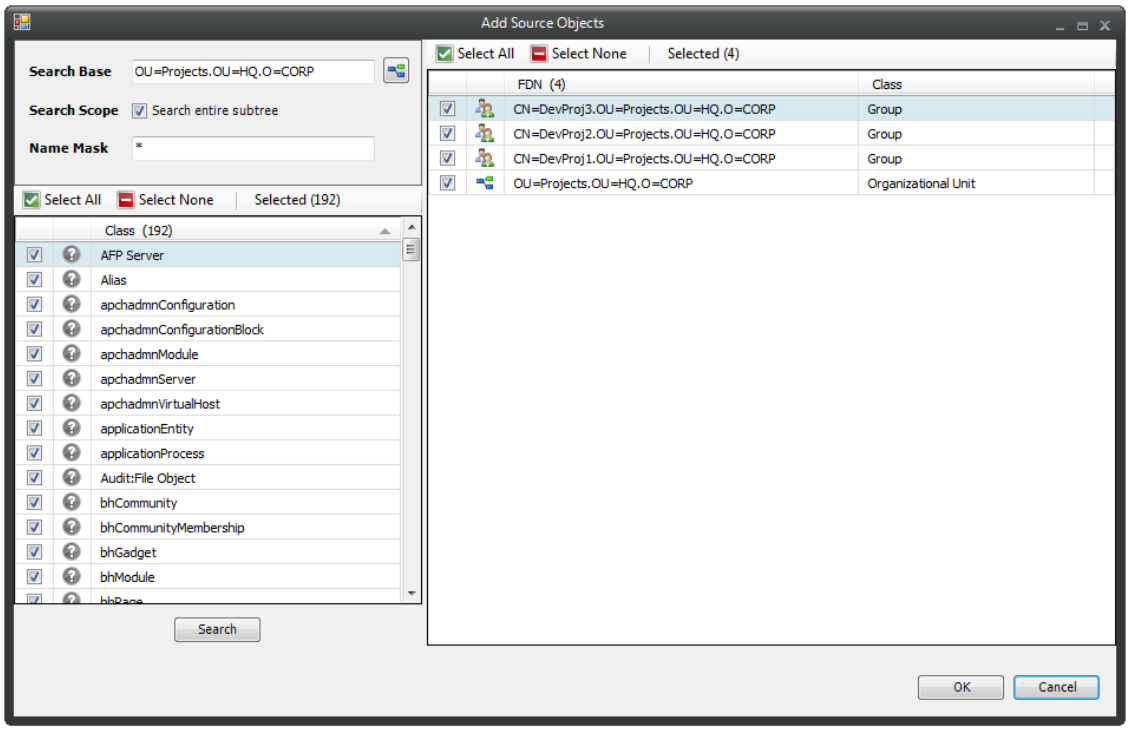
5 In the Add Source Objects page, use the *Search Base*, browse button, *Search Scope*, and *Name Mask* fields to locate and select the container you want to use for your search.

If you wish to limit your search to a selected set of object types, under the *Class* heading, deselect those object types you do not want included in the search.



6 Click *OK*.

7 On the Add Source Object page, click *Search*.



By default, all located objects are selected.

8 Deselect the objects you do not want to append to the identity map.

9 Click *OK*.

11.5.4 Adding or Modifying Target Entries to the Identity Map

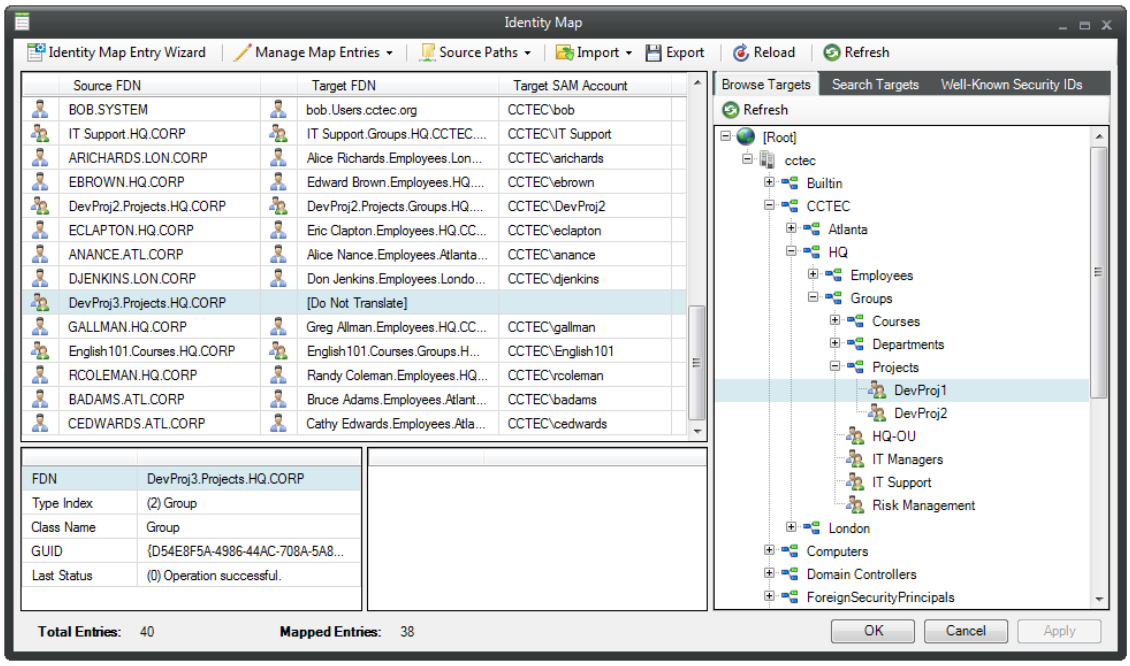
1 In NSMAdmin, click the *Main* tab.

2 Click *Data Migration*.

3 Click *Identity Map Management*.

4 In the Identity Map page, select the listing for the source entry to which you want to add a target or that you want to modify.

5 Use one of the tabs in the right panel of the Identity Map page to locate and select the desired target.



6 Specify the object as the new target object.

   For example, if you were using the *Browse Targets* tab in the example above, you could right-click or drag the object to place it in the *Target SAM Account* field of the selected source object.

7 Click *Apply* to save the modified identity map.

11.5.5 Saving the Identity Map

As you develop your identity map, you might find that you need to work on it at different time intervals during the day or week. To save the identity map, simply click *OK*.

11.5.6 Exporting an Identity Map

When working with identity maps, you might find that you want to experiment with different associations. In such cases, you should have multiple identity maps. To save an identity map that differs from the original, you must export it.

1 Click *Export*.

2 Save the XML file to the location you prefer.

11.5.7 Importing an Identity Map

This action retrieves exported versions of identity maps.

1 Select *Import* > *Import Identity Map File*.

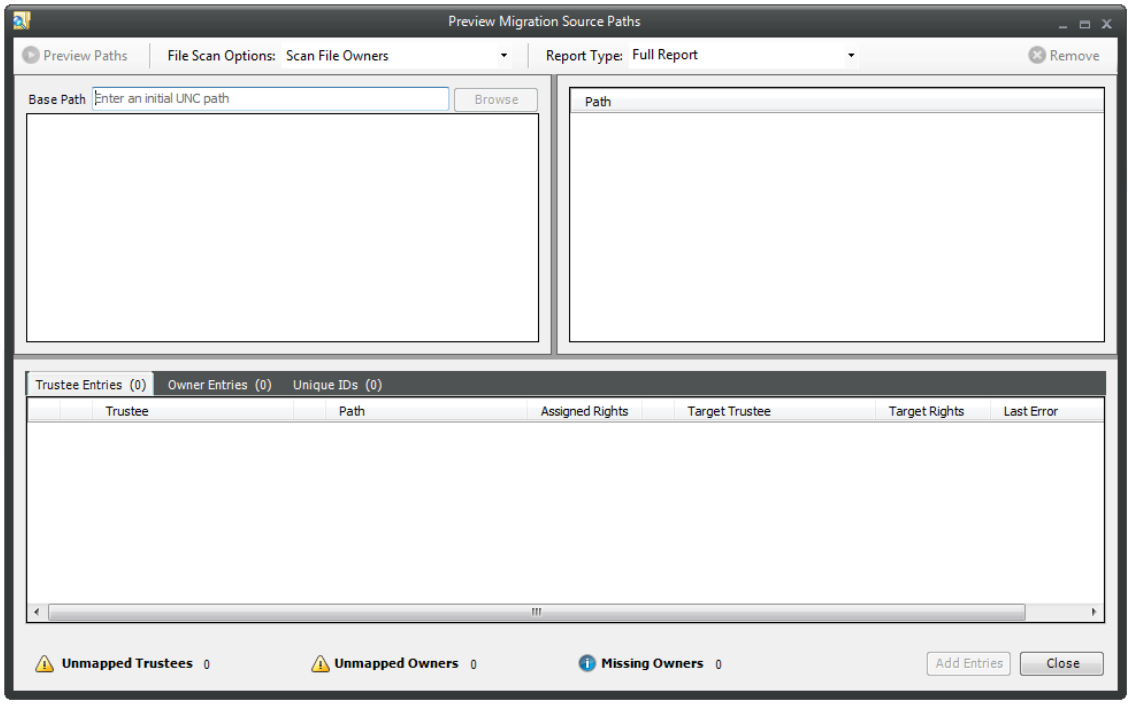
2 Select the file, then click *Open*.

11.5.8 Generating a Preview Report

Before performing a Cross-Empire Data Migration, you should generate a preview report. The report indicates any concerns that might need to be addressed such as objects which have file rights but which have not yet been mapped in the identity map.

The preview report uses your identity map, and searches file and folder rights assignments and ownership of the actual data which you will be migrating to indicate which objects actually have ownership or rights, and if an object is mapped in the identity map.

1. In NSMAdmin, click the *Main* tab.
2. Click *Data Migration*.
3. Click *Identity Map Management*.
4. In the Identity Map page, select *Source Paths* > *Generate Preview Report*.



5. From the *File Scan Options* drop-down menu, choose one of the following:
   - ***Scan Folders Only*:** Select this option to view the trustee assignments and owners of folders.
   - ***Scan File Owners*:** Select this option to view the trustee assignments and owners of folders, along with the owners of files.
   - ***Scan File Owners and Trustees*:** Select this option to view the trustee assignments and owners of folders, as well as the trustee assignments and owners of files.

     Depending on the number of files and folders on your Novell network, the *Scan File Owners and Trustees* option can take a significant amount of time to generate. We recommend using one of the other options first.

6 From the *Report Type* drop-down menu, choose one of the following:

- ***Anomaly Report***: Depending on which of the *File Scan Options* is selected, this generates a report of all of the folders and files that have trustees or owners that are *not* mapped to a target object in the identity map.
- ***Full Report***: Depending on which of the *File Scan Options* are selected, this generates a report of all of the folders and files, along with their corresponding owners and trustees, and indicates whether they are mapped to a target object in the identity map or not.

  Depending on the number of files and folders on your Novell network, generating a full report can take a significant amount of time. We recommend generating an anomaly report instead.

7 In the *Base Path* field, specify an initial UNC path for a server and volume to browse.

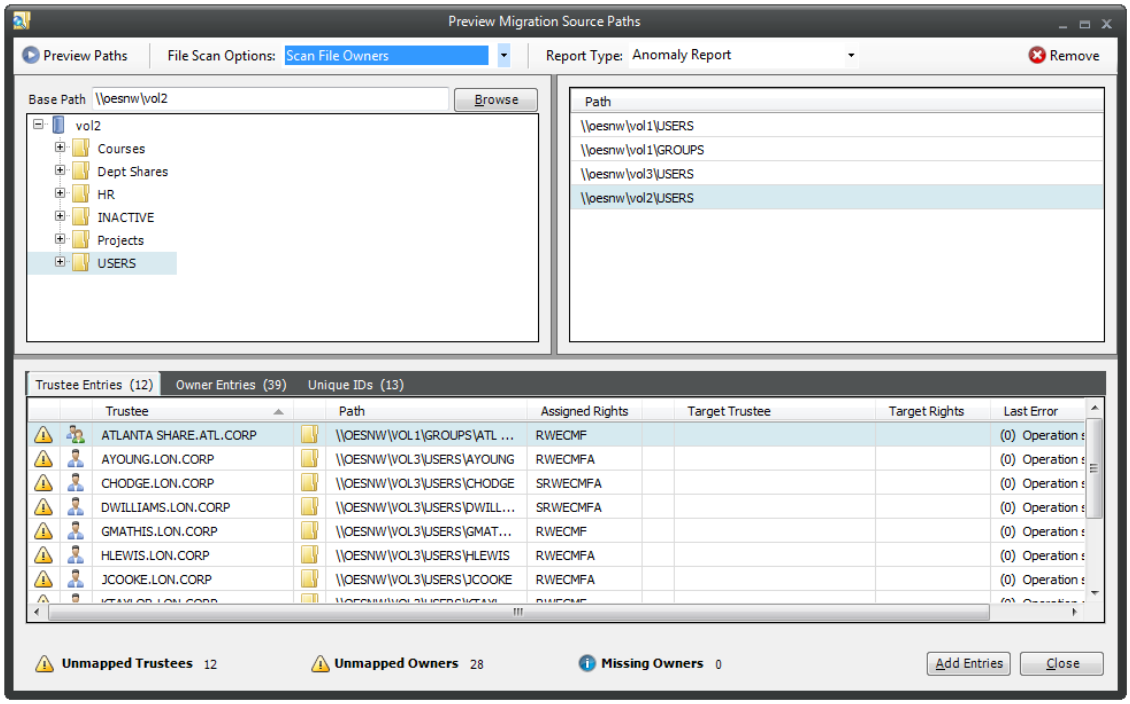
For example, `\\server_name\volume_name\ or \\ip_address\volume_name`.

After you enter a path, you can click the *Browse* button to browse to the folder you want, such as the Users folder.

8 Drag the selected folder to the *Path* pane.

9 Repeat Step 7 and Step 8 to add all other paths to use for generating reports.

10 In the *Path* pane, select the path you want to use for the preview report, then click *Preview Paths*.



11 Use the tabbed reports to preview targets according to trustees, owners, and unique IDs.

For example, in the graphic above, the *Trustee Entries* tab displays the source IDs that have a trustee assignment to a folder but a target ID has not yet been created in the identity map.

The *Owner Entries* tab displays owners of files and folders that do not have a corresponding target in the identity map.

The *Unique IDs* tab displays a single entry for each ID that is mapped in the identity report.

12 Click *Add Entries* to append the entries to the identity map.

The entries are added to the identity map and you can now add target entries by following the procedures in Section 11.5.4, "Adding or Modifying Target Entries to the Identity Map," on page 131.

13 Repeat Step 10 through Step 12 for each of the paths listed in the *Path* pane.

11.5.9 Review Rights and Trustee Assignment Mappings

Despite the inherent differences in rights, trustee assignments, and permissions between Novell and Microsoft networks, the Cross-Empire Data Migration subsystem of Novell Storage Manager for Active Directory does its best to match the Novell rights trustee assignments with the equivalent Microsoft permissions and advanced permissions.

When you generate a Preview Report, you should pay particular attention to the actual rights in the *Assigned Rights* column and the proposed file and folder rights listed in the *Target Rights* column.

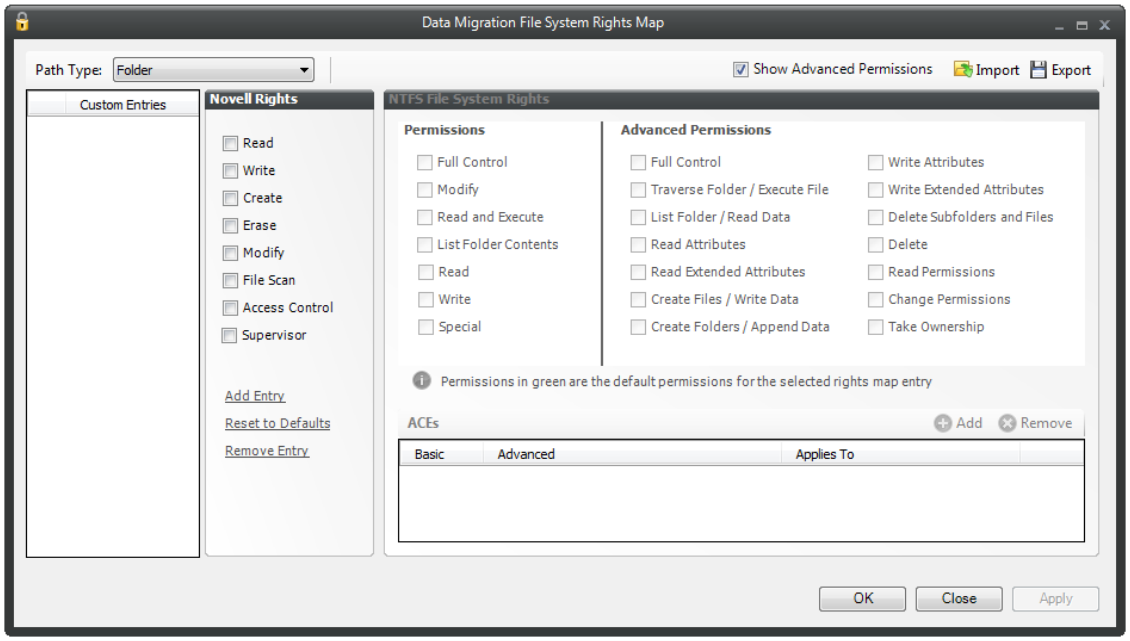
You can modify the rights mappings by using the File System Rights Map. When you do this, you specify a mapping between one particular set of rights on the Novell servers to one particular set of rights on the Microsoft Active Directory servers. As an example, the default mapping is to map the Novell rights RWECMF to the Active Directory rights MELRW. As a further example, perhaps when files have this set of rights you do not want to grant the E (erase) right to files on the target. You could modify the mapping using the procedures below to change the mapping of Novell rights RWECMF to the Active Directory rights MLRW. When you do this, you change the mapping for every file that has that exact set of rights, but it does not change the E mapping in any other set of rights. For instance, if you had trustees that had RWCEF, that mapping would not be changed because you changed the mapping for RWCEMF.

To view or modify these rights:

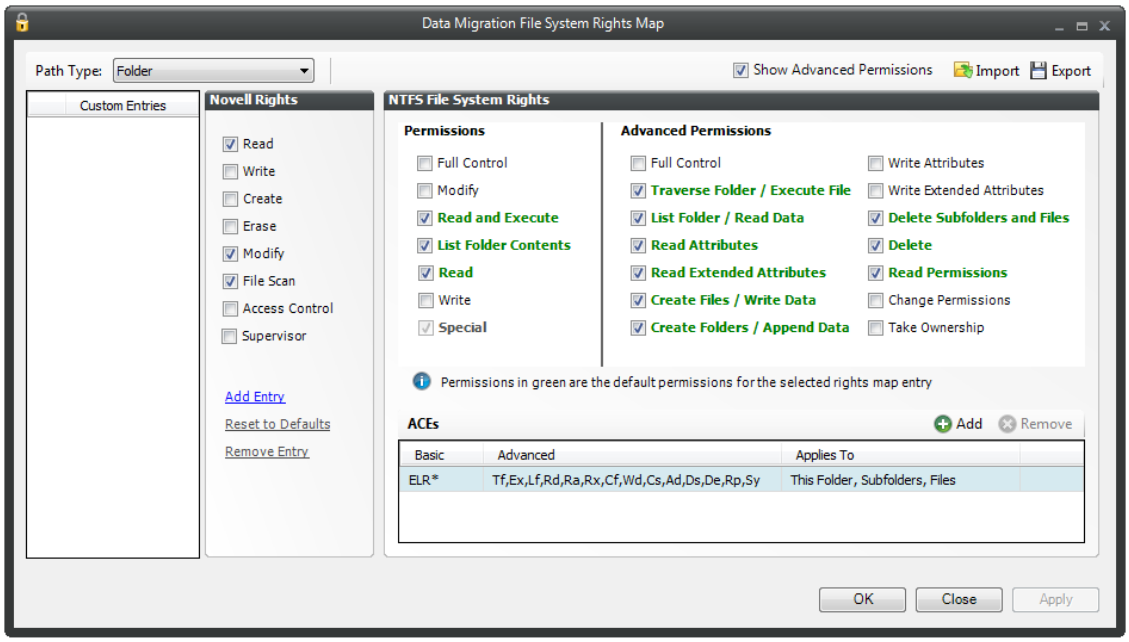
1 In NSMAdmin, click the *Main* tab.

2 Click *Data Migration*.

3 Click *Identity Map Management* > *File System Rights Map*.



4 In the *Novell Rights* column, click the rights to see the equivalent NTFS permissions and advanced permissions.



The default rights are indicated in green.

5 Select or deselect rights as needed.

6 Click *Apply* to save the settings.

11.5.10 Adding Entries from Preview Reports

In Step 12 on page 134, you added entries to the identity map by using the Preview Migration Source Path page's *Add Entries* button. You can also use the *Add Entries from Preview Report* option to retrieve any preview report that you have generated for the directory tree you are working with, and add those entries to the identity map.

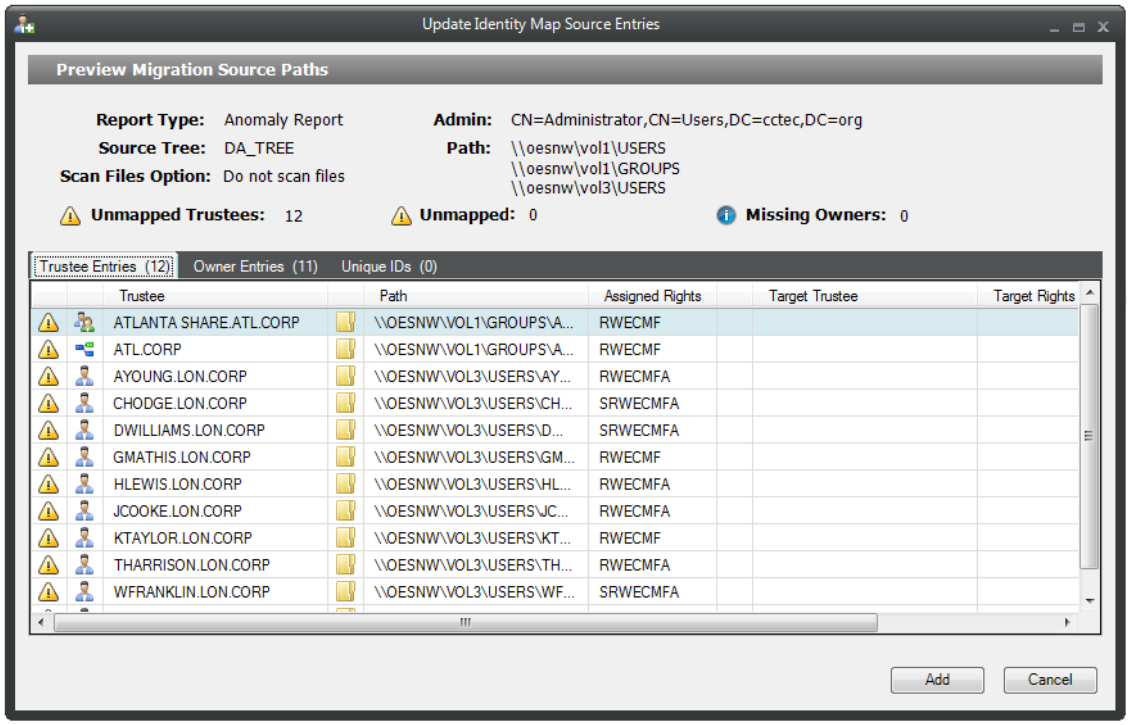
1 In NSMAdmin, click the *Main* tab.

2 Click *Data Migration*.

3 Click *Identity Map Management*.

4 Click *Source Paths* > *Add Entries from Preview Report*.

5 From the Browse Migration Preview Reports dialog box, select the preview report you want to add, then click *OK*.



At this point, you can view the preview report according to the tabbed options.

6 Click *Add* to append the entries to the identity map.

The entries are added to the identity map and you can now add target entries to each by following the procedures under Section 11.5.4, "Adding or Modifying Target Entries to the Identity Map," on page 131.

11.6 Migration Options

The Cross-Empire Data Migration subsystem of Novell Storage Manager for Active Directory provides the following options for migration:

- Section 11.6.1, "Data and Trustees," on page 137
- Section 11.6.2, "Trustees Only," on page 138
- Section 11.6.3, "Data Only," on page 138

11.6.1 Data and Trustees

This option migrates the data and the associated folder and file rights and trustee assignments specified in the identity map.

NOTE: The initial identity map referenced in Step 3 on page 119 does not function as an identity map until you have appended entries to it.

The procedures that begin in Section 11.8, "Performing a User to User Data Migration," on page 139 use the Data and Trustees option.

11.6.2 Trustees Only

This option migrates the rights and trustee assignments of data that has already been migrated. If the data to which the trustee assignments are assigned has not been migrated, the associated rights and trustee assignments for those files or folders are not migrated.

If you attempt to use this option and you have not created an identity map, you cannot proceed.

This option is frequently used when migrating the rights and trustee assignments from a single Novell source to a remote Windows Server that does not have an installed Novell Client.

NOTE: In this scenario, you can avoid installing a Novell Client on the Windows Server and instead install the Novell Client with NMAS, along with the NSM Agent, on a Windows 7 workstation in the same domain.

11.6.3 Data Only

This option migrates only the data and not the associated rights and trustee assignments. After you have migrated the data, you can later go back and apply the file rights and trustee assignments to the data through the *Migrate Trustees* option.

When data is migrated by using this option, file ownership is set according to the Novell Storage Manager policy for the migration target. If there is no policy in place, the owner is the Novell Storage Manager proxy user in Active Directory.

In the procedures included in the remainder of this section, the *Copy Options - Rights and Ownership* page is not applicable for a Data Only migration.

11.7 Viewing the Migration Log File

The migration log file can be used to track the status of the migration. You can view the file by using a Windows tail program or an application such as `dbgview.exe`.

To view the log file using `dgbview.exe`, refer to the application's documentation for configuring and viewing log file data.

Procedures for viewing the log file data using a Windows tail program follow:

1. Download a Windows tail program and install it on the NSM Engine host or the Cross-Empire Data Migration enabled NSM Agent tasked with the migration.

   To verify that the NSM Agent is Cross-Empire Data Migration enabled, refer to the Agent Servers page in NSMAdmin. For more information, see Section 12.3.3, "Agent Servers," on page 234.

2 Do one of the following:

- If the server to which you are migrating data is running a Cross-Empire Data Migration capable agent, or is set up to be proxied by a Cross-Empire Data Migration capable agent, at the NSM Agent server, use the Windows tail application to open the log file at:

  `C:\ProgramData\Novell\Storage Manager\Agent\Log\nsmagent-ad.log`

- If the server to which you are migrating data is not running a Cross-Empire Data Migration capable agent, and is not set up to be proxied by a Cross-Empire Data Migration capable agent, at the NSM Engine server, use the Windows tail application to open the log file at:

  `C:\ProgramData\Novell\Storage Manager\Engine\Log\nsmengine-ad.log`

3 Refer to the log file during the migration to view the status.

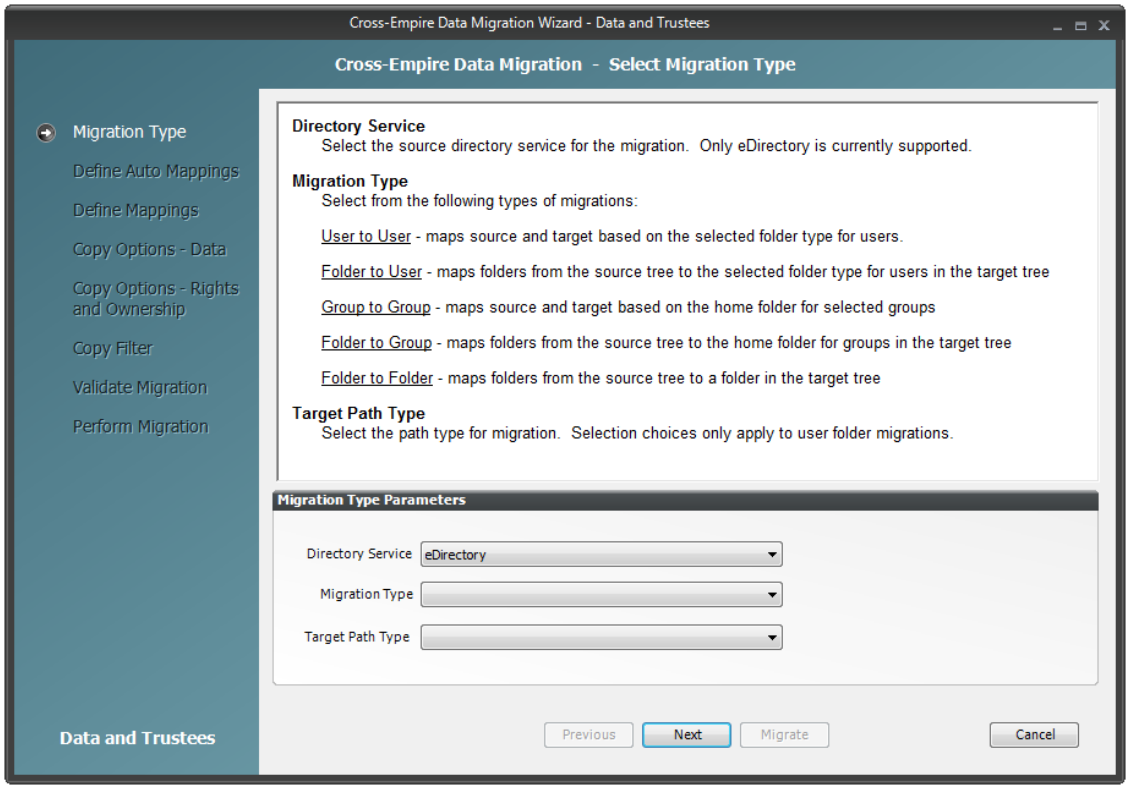
11.8 Performing a User to User Data Migration

1 Make sure you have completed the prerequisites and have created a migration proxy account. For more information on the prerequisites, see Section 11.3, "Prerequisites," on page 115. For more information on creating a migration proxy account, see Section 11.4, "Creating the Migration Proxy Account," on page 117.

2 In NSMAdmin, click the *Main* tab.

3 Click *Data Migration*.

4 Click *Migrate Data and Trustees*.

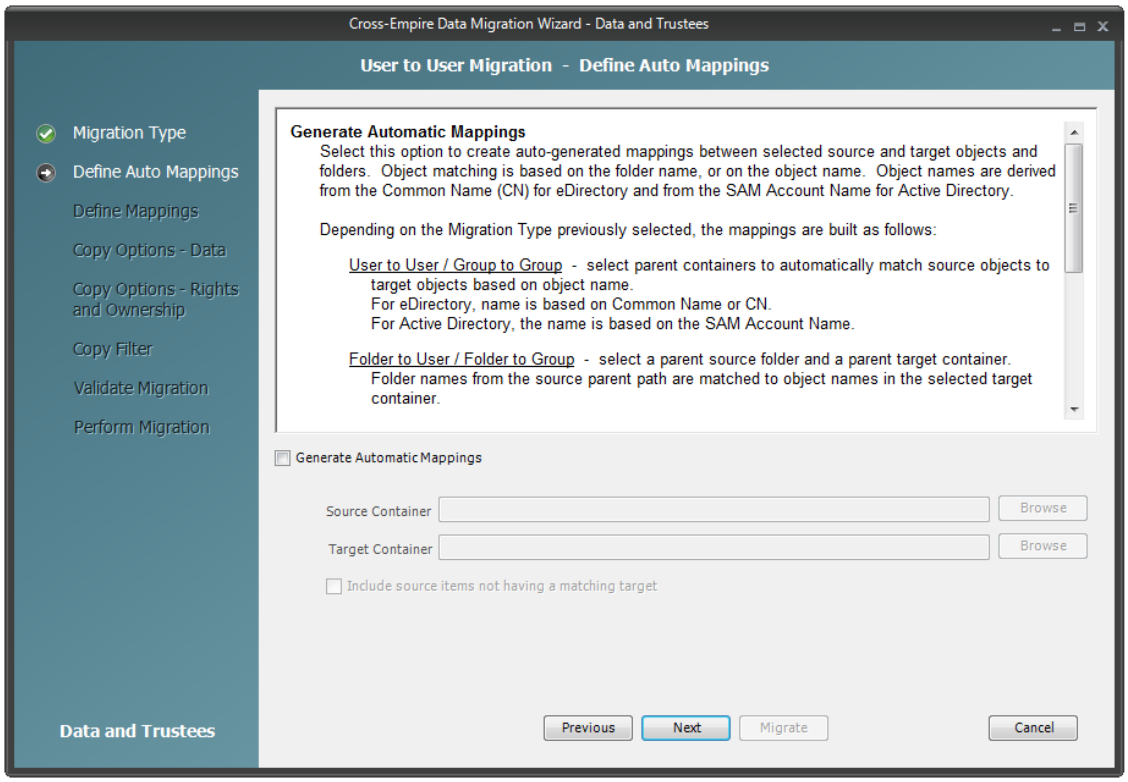


5 From the *Migration Type* drop-down menu, select *User to User.*

6 From the *Target Path Type* drop-down menu, select the target path type for the data that you will migrate.

For example, if you select *Home Folder*, the data is copied to each user's home folder path as defined in directory services.

7 Click *Next*.



8 Do one of the following:

- Fill in the following fields:

  Generate Automatic Mappings: If you are migrating a large number of users, select this check box to activate the other fields.

  Source Container: Browse to select the source container.

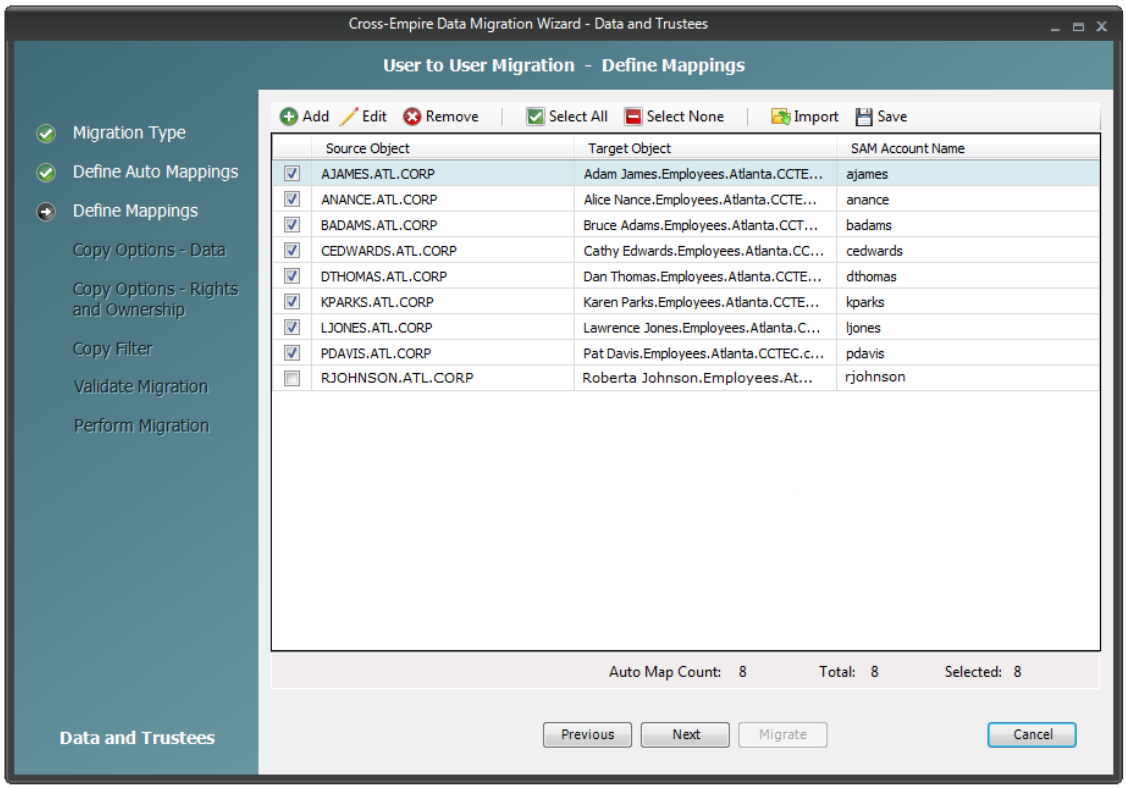
  Target Container: Browse to select the target container.

  Include Source items not having a matching target: Indicate if you want to identify source objects not having a matching target object.

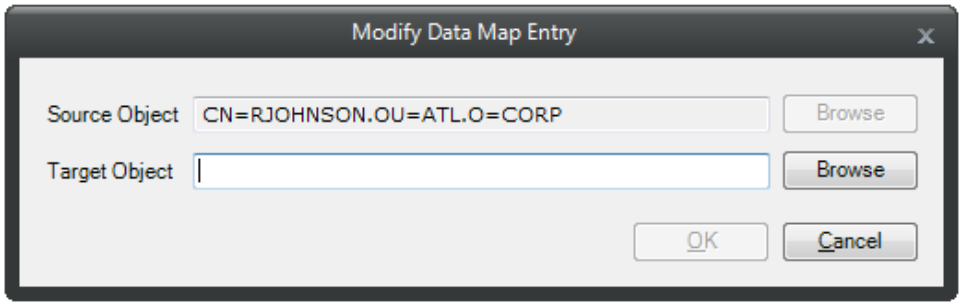
- If you are migrating only a few users, use the *Add* button on the next wizard page to add the users individually.

9 Click *Next*.

The Data Migration Wizard attempts to match the Common Name (CN) of objects from the eDirectory source with the SAM (Security Accounts Manager) Account Names in the Active Directory target. If there is a match, the listed object in the *Source Object* field is selected and a corresponding match is listed in the Target Object column.



10 Specify a target object for each source object that is not automatically matched by double-clicking the name to bring up the Modify Data Map Entry dialog box.



11 Click *Browse*, specify the target object, then click *OK*.

The target object is displayed in the Target Object column.

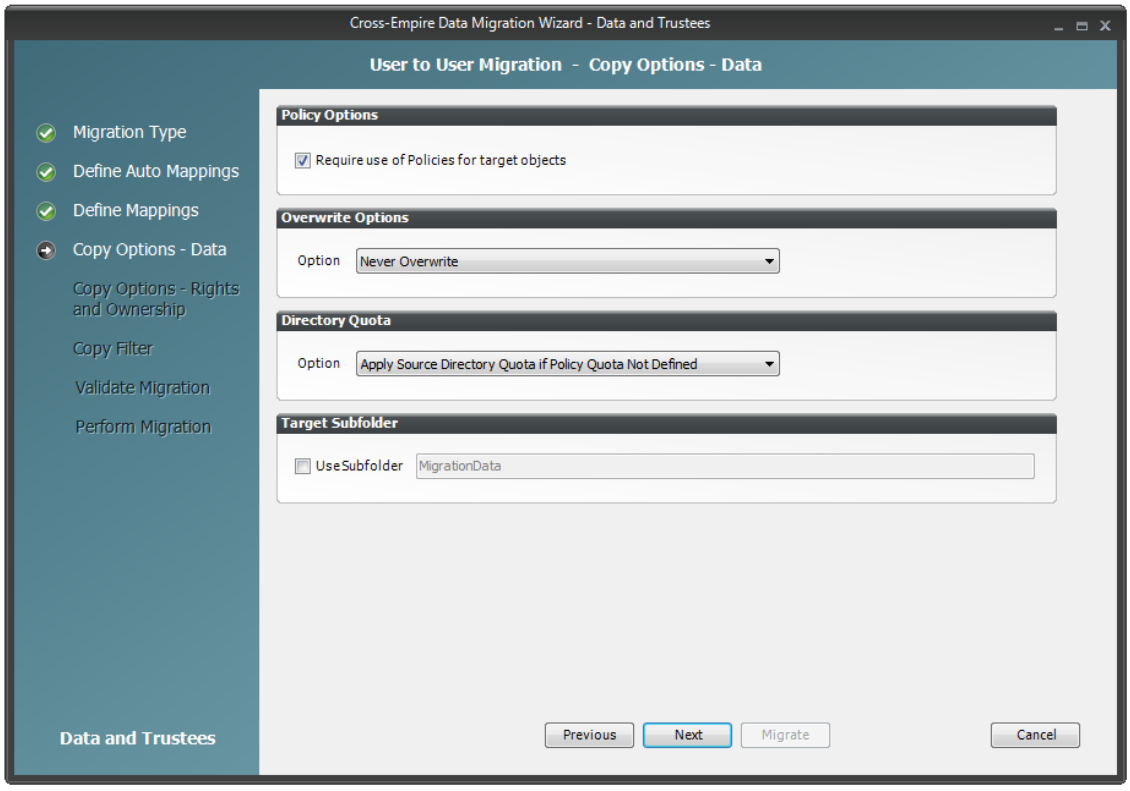
12 Click the check box corresponding to the listing with the new target.

13 Repeat Step 10 and Step 11 to specify all target objects that are not listed.

To change the specified target object, use the *Edit* button.

To add an object to the Source Object column, use the *Add* button.

14 When all of the objects you want to migrate are selected and have an associated target object, click *Next*.



15 Fill in the following fields:

Require use of policies for target objects: If you are migrating data for objects to an Active Directory container that has an associated Novell Storage Manager policy, leave this check box selected.

If this check box is selected and there is no associated Novell Storage Manager policy, the object's data is not eligible for migration.

Additionally, if you are migrating a user and the target user is not currently managed by an associated policy, but the object does have a policy that would apply to it, then Novell Storage Manager automatically applies that policy to the target user.

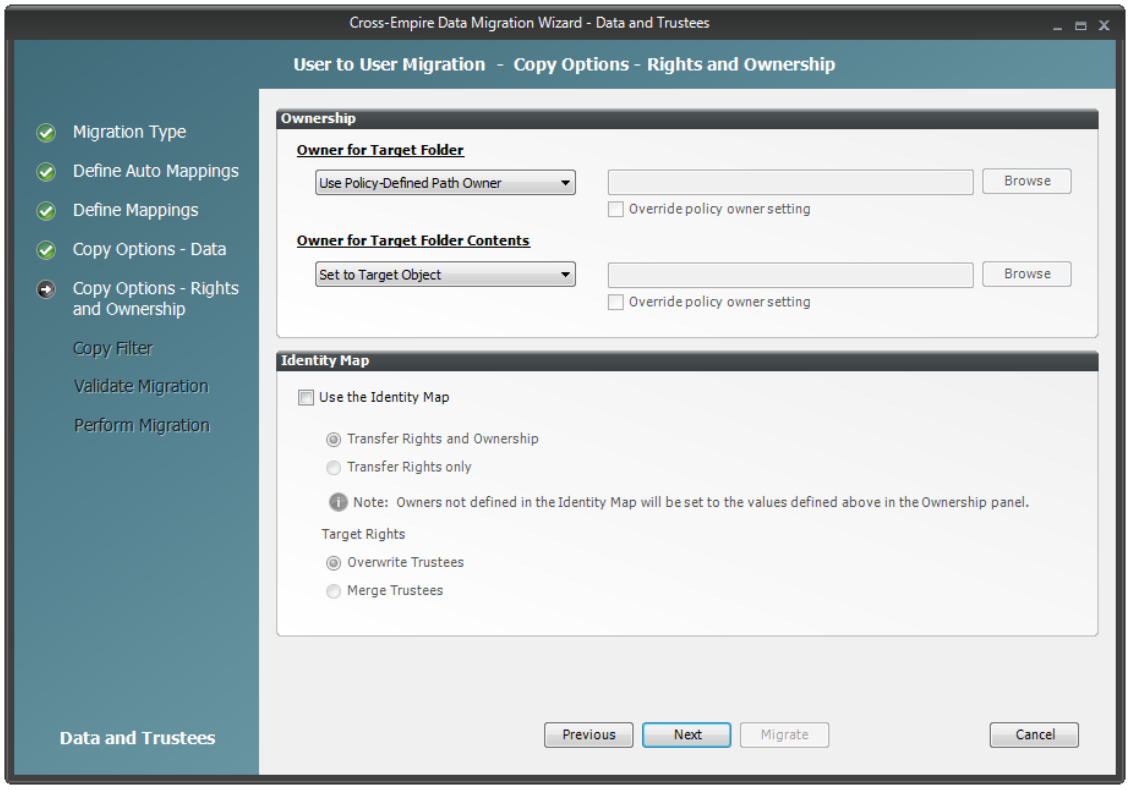
If you are migrating object data to an Active Directory container that does not have an associated Novell Storage Manager policy, deselect this check box.

Overwrite Options: Indicate what you want to take place when duplicate filenames are encountered in the source and target.

Directory Quota: Specify how quota settings from the source Novell file system should be applied after the migration.

Target Subfolder: If you want migrated data to be placed in a subfolder, select the *Use Subfolder* check box and specify the subfolder name in the field.

16 Click *Next*.



17 Fill in the following fields:

Owner for Target Folder: Use these settings to specify how ownership of the migrated folder is determined.

If you selected the *Require use of Policies for target objects* check box in the previous wizard page, only the *Use Policy-Defined Path Owner* and *Set Explicit Owner* options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Use Policy-Defined Path Owner:** Ownership of the files is determined according to the settings in the Novell Storage Manager policy associated with the container where the object is managed.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the *Override policy owner setting* check box.

Owner for Target Folder Contents: Use these settings to specify how ownership of the migrated folder contents is determined.

If you selected the *Require use of Policies for target objects* check box in the previous wizard page, only the *Set to Target Object* and *Set Explicit Owner* options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the *Override policy owner setting* check box.

Use the Identity Map: Selecting this check box indicates that you want Novell Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from eDirectory to Microsoft Active Directory.

- **Transfer Rights and Ownership:** Selecting this option indicates that you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you may not want to provide.
- **Transfer Rights Only:** Selecting this option indicates that you want to transfer only the file and folder security rights.
- **Overwrite Trustees:** Selecting this option indicates that you want any existing trustee assignments for a target file or folder, to be overridden by the established Novell eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Selecting this option indicates that you want the established Novell eDirectory trustee assignments merged with those of the target files or folders in Active Directory.

18 Click *Next*.

19 (Conditional) If you want to use a filter to include or exclude specific files, select the *Use Copy Filter* check box and click the *Add* button.

19a Fill in the following fields:

Description: Specify a description of the filter.

Action: From the drop-down menu, select either *Migrate* or *Ignore*, based on whether the filter specifies to migrate files or folders or to ignore them.

Files, Folders: Specify if the filter applies to files or folders.

Masks: List the file types to migrate or ignore.

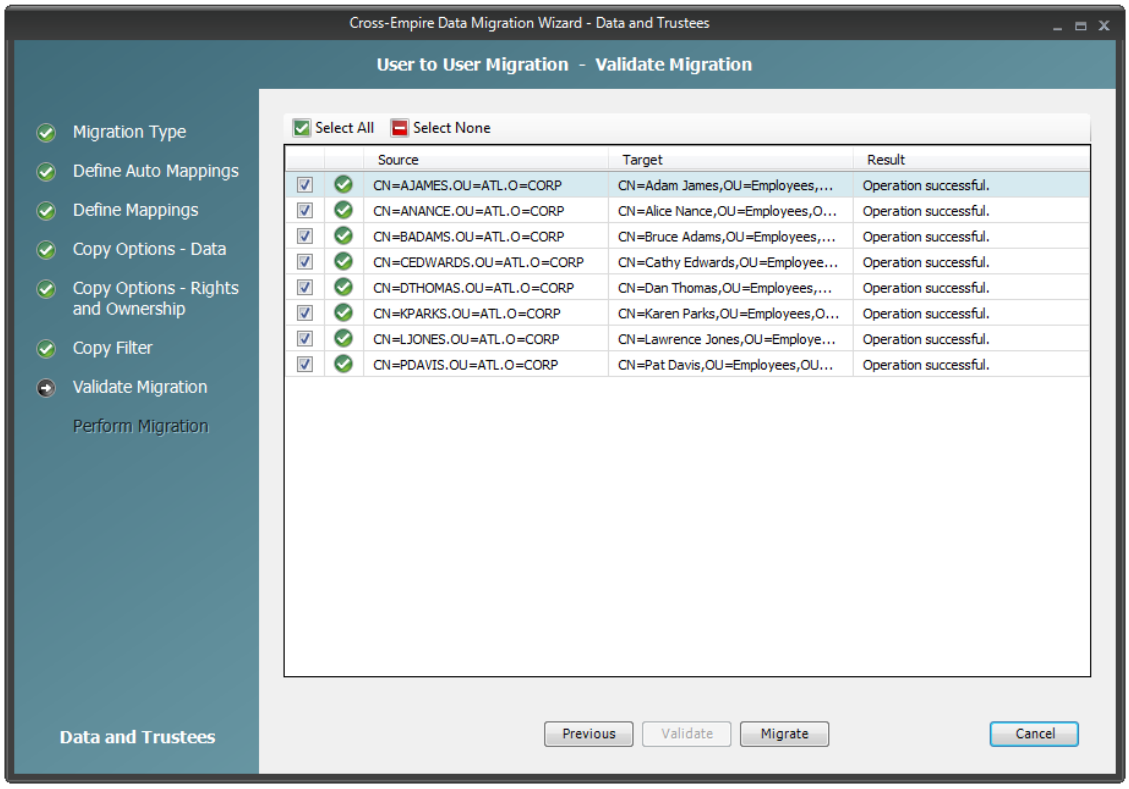
19b Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 5.5.8, "Setting Vault Rules," on page 49

19c Click *OK*.

20 Click *Validate*.

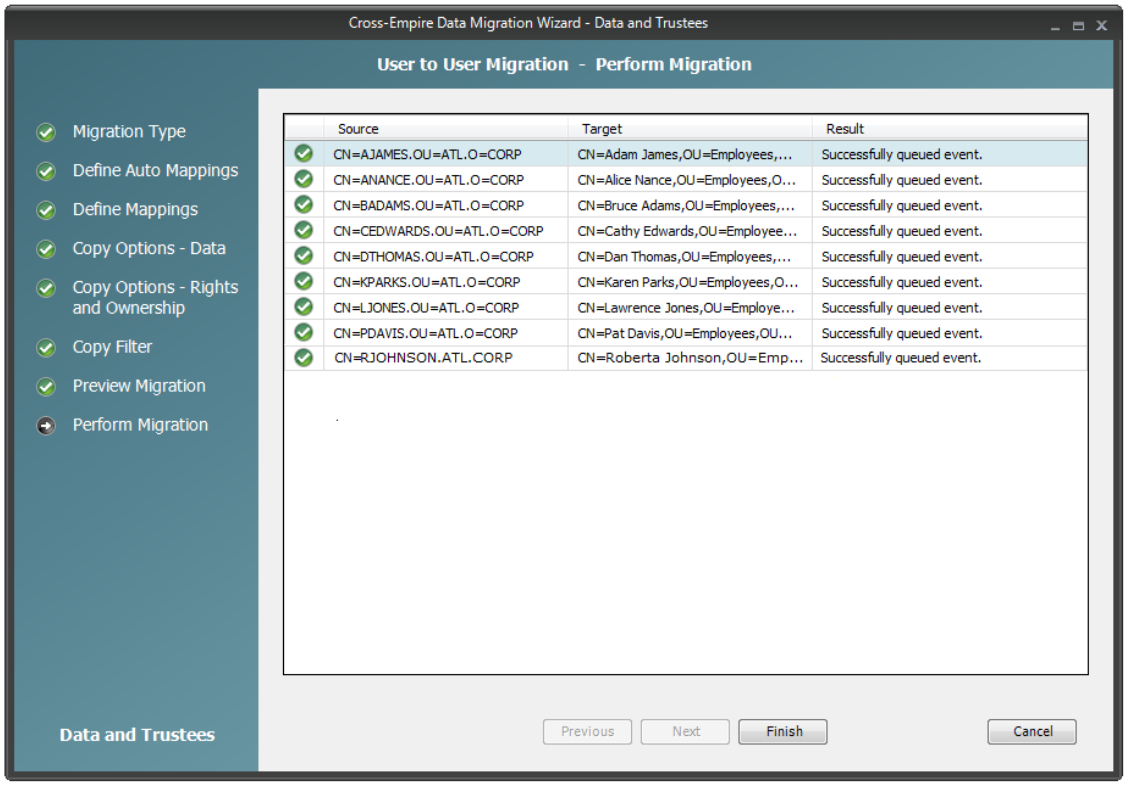
Validate shows the result of certain checks that can be run prior to the migration. The *Result* column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



21 (Conditional) Take any necessary action in the Active Directory target and then re-run the Data Migration Wizard.

22 Click *Migrate*.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click *Pending Events*. For more information on Pending Events, see Section 12.1.6, “Pending Events,” on page 219.



23 Click *Finish* to close the Data Migration Wizard.

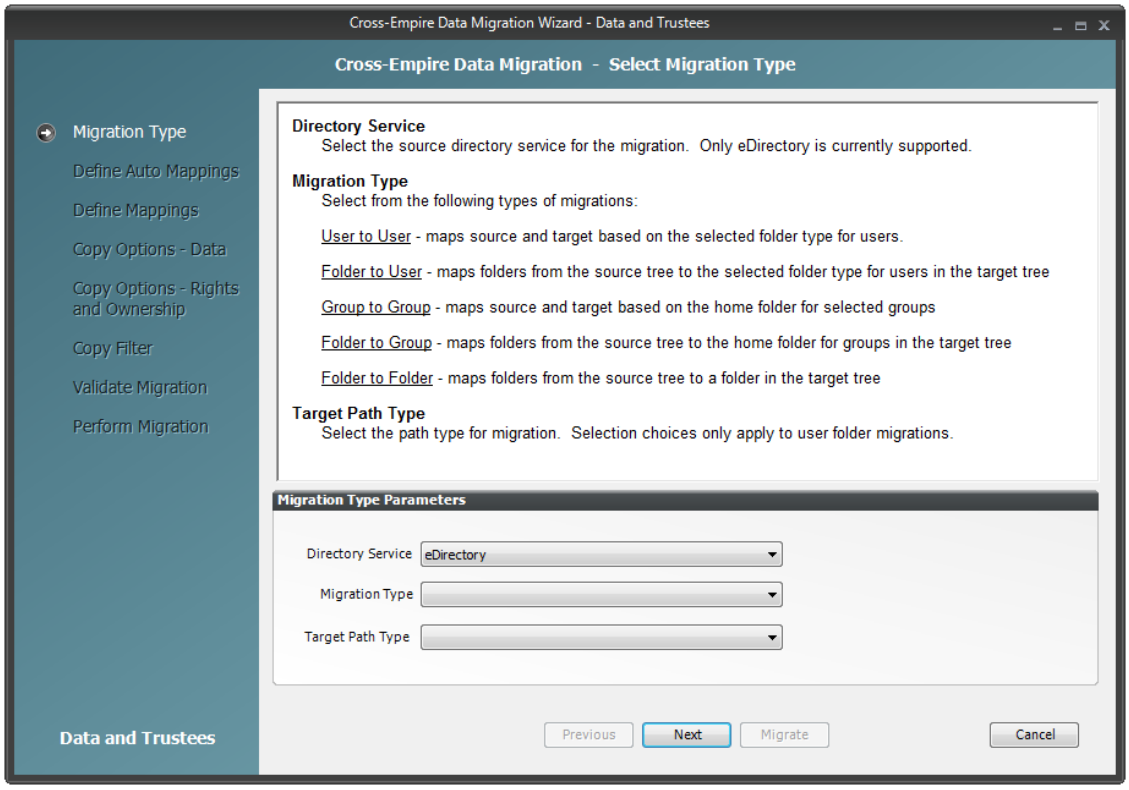
11.9 Performing a Folder to User Data Migration

1 Make sure you have completed the prerequisites and have created a migration proxy account. For more information on the prerequisites, see Section 11.3, “Prerequisites,” on page 115. For more information on creating a migration proxy account, see Section 11.4, “Creating the Migration Proxy Account,” on page 117.

2 In NSMAdmin, click the *Main* tab.

3 Click *Data Migration*.

4 Click *Migrate Data and Trustees*.

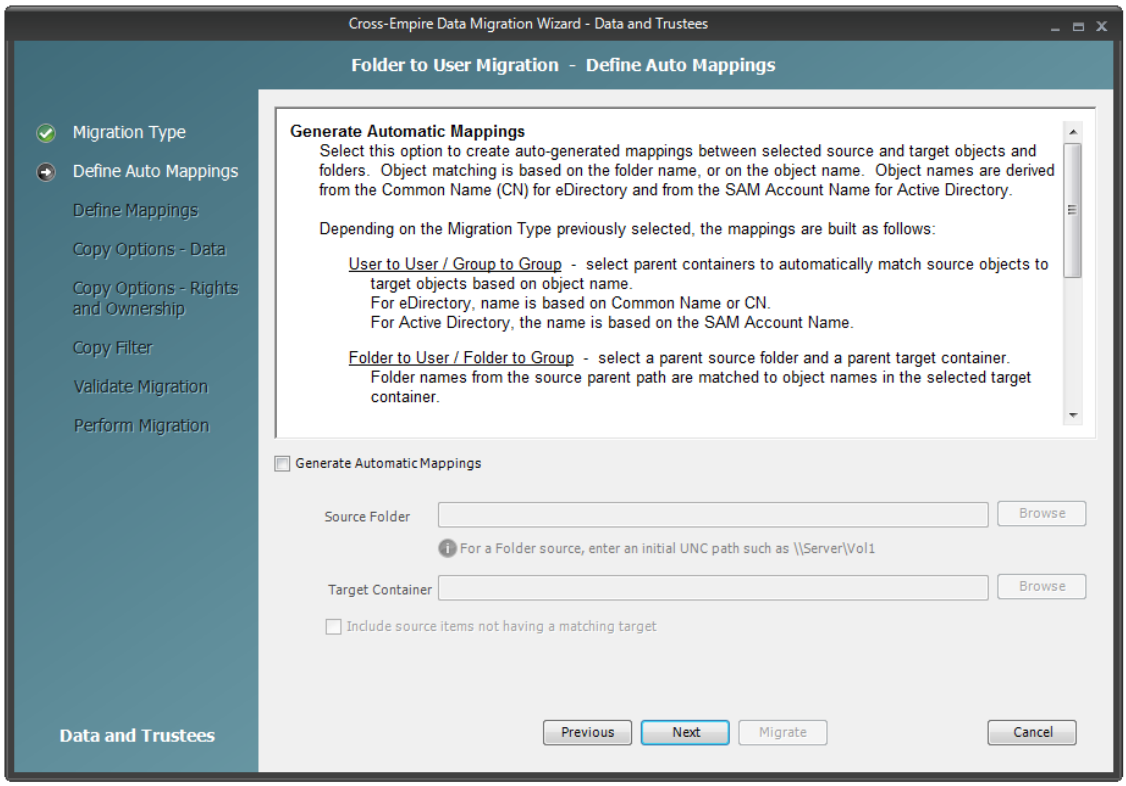


5 From the *Migration Type* drop-down menu, select *Folder to User.*

6 From the *Target Path Type* drop-down menu, select the target path type for the data that you will migrate.

For example, if you select *Home Folder*, the data is copied to each user's home folder path as defined in directory services.

7 Click *Next*.



8 Do one of the following:

- Fill in the following fields:

  Generate Automatic Mappings: If you are migrating a large number of folders, select this check box to activate the other fields.

  Source Folder: Specify an initial UNC path for a server and volume to browse.

  For example, `\\server_name\volume_name\` or `\\ip_address\volume_name`.

  After a path is entered, you can click the *Browse* button to browse to the folder you want.

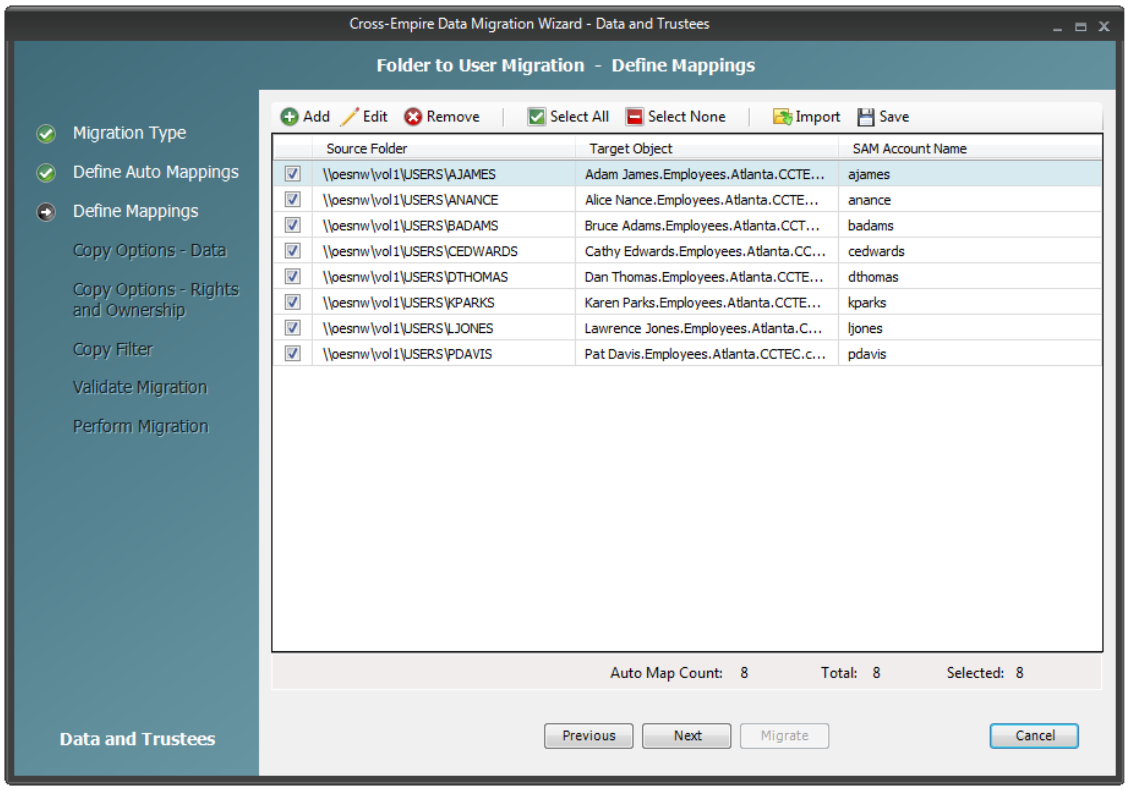
  Target Container: Browse to select the target container.

  Include source items not having a matching target: Indicate if you want to identify source data not having a matching target.

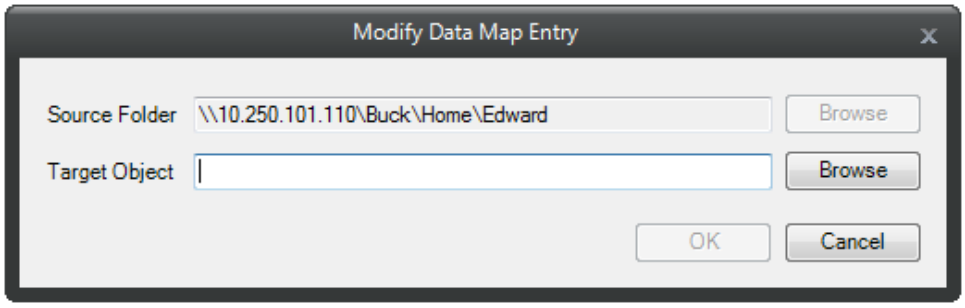
- If you are migrating only a few users, use the *Add* button on the next wizard page to add the users individually.

9 Click *Next*.

The Data Migration Wizard attempts to match the names of the subfolders of the source path with the SAM (Security Accounts Manager) Account Names in the Active Directory target. If there is a match, the listed folder in the *Source Folder* field is selected and a corresponding match is listed in the Target Object column.



10 Specify a target object for each source object that is not automatically matched by double-clicking the name to bring up the Modify Data Map Entry dialog box.



11 Click *Browse*, specify the target object, then click *OK*.

The target object is displayed in the Target Object column.

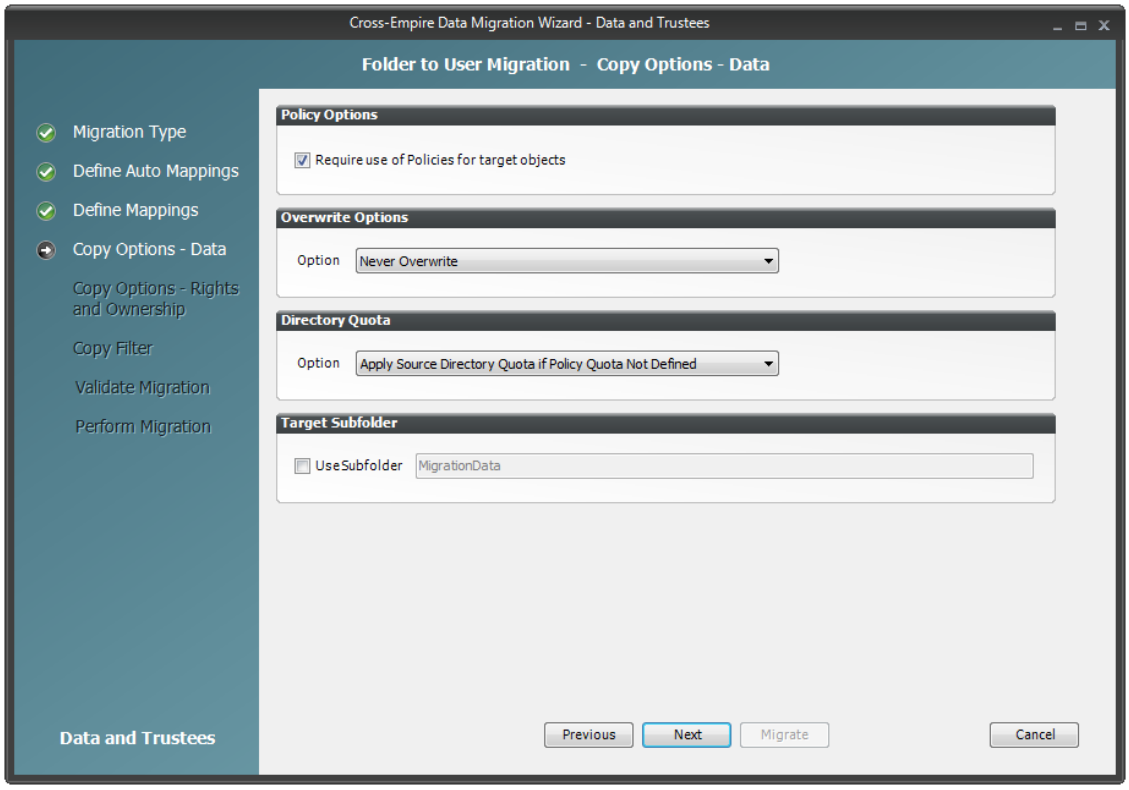
12 Click the check box corresponding to the listing with the new target.

13 Repeat Step 10 and Step 11 to specify all target objects that are not listed.

To change the specified target object, use the *Edit* button.

To add an object to the Source Object column, use the *Add* button.

14 When all of the objects you want to migrate are selected and have an associated target object, click *Next*.



15 Fill in the following fields:

Require use of Policies for target objects: If you are migrating data for objects to an Active Directory container that has an associated Novell Storage Manager policy, leave this check box selected.

If this check box is selected and there is no associated Novell Storage Manager policy, the object's data is not eligible for migration.

Additionally, if you are migrating a folder and the target user is not currently managed by an associated policy, but the user does have a policy that would apply to it, Novell Storage Manager automatically applies that policy to the target user.

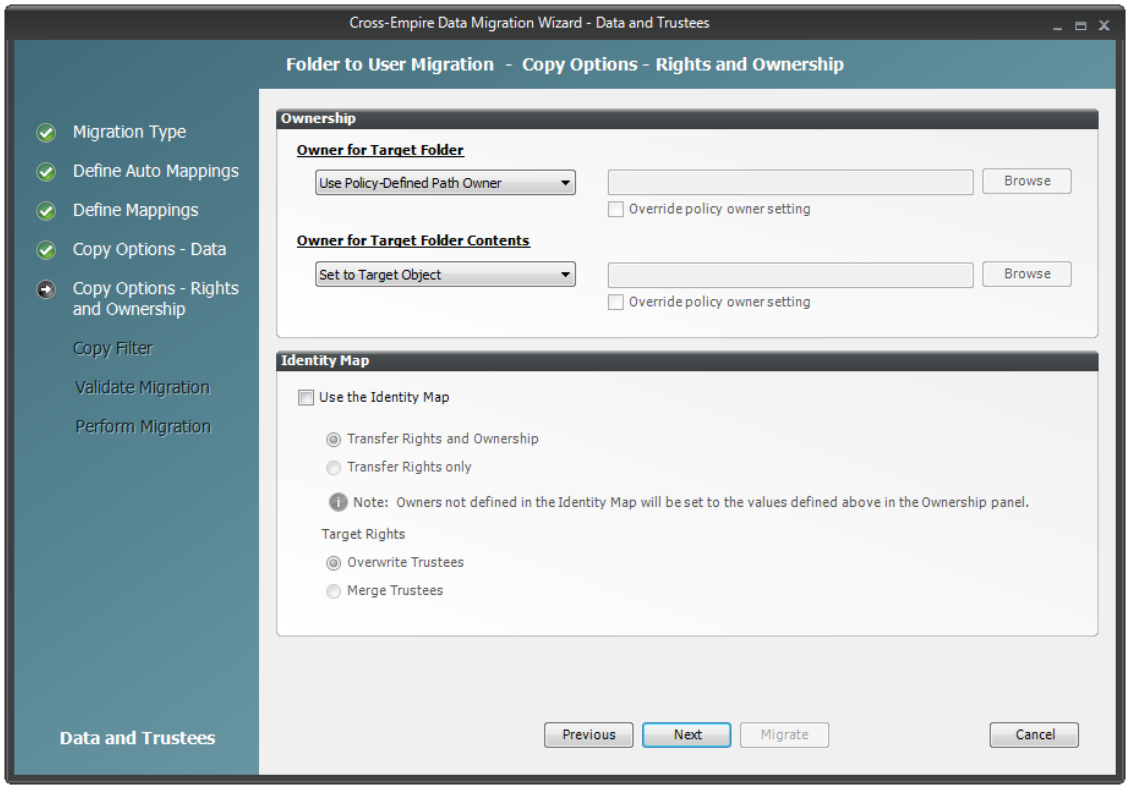
If you are migrating folders to an Active Directory container that does not have an associated Novell Storage Manager policy, deselect this check box.

Overwrite Options: Indicate what you want to take place when duplicate filenames are encountered in the source and target.

Directory Quota: Specify how quota settings from the source Novell file system should be applied after the migration.

Target Subfolder: If you want migrated data to be placed in a subfolder, select the *Use subfolder* check box and specify the subfolder name in the field.

16 Click *Next*.



17 Fill in the following fields:

Owner for Target Folder: Use these settings to specify how ownership of the migrated folder is determined.

If you selected the *Require use of Policies for target objects* check box in the previous wizard page, only the *Use Policy-Defined Path Owner* and *Set Explicit Owner* options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Use Policy-Defined Path Owner:** Ownership of the files is determined according to the settings in the Novell Storage Manager policy associated with the container where the object is managed.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the *Override policy owner setting* check box.

Owner for Target Folder Contents: Use these settings to specify how ownership of the migrated folder contents is determined.

If you selected the *Require use of Policies for target objects* check box in the previous wizard page, only the *Set to Target Object*, and *Set Explicit Owner* options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the *Override policy owner setting* check box.

Use the Identity Map: Selecting this check box indicates that you want Novell Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from eDirectory to Microsoft Active Directory.

- **Transfer Rights and Ownership:** Selecting this option indicates that you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you may not want to provide.
- **Transfer Rights Only:** Selecting this option indicates that you want to transfer only the file and folder security rights.
- **Overwrite Trustees:** Selecting this option indicates that you want any existing trustee assignments for a target file or folder, to be overridden by the established Novell eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Selecting this option indicates that you want the established Novell eDirectory trustee assignments merged with those of the target files or folders in Active Directory.

18 Click *Next*.

19 (Conditional) If you want to use a filter to include or exclude specific files, select the *Use Copy Filter* check box and click the *Add* button.

19a Fill in the following fields:

Description: Specify a description of the filter.

Action: From the drop-down menu, select either *Migrate* or *Ignore*, based on whether the filter specifies to migrate files or folders or to ignore them.

Files, Folders: Specify if the filter applies to files or folders.

Masks: List the file types to migrate or ignore.

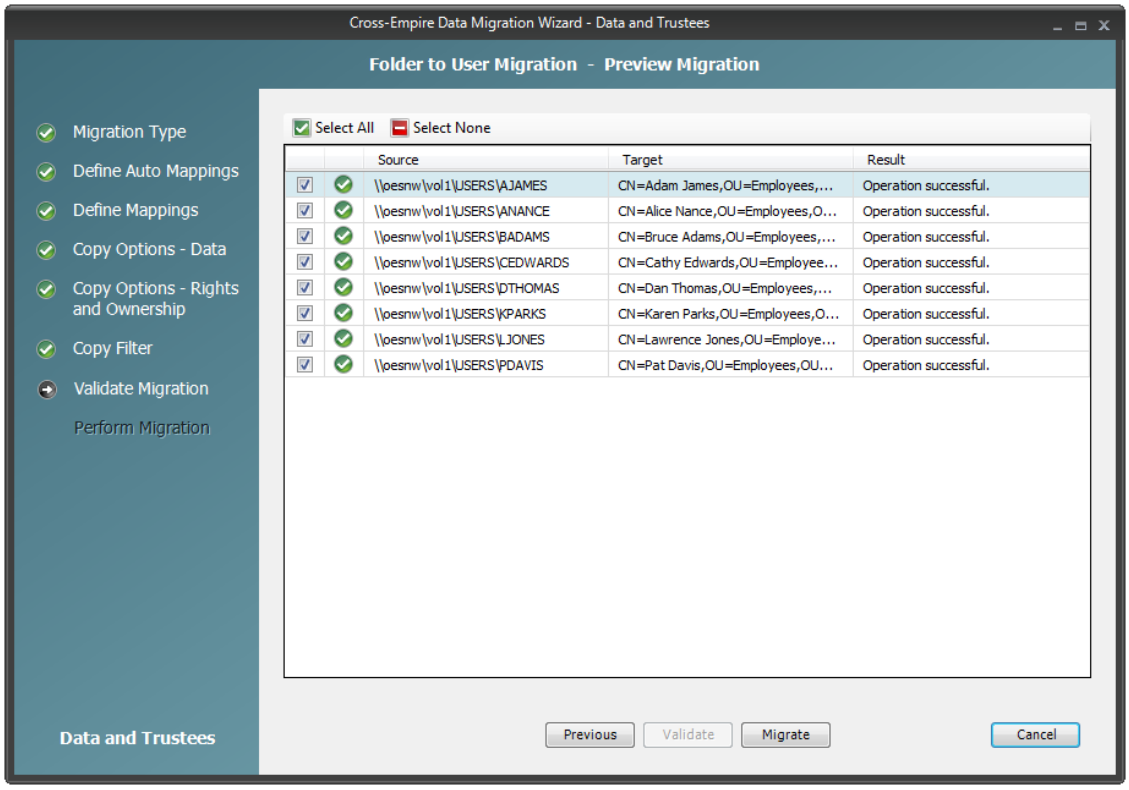
19b Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 5.5.8, "Setting Vault Rules," on page 49.

19c Click *OK*.

20 Click *Validate*.

Validate shows the result of certain checks that can be run prior to the migration. The *Result* column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



21 (Conditional) Take any necessary action in the Active Directory target and then re-run the Data Migration Wizard.

22 Click *Migrate*.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click *Pending Events*. For more information on Pending Events, see Section 12.1.6, “Pending Events,” on page 219.

23 Click *Finish* to close the Data Migration Wizard.

11.10 Performing a Group to Group Data Migration

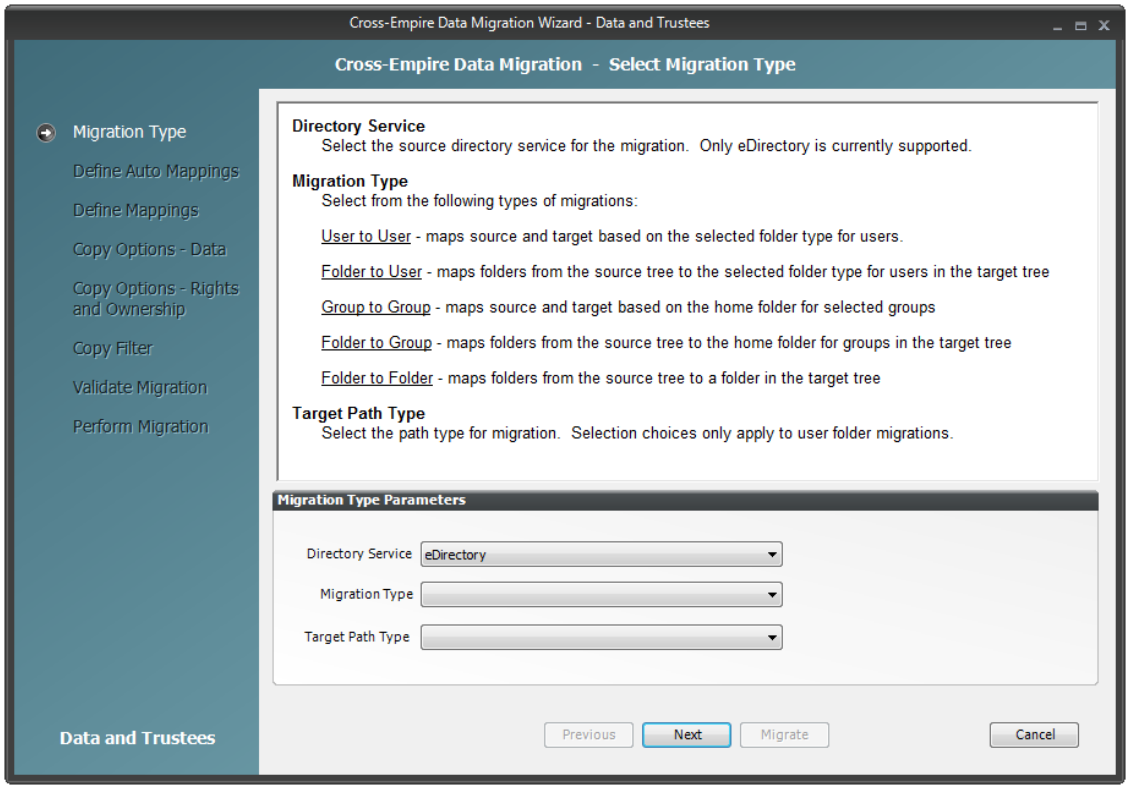
IMPORTANT: This migration option can be performed only if the source volume from which you are migrating has group home folders being managed by Novell Storage Manager for eDirectory group-based collaborative storage policies.

1 Make sure you have completed the prerequisites and have created a migration proxy account. For more information on the prerequisites, see Section 11.3, “Prerequisites,” on page 115. For more information on creating a migration proxy account, see Section 11.4, “Creating the Migration Proxy Account,” on page 117.

2 In NSMAdmin, click the *Main* tab.

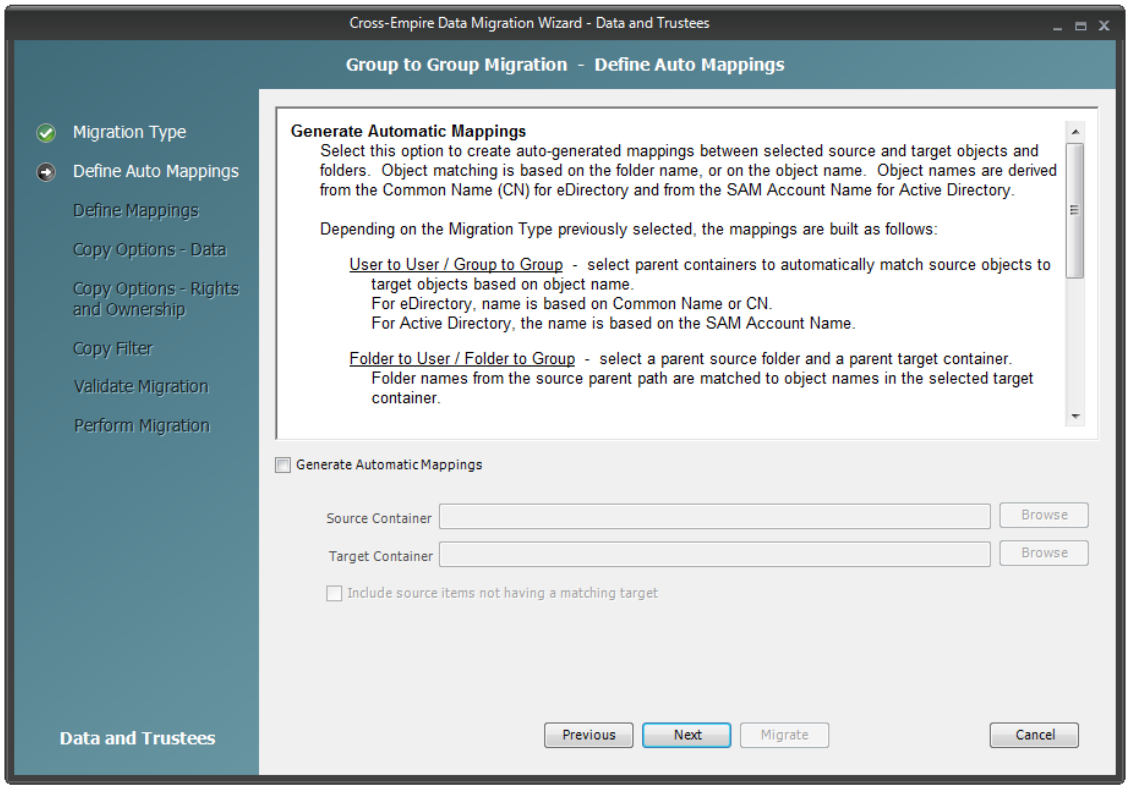
3 Click *Data Migration*.

4 Click *Migrate Data and Trustees*.



5 From the *Migration Type* drop-down menu, select *Group to Group*.

6 Click *Next*.



7 Do one of the following:

- Fill in the following fields:

  Generate Automatic Mappings: If you are migrating a large number of folders, select this check box to activate the other fields.

  Source Container: Browse to select the source container.

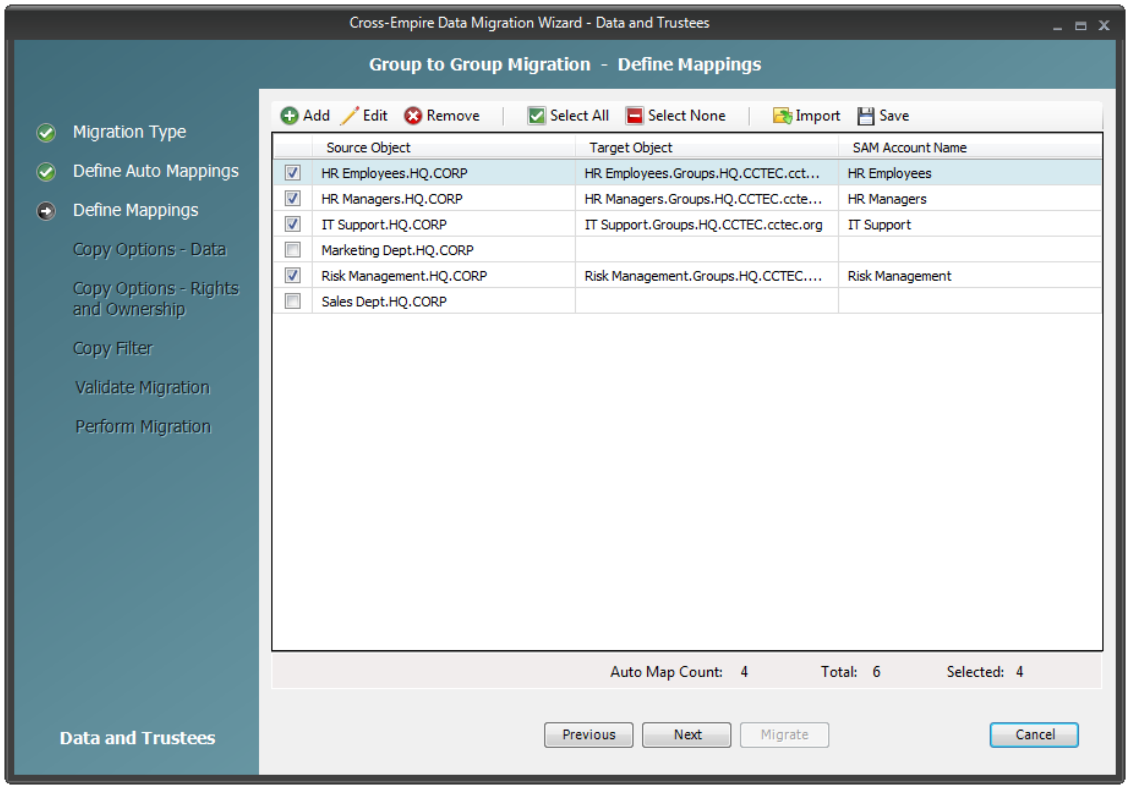
  Target Container: Browse to select the target container.

  Include source items not having a matching target: Indicate if you want to identify source data not having a matching target.

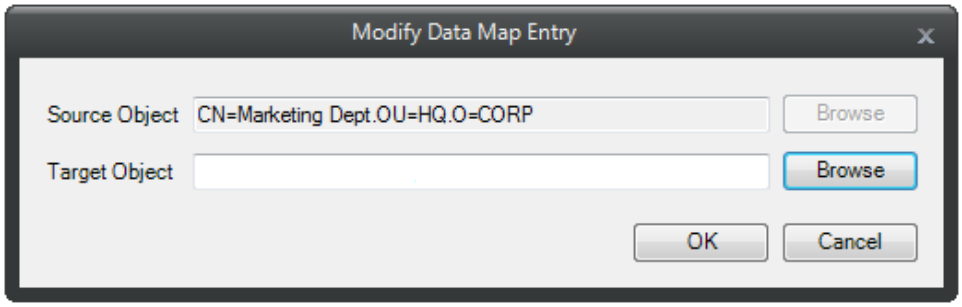
- If you are migrating only a few groups, use the *Add* button in the next wizard page to add the groups individually.

8 Click *Next*.

The Data Migration Wizard attempts to match the Common Names (CN) of objects from the eDirectory source with the SAM (Security Accounts Manager) Account Names in the Active Directory target. If there is a match, the listed object in the *Source Object* field is selected and a corresponding match is listed in the Target Object column.



9 Specify a target object for each source object that is not automatically matched by double-clicking the name to bring up the Modify Data Map Entry dialog box.



10 Click *Browse*, specify the target object, then click *OK*.

The target object is displayed in the Target Object column.

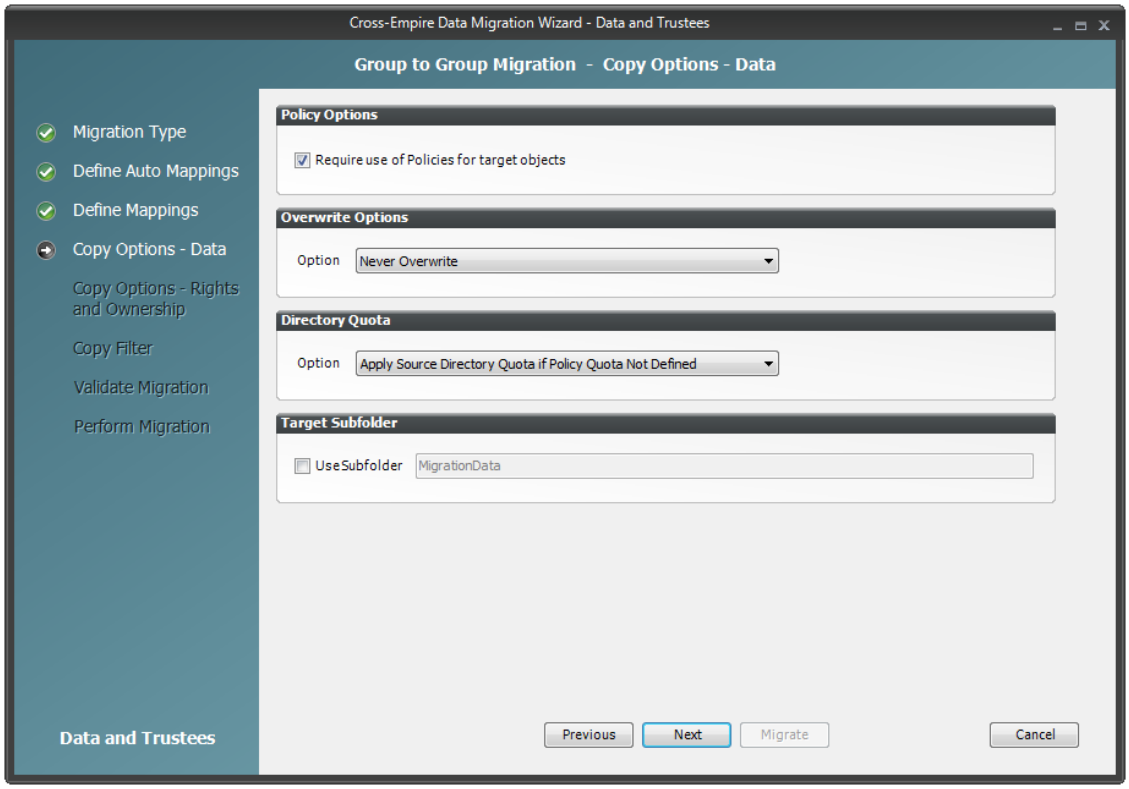
11 Click the check box corresponding to the listing with the new target.

12 Repeat Step 9 and Step 10 to specify all target objects that are not listed.

To change the specified target object, use the *Edit* button.

To add an object to the Source Object column, use the *Add* button.

13 When all of the objects you want to migrate are selected and have an associated target object, click *Next*.



14 Fill in the following fields:

Require use of Policies for target objects: If you are migrating data for objects to an Active Directory container that has an associated Novell Storage Manager policy, leave this check box selected.

If this check box is selected and there is no associated Novell Storage Manager policy, the object's data is not eligible for migration.

Additionally, if you are migrating a group folder and the target group is not currently managed by an associated policy, but the group does have a policy that would apply to it, Novell Storage Manager will automatically apply that policy to the target group.

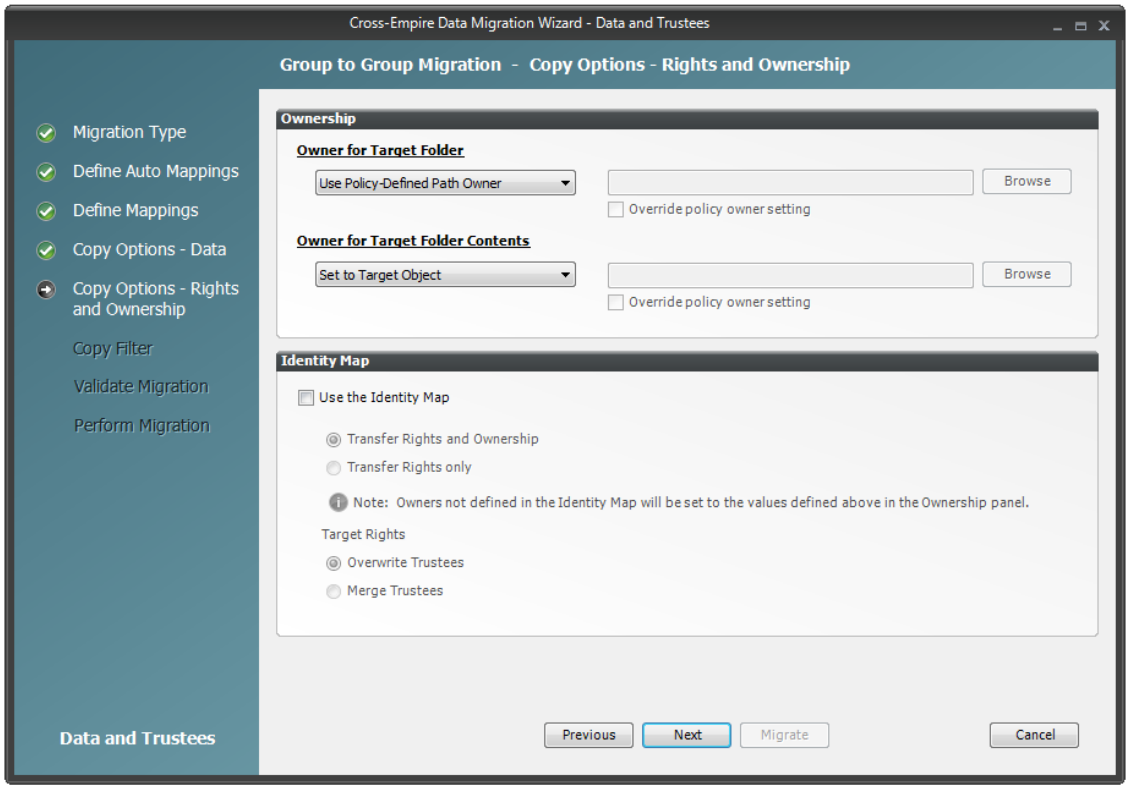
If you are migrating group folders to an Active Directory container that does not have an associated Novell Storage Manager policy, deselect this check box.

Overwrite Options: Indicate what you want to take place when duplicate filenames are encountered in the source and target.

Directory Quota: Specify how quota settings from the source Novell file system should be applied after the migration.

Target Subfolder: If you want migrated data to be placed in a subfolder, select the *Use subfolder* check box and specify the subfolder name in the field.

15 Click *Next*.



16 Fill in the following fields:

Owner for Target Folder: Use these settings to specify how ownership of the migrated folder is determined.

If you selected the *Require use of Policies for target objects* check box in the previous wizard page, only the *Use Policy-Defined Path Owner* and *Set Explicit Owner* options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Use Policy-Defined Path Owner:** Ownership of the files is determined according to the settings in the Novell Storage Manager policy associated with the container where the object is managed.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the *Override policy owner setting* check box.

Owner for Target Folder Contents: Use these settings to specify how ownership of the migrated folder contents is determined.

If you selected the *Require use of Policies for target objects* check box in the previous wizard page, only the *Set to Target Object* and *Set Explicit Owner* options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the *Override policy owner setting* check box.

Use the Identity Map: Selecting this check box indicates that you want Novell Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from eDirectory to Microsoft Active Directory.

- **Transfer Rights and Ownership:** Selecting this option indicates that you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you may not want to provide.
- **Transfer Rights Only:** Selecting this option indicates that you want to transfer only the file and folder security rights.
- **Overwrite Trustees:** Selecting this option indicates that you want any existing trustee assignments for a target file or folder, to be overridden by the established Novell eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Selecting this option indicates that you want the established Novell eDirectory trustee assignments merged with those of the target files or folders in Active Directory.

17 Click *Next*.

18 (Conditional) If you want to use a filter to include or exclude specific files, select the *Use Copy Filter* check box and click the *Add* button.

18a Fill in the following fields:

Description: Specify a description of the filter.

Action: From the drop-down menu, select either *Migrate* or *Ignore*, based on whether the filter specifies to migrate files or folders or to ignore them.

Files, Folders: Specify if the filter applies to files or folders.

Masks: List the file types to migrate or ignore.

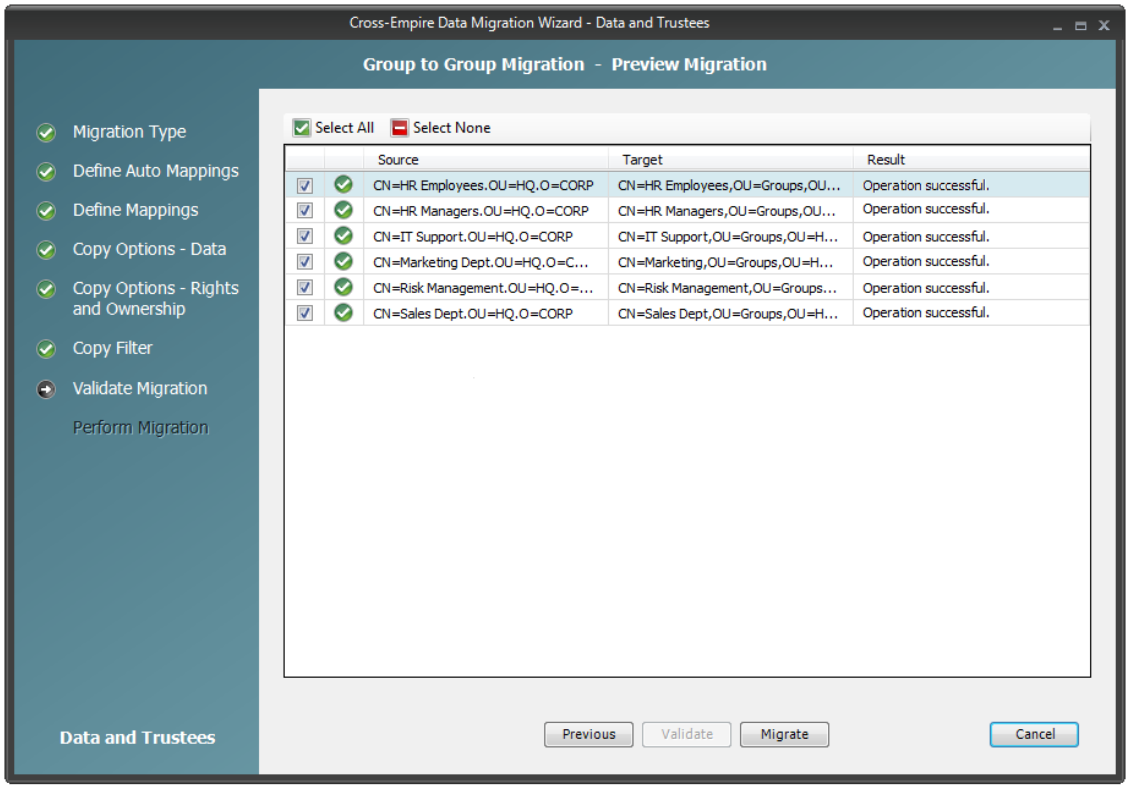
18b Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 5.5.8, "Setting Vault Rules," on page 49.

18c Click *OK*.

19 Click *Validate*.

Validate shows the result of certain checks that can be run prior to the migration. The *Result* column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



20 (Conditional) Take any necessary action in the Active Directory target and then re-run the Data Migration Wizard.

21 Click *Migrate*.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click *Pending Events*. For more information on Pending Events, see Section 12.1.6, "Pending Events," on page 219.

22 Click *Finish* to close the Data Migration Wizard.

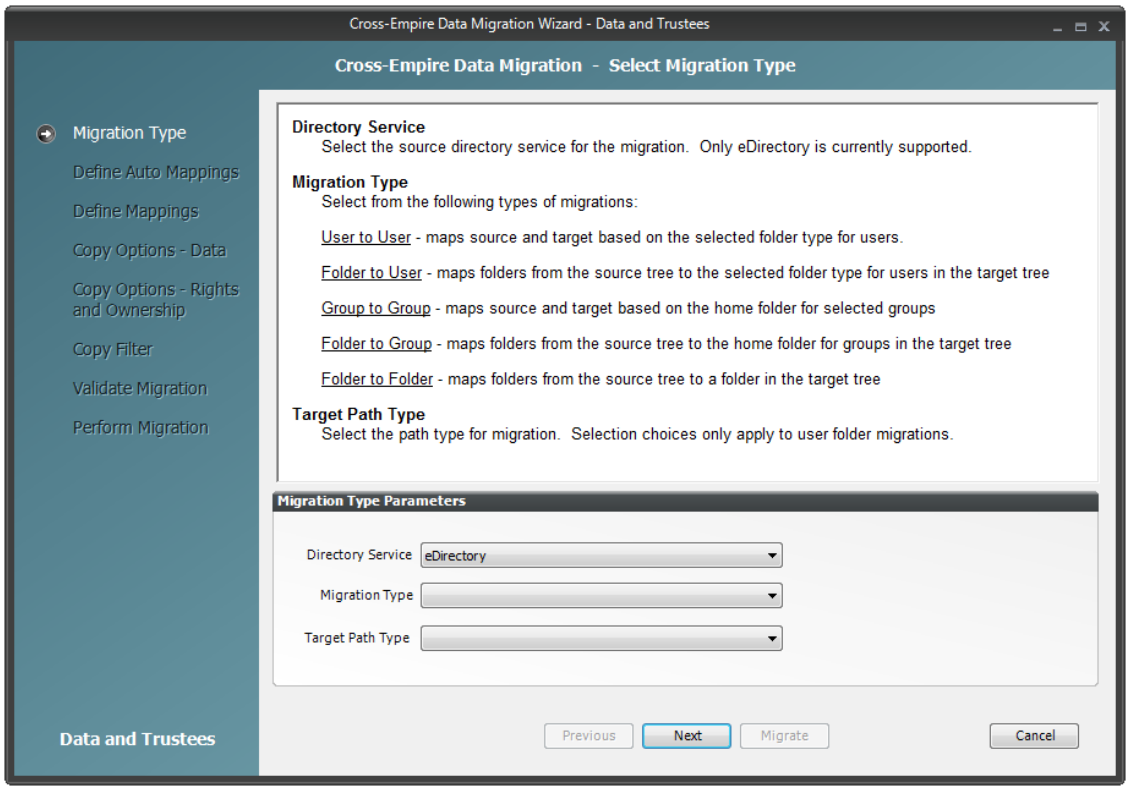
11.11 Performing a Folder to Group Migration

1 Make sure you have completed the prerequisites and have created a migration proxy account. For more information on the prerequisites, see Section 11.3, "Prerequisites," on page 115. For more information on creating a migration proxy account, see Section 11.4, "Creating the Migration Proxy Account," on page 117.

2 In NSMAdmin, click the *Main* tab.

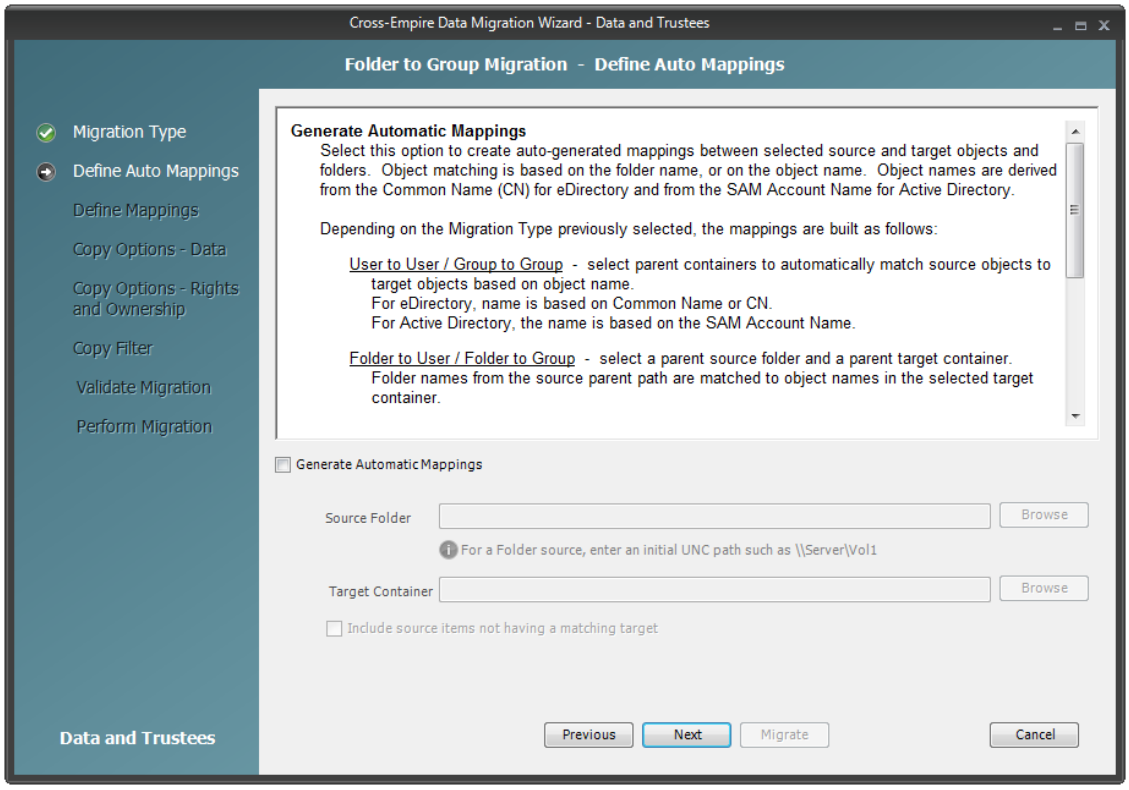
3 Click *Data Migration*.

4 Click *Migrate Data and Trustees*.



5 From the *Migration Type* drop-down menu, select *Folder to Group*.

6 Click *Next*.



7 Do one of the following:

- Fill in the following fields:

  Generate Automatic Mappings: If you are migrating a large number of folders, select this check box to activate the other fields.

  Source Folder: Specify an initial UNC path for a server and volume to browse.

  For example `\\server_name\volume_name\` or `\\ip_address\volume_name`.

  After a path is entered, you can click the *Browse* button to browse to the folder you want.

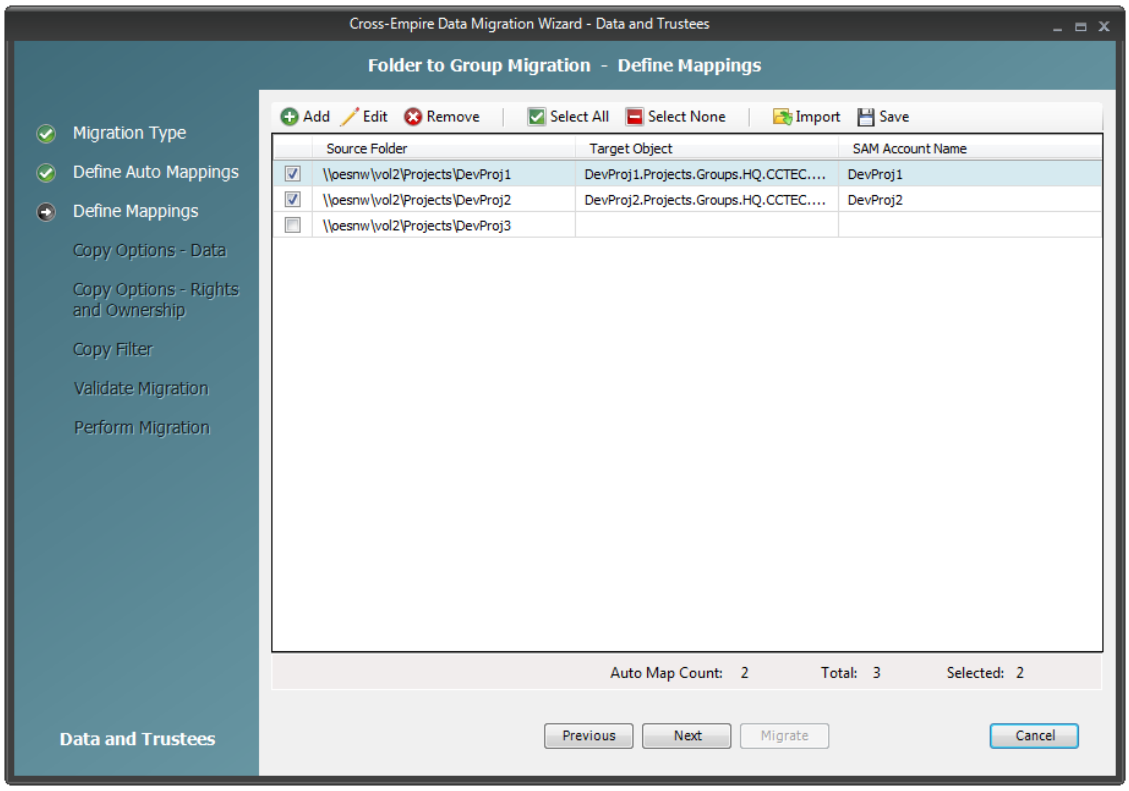
  Target Container: Browse to select the target container.

  Include source items not having a matching target: Indicate if you want to identify source data not having a matching target.

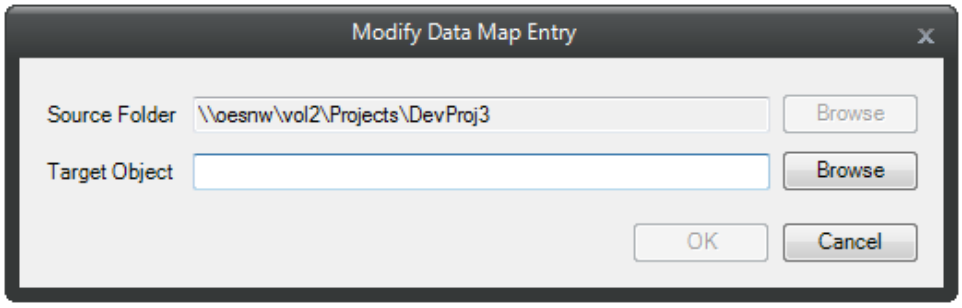
- If you are migrating only a few users, use the *Add* button on the next wizard page to add the users individually.

8 Click *Next*.

The Data Migration Wizard attempts to match the names of subfolders of the source path with the SAM (Security Accounts Manager) Account Names of groups in the Active Directory target. If there is a match, the listed folder in the *Source Folder* field is selected and a corresponding match is listed in the Target Object column.



9 Specify a target object for each source object that is not automatically matched by double-clicking the name to bring up the Modify Data Map Entry dialog box.



10 Click *Browse*, specify the target object, then click *OK*.

The target object is displayed in the Target Object column.

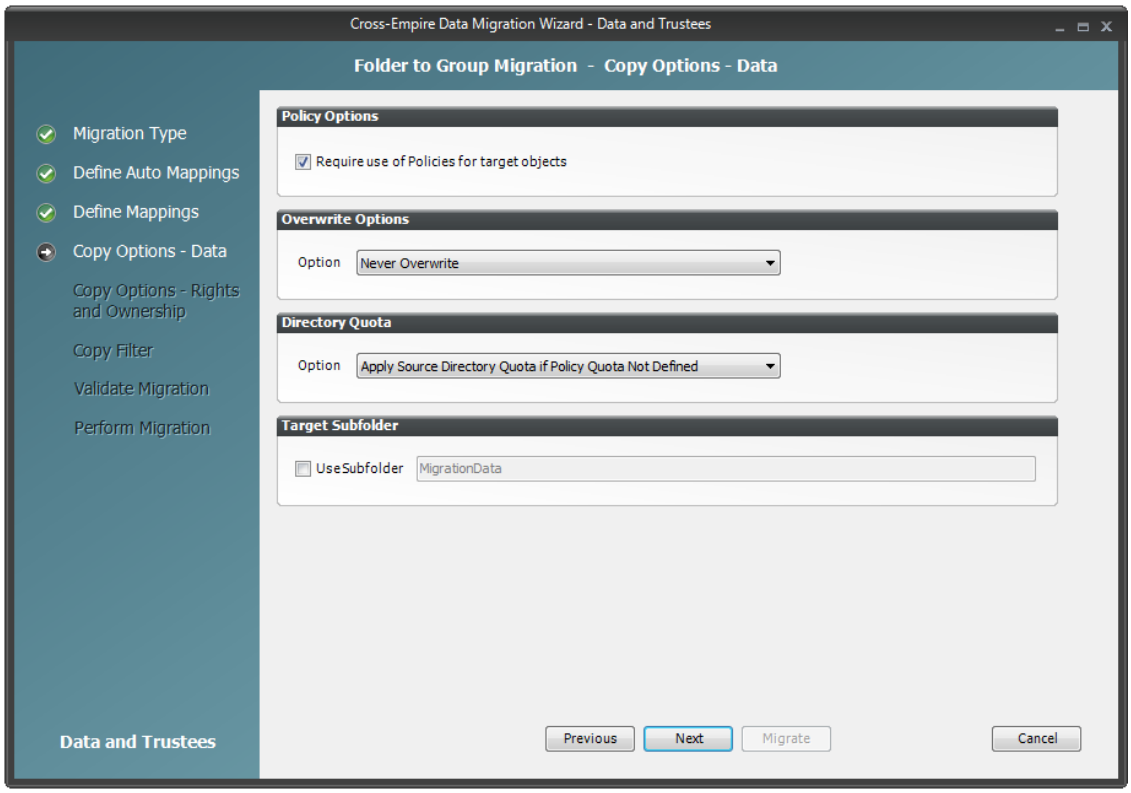
11 Click the check box corresponding to the listing with the new target.

12 Repeat Step 9 and Step 10 to specify all target objects that are not listed.

To change the specified target object, use the *Edit* button.

To add an object to the Source Object column, use the *Add* button.

13 When all of the objects you want to migrate are selected and have an associated target object, click *Next*.



14 Fill in the following fields:

Require use of Policies for target objects: If you are migrating data for objects to an Active Directory container that has an associated Novell Storage Manager policy, leave this check box selected.

If this check box is selected and there is no associated Novell Storage Manager policy, the object's data is not eligible for migration.

Additionally, if you are migrating a folder and the target group is not currently managed by an associated policy, but the group does have a policy that would apply to it, Novell Storage Manager automatically applies that policy to the target group.

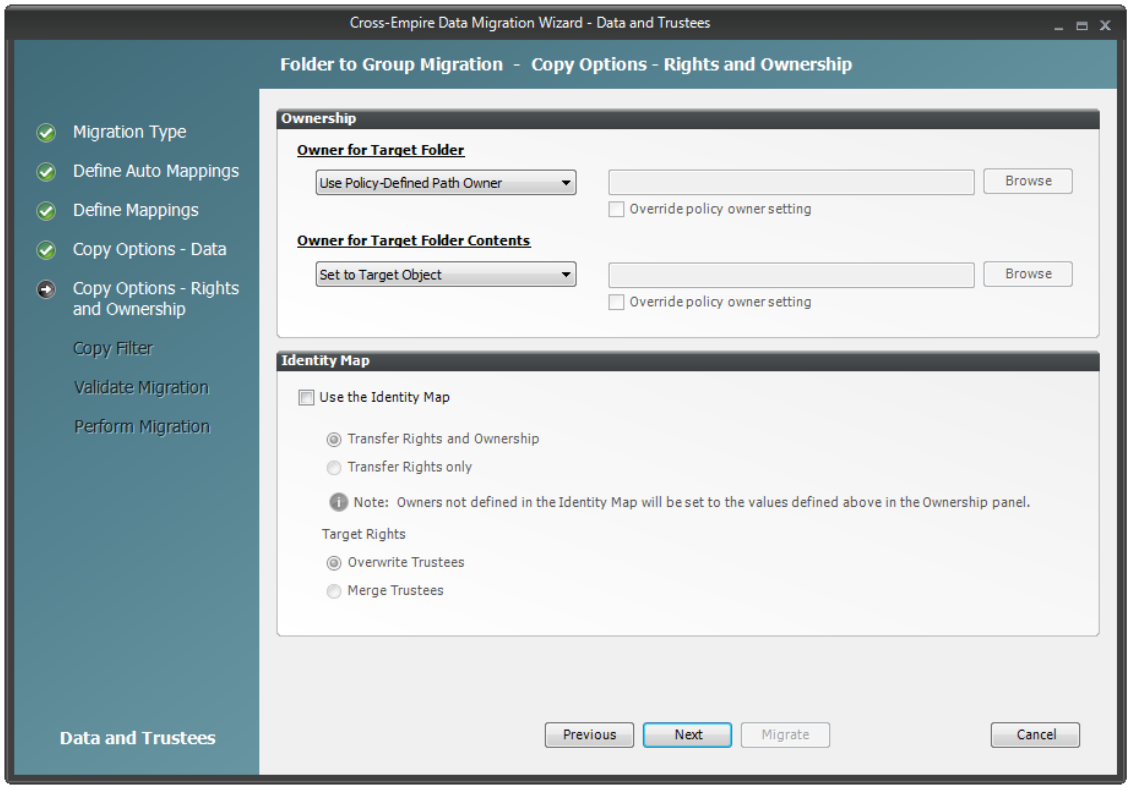
If you are migrating folders to an Active Directory container that does not have an associated Novell Storage Manager policy, deselect this check box.

Overwrite Options: Indicate what you want to take place when duplicate filenames are encountered in the source and target.

Directory Quota: Specify how quota settings from the source Novell file system should be applied after the migration.

Target Subfolder: If you want migrated data to be placed in a subfolder, select the *Use subfolder* check box and specify the subfolder name in the field.

15 Click *Next*.



16 Fill in the following fields:

Owner for Target Folder: Use these settings to specify how ownership of the migrated folder is determined.

If you selected the *Require use of Policies for target objects* check box in the previous wizard page, only the *Use Policy-Defined Path Owner* and *Set Explicit Owner* options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Use Policy-Defined Path Owner:** Ownership of the files is determined according to the settings in the Novell Storage Manager policy associated with the container where the object is managed.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the *Override policy owner setting* check box.

Owner for Target Folder Contents: Use these settings to specify how ownership of the migrated folder contents is determined.

If you selected the *Require use of Policies for target objects* check box in the previous wizard page, only the *Set to Target Object* and *Set Explicit Owner* options are available on the drop-down menu.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set to Target Object:** Specifies the target object as the owner of the migrated files. If the policy specifies a different owner, the policy's owner is applied.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder, unless the policy specifies another object as the owner. To override the policy's configuration, select the *Override policy owner setting* check box.

Use the Identity Map: Selecting this check box indicates that you want Novell Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from eDirectory to Microsoft Active Directory.

- **Transfer Rights and Ownership:** Selecting this option indicates that you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you may not want to provide.
- **Transfer Rights Only:** Selecting this option indicates that you want to transfer only the file and folder security rights.
- **Overwrite Trustees:** Selecting this option indicates that you want any existing trustee assignments for a target file or folder, to be overridden by the established Novell eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Selecting this option indicates that you want the established Novell eDirectory trustee assignments merged with those of the target files or folders in Active Directory.

17 Click *Next*.

18 (Conditional) If you want to use a filter to include or exclude specific files, select the *Use Copy Filter* check box and click the *Add* button.

18a Fill in the following fields:

Description: Specify a description of the filter.

Action: From the drop-down menu, select either *Migrate* or *Ignore*, based on whether the filter specifies to migrate files or folders or to ignore them.

Files, Folders: Specify if the filter applies to files or folders.

Masks: List the file types to migrate or ignore.

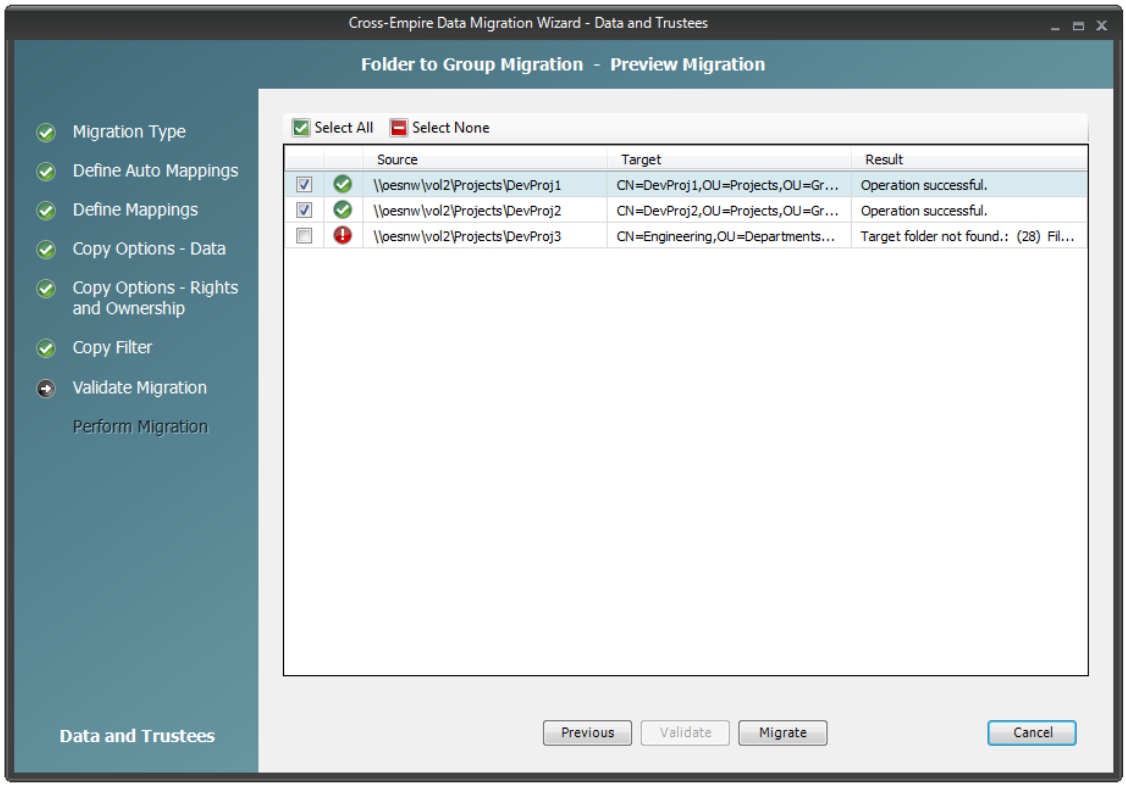
18b Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 5.5.8, "Setting Vault Rules," on page 49.

18c Click *OK*.

19 Click *Validate*.

Validate shows the result of certain checks that can be run prior to the migration. The *Result* column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



20 (Conditional) Take any necessary action in the Active Directory target and then re-run the Data Migration Wizard.

21 Click *Migrate*.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click *Pending Events*. For more information on Pending Events, see Section 12.1.6, "Pending Events," on page 219.

22 Click *Finish* to close the Data Migration Wizard.

11.12 Performing a Folder to Folder Migration

A folder to folder migration has flexible target specification options that are not available in the previous migration options. When you perform a folder to folder migration, you can either specify an existing target folder or create a target folder in the Data Migration Wizard. You can also decide whether to migrate all of the files at once, or skip some files and migrate them later.

The preferred time for performing a folder to folder migration is when all files located in the folders to be migrated are closed, such as during the weekend. However, if you have terabytes of data to migrate, some folder to folder migrations might need to be started during the week, when some of the files intended for migration are open. In cases such as these, we recommend a two-phased folder to folder migration:

Migrating Closed Files: While users are still logged in, you migrate all of the closed files on your network. This will be the vast majority of your network files. Because the *Skip Open Files* option is selected, open files are not migrated, but the filenames and paths of all of the open files are logged in a text file.

NOTE: If you perform a Cross-Empire Data Migration when all users are logged off, you do not need to migrate skipped files.

Migrating Skipped, New, and Modified Files: After having all users log off, migrate the skipped files, migrate the new and modified files, then compare the files on the source and target servers to verify that everything migrated correctly.

- Section 11.12.1, "Migrating to an Existing Target Folder," on page 167
- Section 11.12.2, "Creating a Target Folder in the Data Migration Wizard," on page 196

11.12.1 Migrating to an Existing Target Folder

- "Migrating Closed Files" on page 167
- "Migrating Skipped Files" on page 175
- "Creating a Job File to Scan the Source Server for New or Modified Folders and Files" on page 179
- "Using the NovScan NLM to Run the Job File" on page 181
- "Migrating the New and Modified Files" on page 182
- "Creating a Job File to Scan the Source Server for All Folders and Files" on page 186
- "Using the NovScan NLM to Run the Job File" on page 188
- "Scanning the Target Server for All Folders and Files" on page 189
- "Comparing the Source and Target Lists" on page 193

Migrating Closed Files

1 Make sure you have completed the prerequisites and have created a migration proxy account.

For more information on the prerequisites, see Section 11.3, "Prerequisites," on page 115. For more information on creating a migration proxy account, see Section 11.4, "Creating the Migration Proxy Account," on page 117.

2 (Conditional) If you want to migrate closed files now and skip some files to migrate later, complete the following steps:

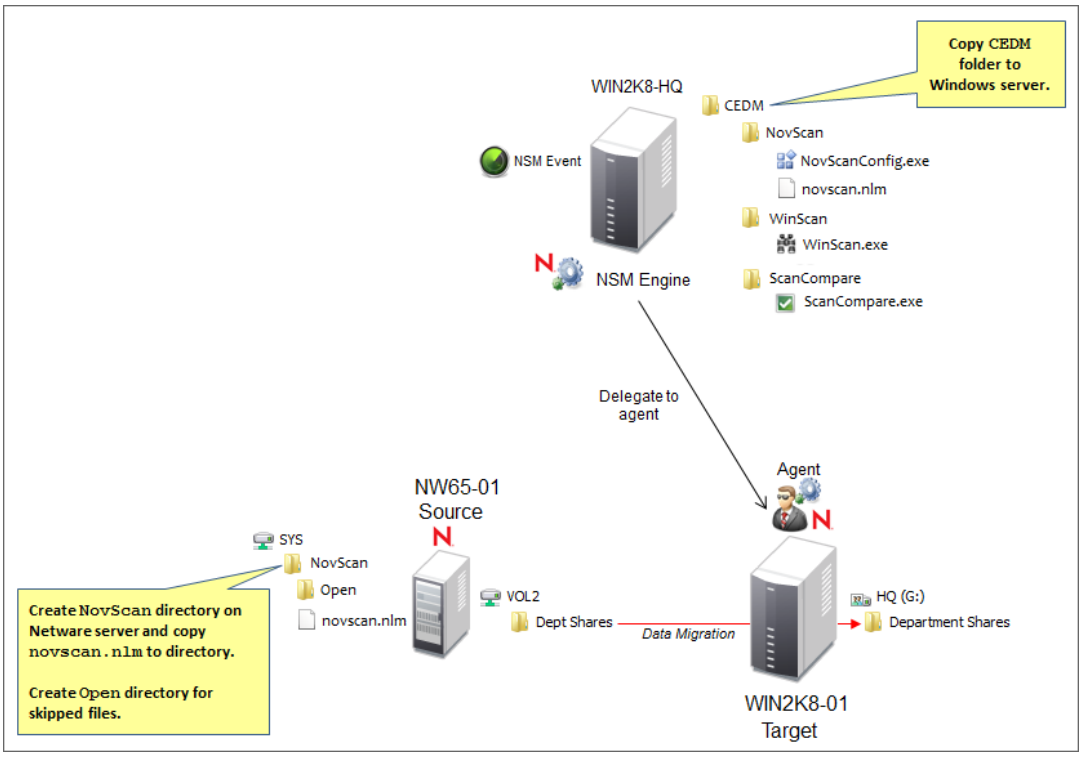
2a From the Novell Storage Manager ISO image, copy the `CEDM` folder to the Windows target server.

2b On each NetWare server from which you are going to migrate data, create a `NovScan` directory.

2c From the Novell Storage Manager ISO image, copy the `novscan.nlm` file from the `Utilities\CEDM\NovScan` folder to the NovScan directory you created in Step 2b.

2d In the new `NovScan` directory, create a new subdirectory and name it `Open`.

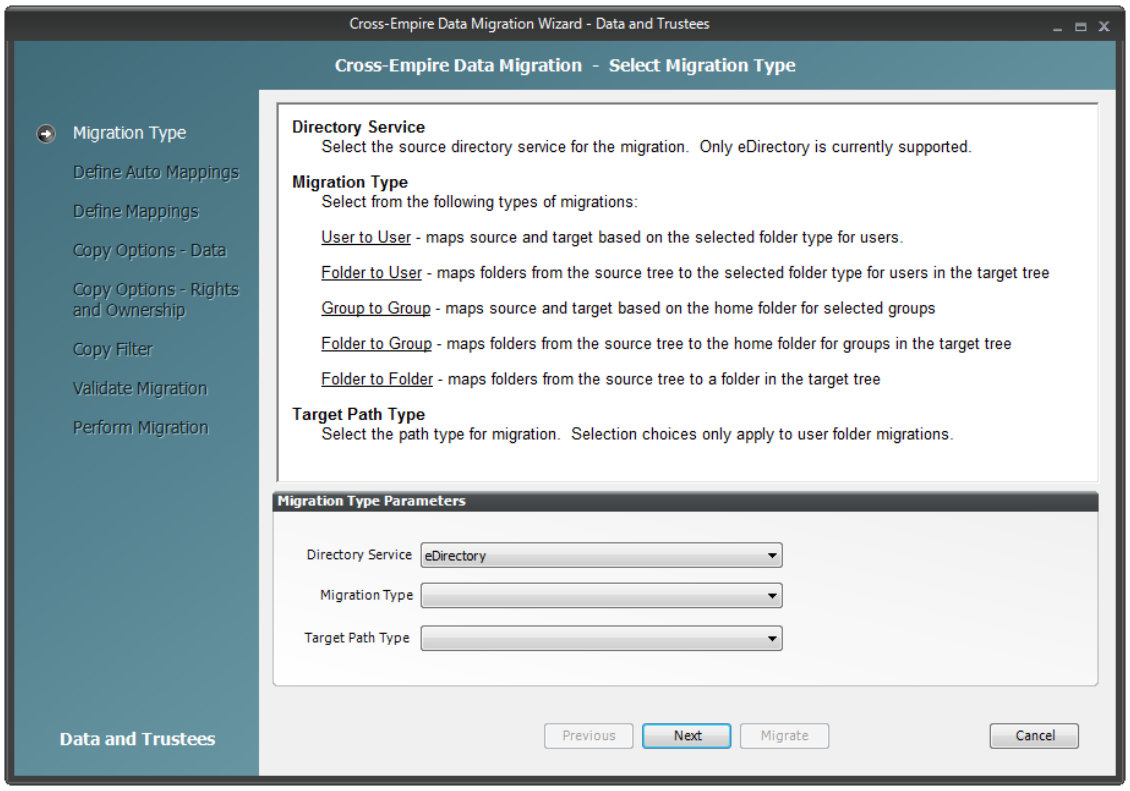
Figure 11-1 *Summary of Substeps to Complete*



3 In NSMAdmin, click the *Main* tab.

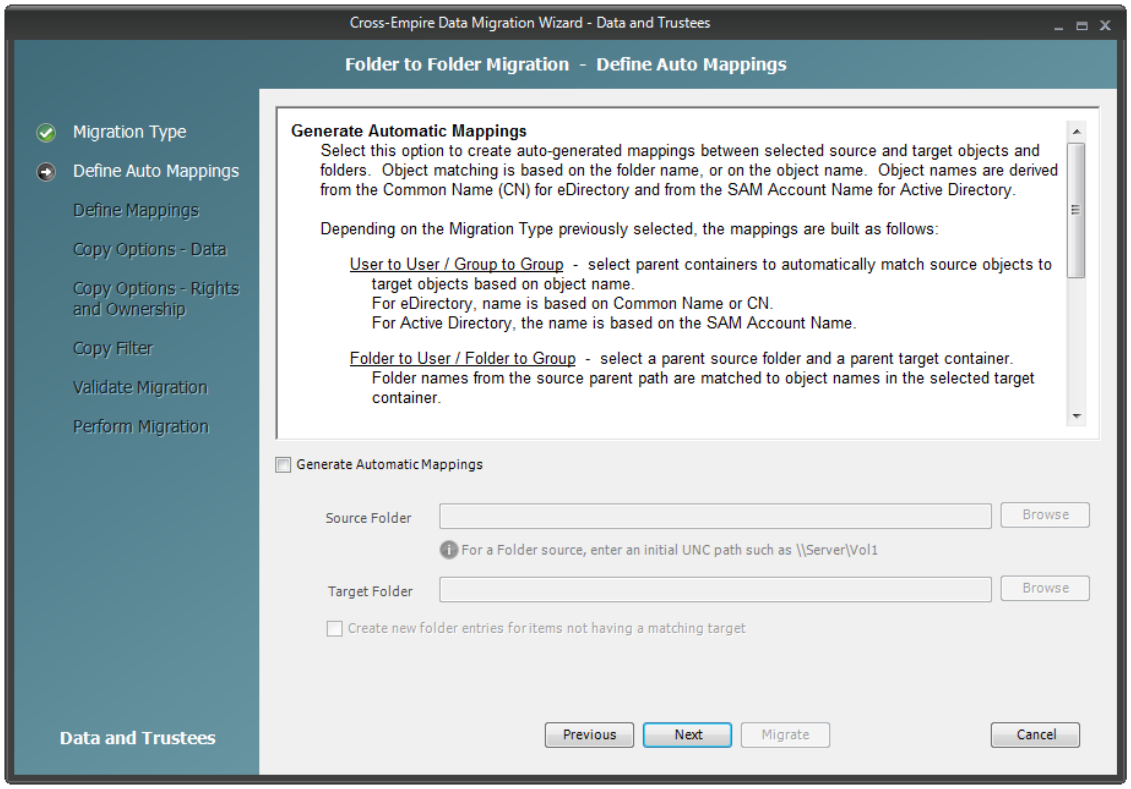
4 Click *Data Migration*.

5 Click *Migrate Data and Trustees*.



6 From the *Migration Type* drop-down menu, select *Folder to Folder.*

7 Click *Next*.



8 Fill in the following fields:

Generate Automatic Mappings: Select this check box to activate the other fields.

Source Folder: Specify an initial UNC path for a server and volume to browse.

For example, `\\server_name\volume_name\` or `\\ip_address\volume_name`.

After a path is entered, you can click the *Browse* button to browse to the folder you want.

Target Folder: Browse to select the target folder.

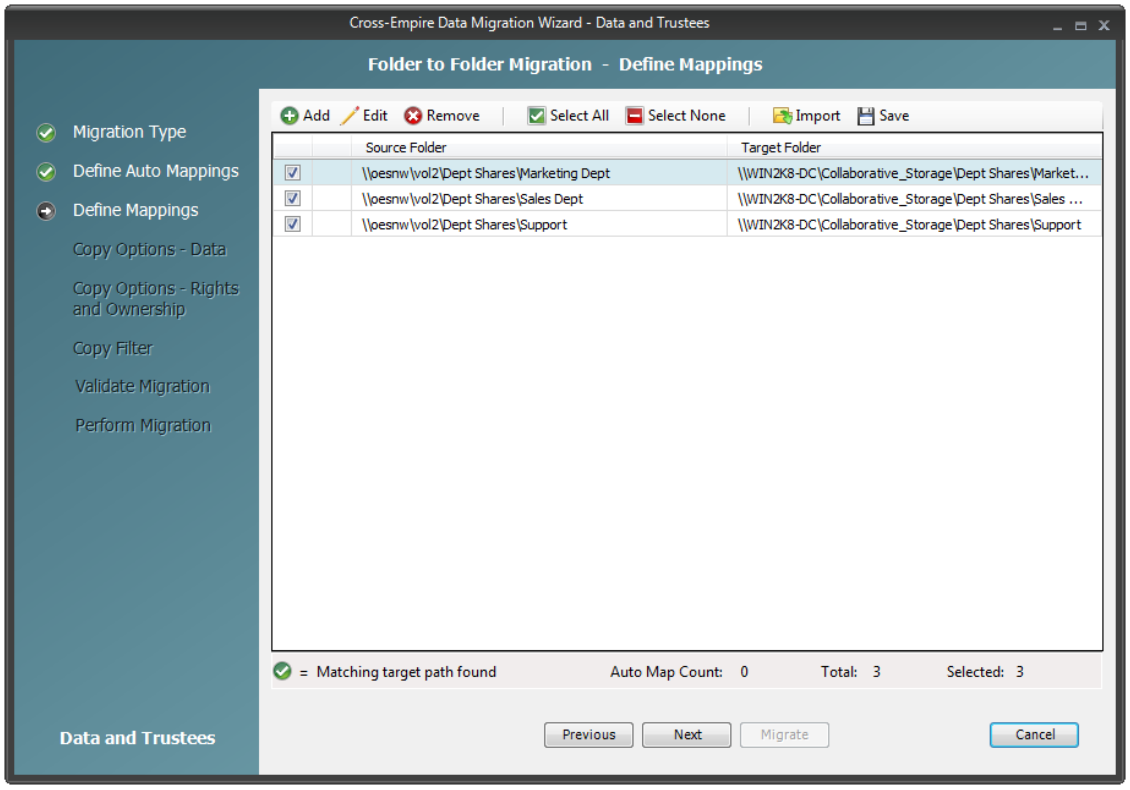
Create new folder entries for items not having a matching target: Selecting this check box indicates that you want Novell Storage Manager to display both matching and non-matching source and target folders.

Selecting this check box also indicates that you want Novell Storage Manager to create and populate any subfolders that do not exist in the target folder.

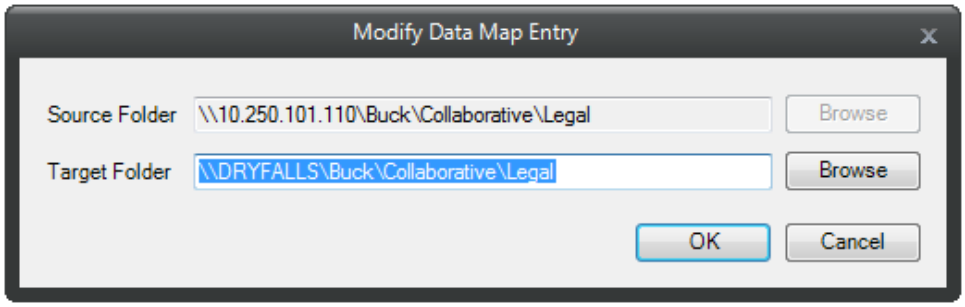
For example, assume that the source path at `\\10.10.10.233\Vol2\Projects` is being migrated to `\\Corpserver\Projects` and the `Projects` directory on the source server has a `Stategov` subfolder. If there is no `Stategov` subfolder in the target folder, a `Stategov` subdirectory is created to include the directory contents.

9 Click *Next*.

The Data Migration Wizard attempts to match the names of the subfolders of the source path with the subfolders of the specified target directory. If there is a match, the listed folder in the *Source Folder* field is selected and a corresponding match is listed in the Target Folder column.

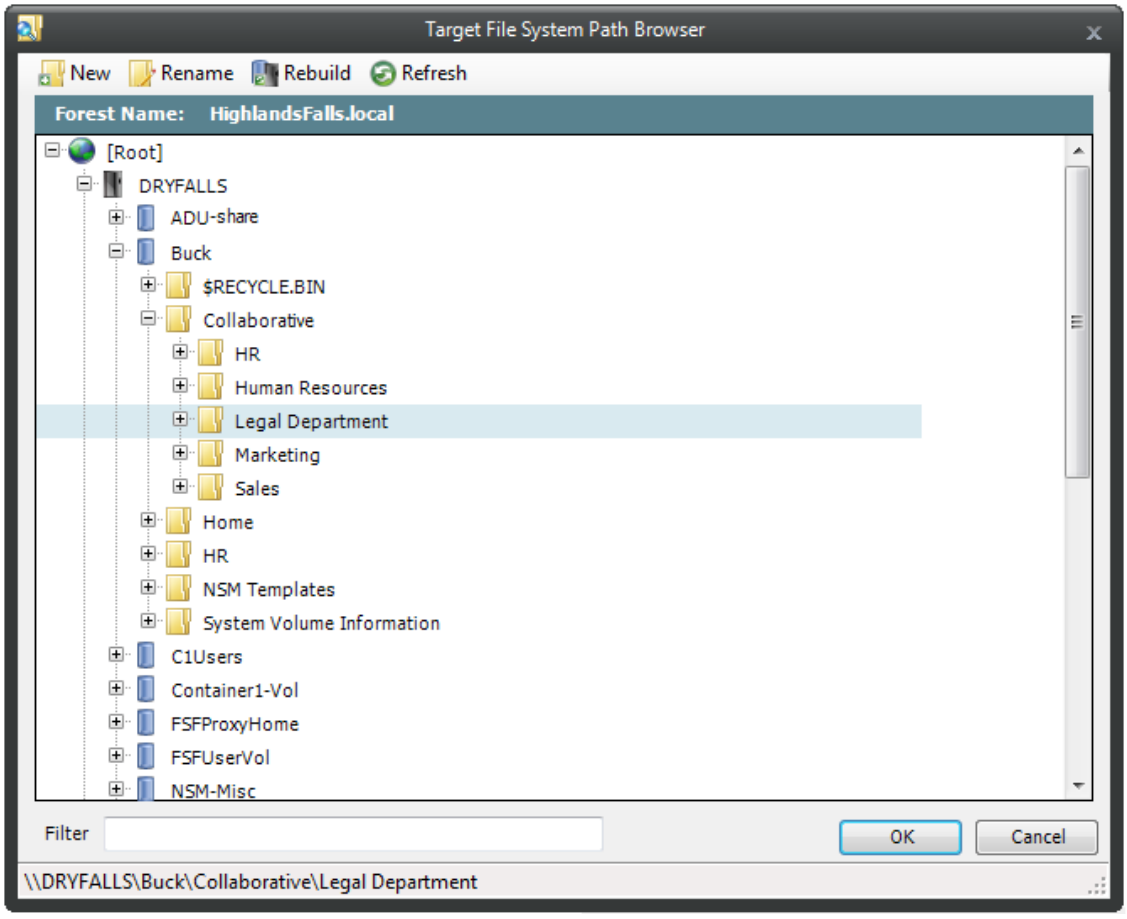


10 Specify a target folder for each source folder that is not automatically matched or that has an improperly matched subfolder by double-clicking the name to bring up the Modify Data Map Entry dialog box.

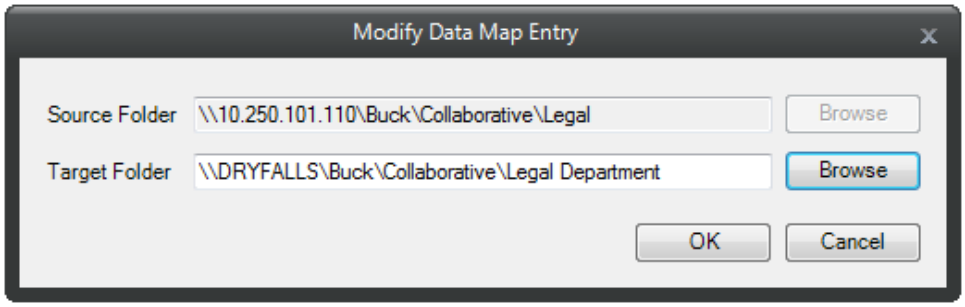


11 Remove the existing path in the *Target Folder* field and click *Browse*.

12 Locate and select the desired target folder, then click *OK*.



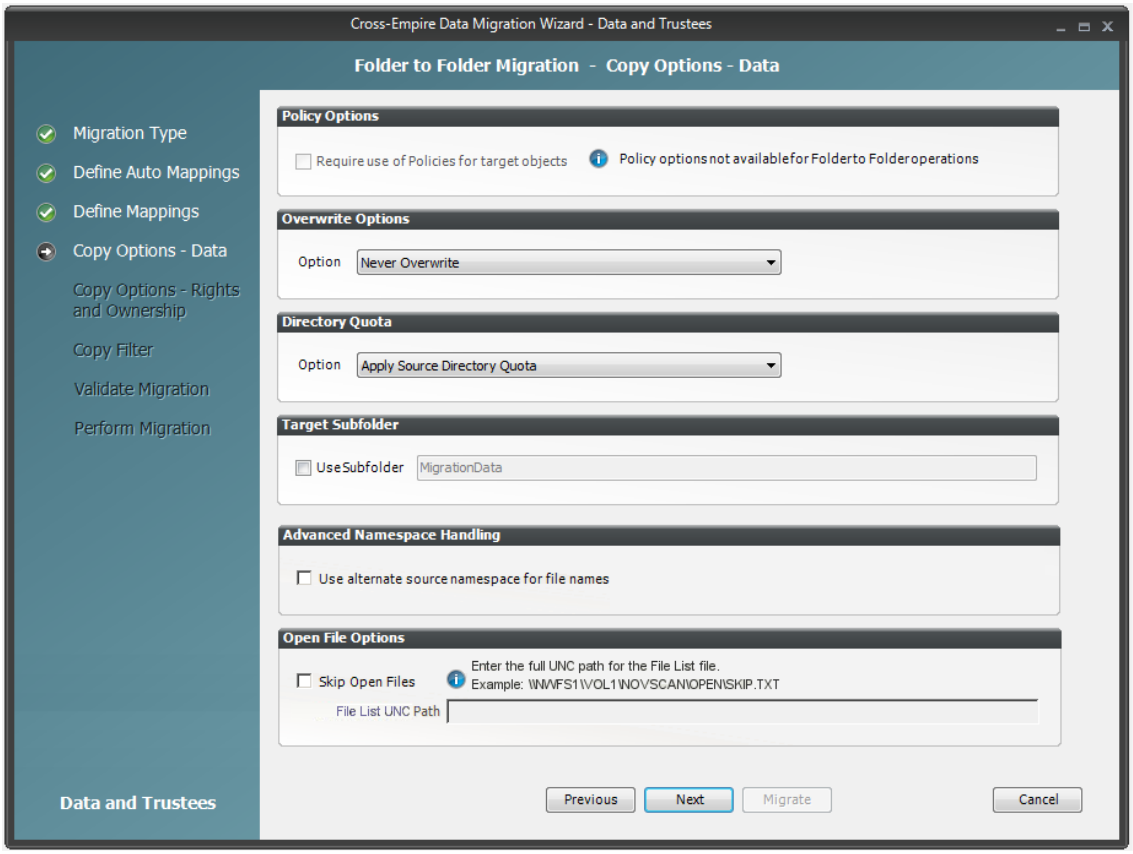
The new target path is indicated in the *Target Folder* field of the Modify Data Map Entry dialog box.



13 Click *OK*.

14 Click the check box corresponding to the listing with the new target.

15 Click *Next*.



16 Fill in the following fields:

Overwrite Options: Indicate what you want to take place when duplicate filenames are encountered in the source and target.

Directory Quota: Specify how quota settings from the source Novell file system should be applied after the migration.

Target Subfolder: If you want migrated data to be placed in a subfolder, select the *Use subfolder* check box and specify the subfolder name in the field.

Advanced Namespace Handling: Selecting this check box allows the Cross-Empire Data Migration subsystem to look for alternate namespaces for files that the Novell file system cannot resolve and therefore cannot migrate.

For example, files originally saved on a Mac or Linux system might use characters that the Novell file system cannot recognize. By looking for an alternative namespace, the Novell file system might be able to resolve the problem and migrate the file.

Open File Options: If you want the Cross-Empire Data Migration subsystem to skip all open files on the network and not migrate them, select *Skip Open Files*.

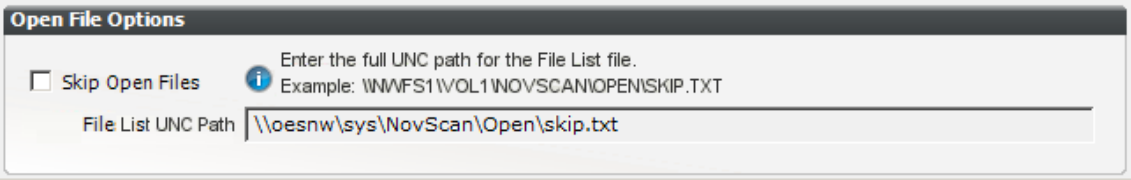
Selecting *Skip Open Files* activates the *File List UNC Path* field where you specify the name and location of the log file listing all of the open files that are skipped during the migration.

Specify the UNC path for the directory you created in Step 2d on page 167 along with a filename for the text file that will list the skipped files.

For example, `\\server_name\volume_name\directory_name\Open\skip.txt`

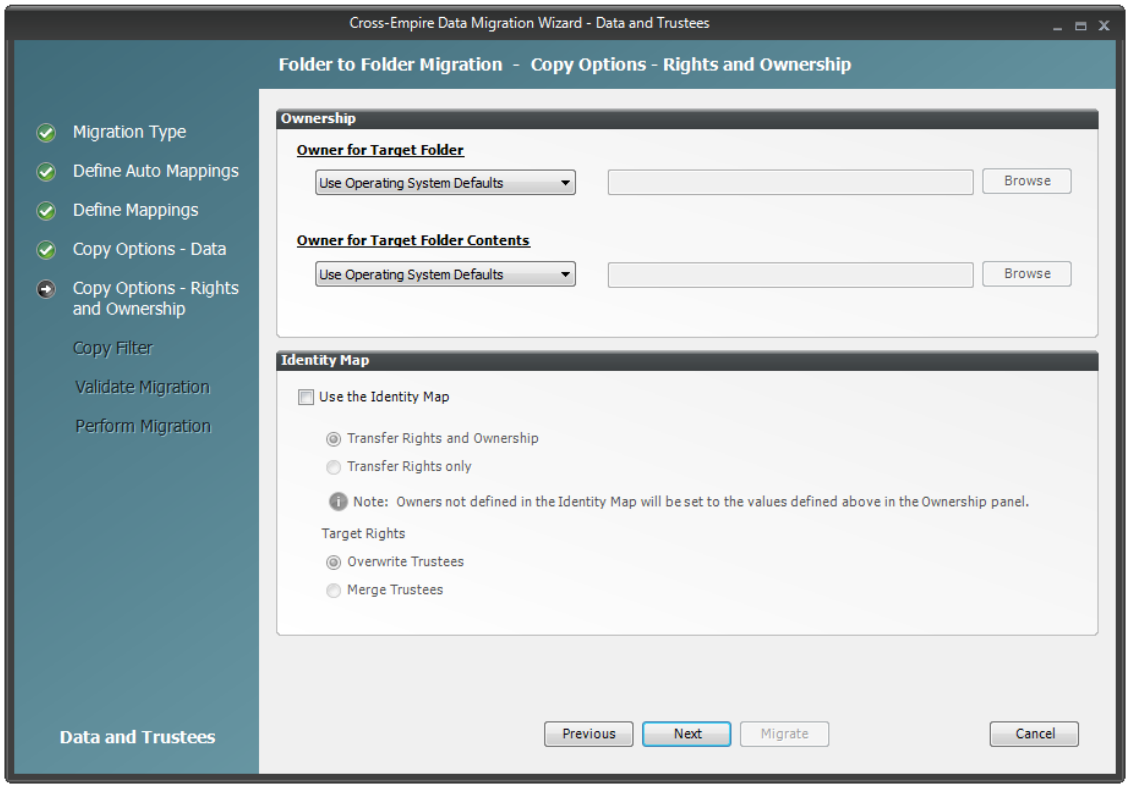
or

`\\ip_address\volume_name\Open\skip.txt`



The Cross-Empire Data Migration subsystem does not validate the path, so you must make sure that the path entered is correct. Otherwise, the migration fails.

17 Click *Next*.



18 Fill in the following fields:

Owner for Target Folder: Use these settings to specify how ownership of the migrated folder is determined.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the setting on the target server.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder.

Owner for Target Folder Contents: Use these settings to specify how ownership of the migrated folder contents is determined.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder.

Use the Identity Map: Select this check box if you want Novell Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from eDirectory to Microsoft Active Directory.

- **Transfer Rights and Ownership:** Select this option if you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you might not want to provide.
- **Transfer Rights Only:** Select this option to transfer only the file and folder security rights.
- **Overwrite Trustees:** Select this option to override any existing trustee assignments for a target file or folder with the established Novell eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Select this option to merge the established Novell eDirectory trustee assignments with those of the target files or folders in Active Directory.

19 Click *Next*.

20 (Conditional) If you want to use a filter to include or exclude specific files, select the *Use Copy Filter* check box and click the *Add* button.

20a Fill in the following fields:

Description: Specify a description of the filter.

Action: From the drop-down menu, select either *Migrate* or *Ignore*, based on whether the filter specifies to migrate files or folders or to ignore them.

Files, Folders: Specify if the filter applies to files or folders.

Masks: List the file types to migrate or ignore.

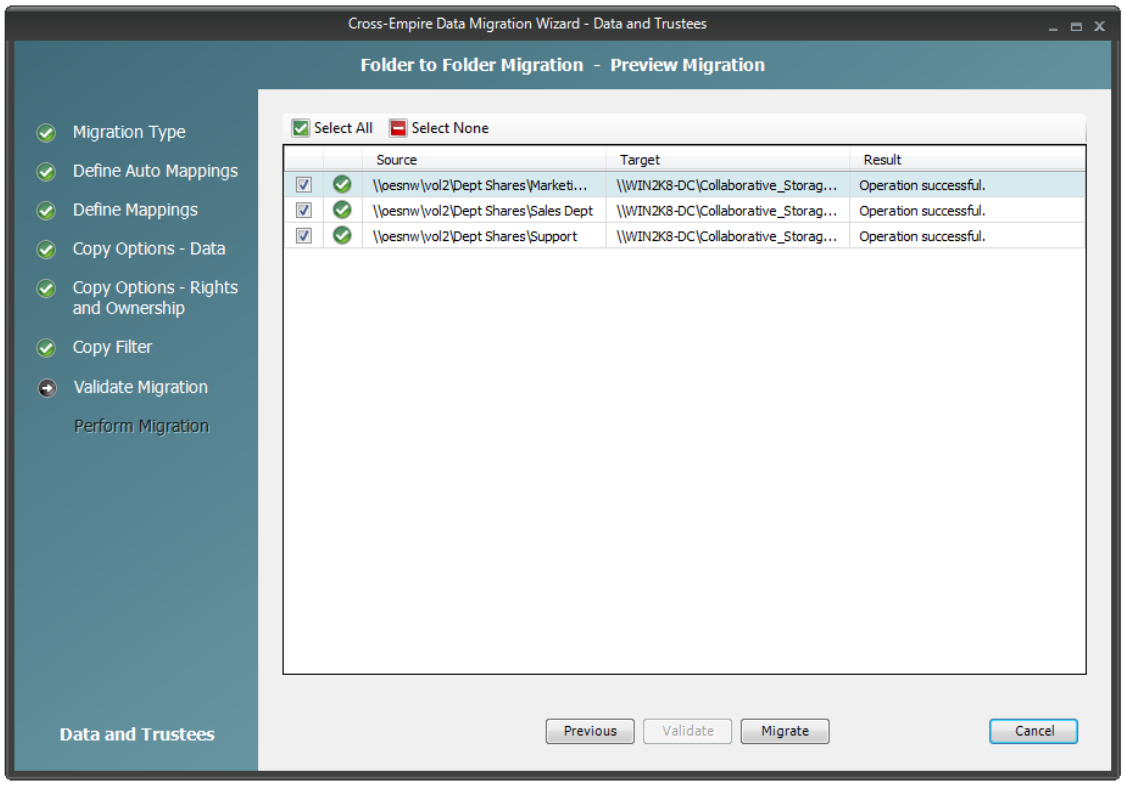
20b Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 5.5.8, "Setting Vault Rules," on page 49.

20c Click *OK*.

21 Click *Validate*.

Validate shows the result of certain checks that can be run prior to the migration. The *Result* column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



22 (Conditional) Take any necessary action in the Active Directory target and then re-run the Data Migration Wizard.

23 Click *Migrate*.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click *Pending Events*. For more information on Pending Events, see Section 12.1.6, "Pending Events," on page 219.

24 Do one of the following:

- If you skipped some files to migrate later, click *Finish* and then continue with "Migrating Skipped Files" on page 175.
- If you have migrated all of your data, click *Finish*.

  You are now finished with the folder to folder migration.

Migrating Skipped Files

The second phase of a folder to folder data migration is conducted when all of the users are logged off the network, so all network files are closed.

1 Have everyone log off the network so that there are no open files on the source NetWare or Open Enterprise Server machines.

2 Open the text file that you created in Step 16 on page 172 and view the files that were skipped.

Do not make any changes to the file. Doing so causes errors during the migration.

3 Save a copy of the text file.

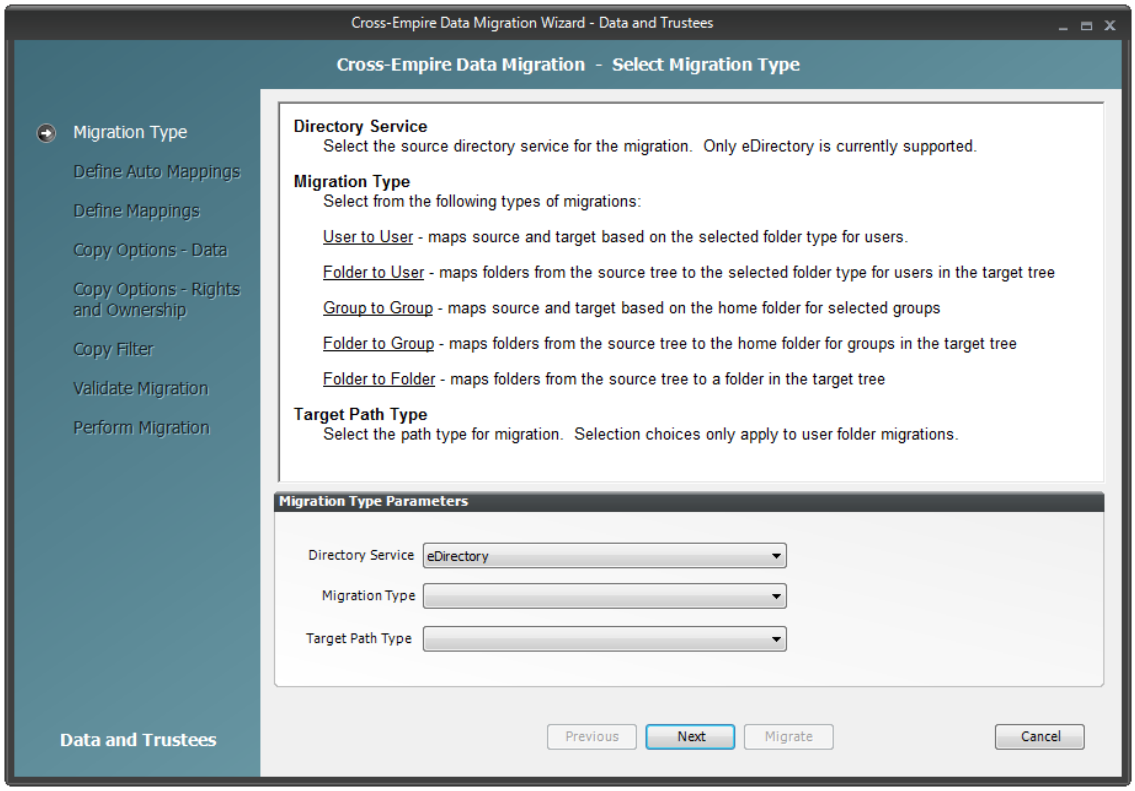
For example, if you named the file `skip.txt`, save a copy as `skip_copy.txt`.

After the Cross-Empire Data Migration subsystem migrates the skipped files, it deletes the text file. You can use the copy to verify that the files were migrated.

4 In NSMAdmin, click the *Main* tab.

5 Click *Data Migration*.

6 Click *Migrate Data and Trustees*.



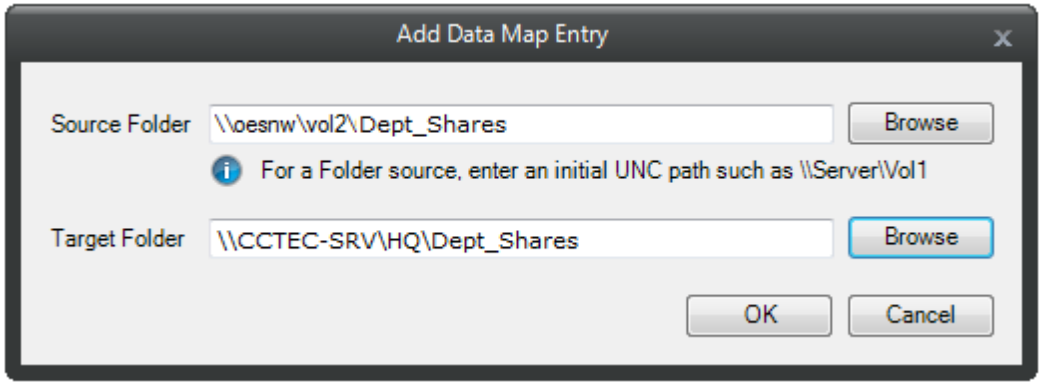
7 From the *Migration Type* drop-down menu, select *Folder to Folder Using File List*.

8 Click *Next*.

9 Skip the Automatic Mappings settings by clicking *Next*.

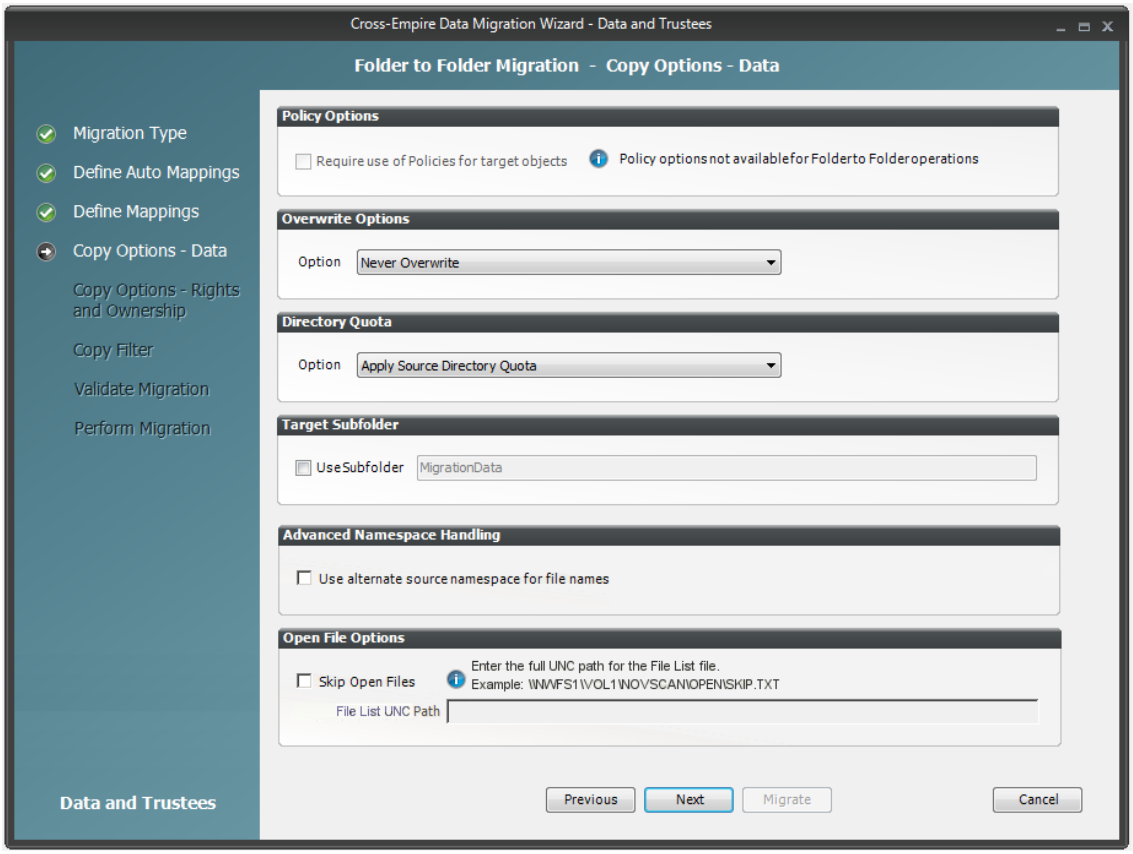
10 On the Define Mappings wizard page, click *Add*.

11 In the Add Data Entry dialog box, browse to and select the source and target.

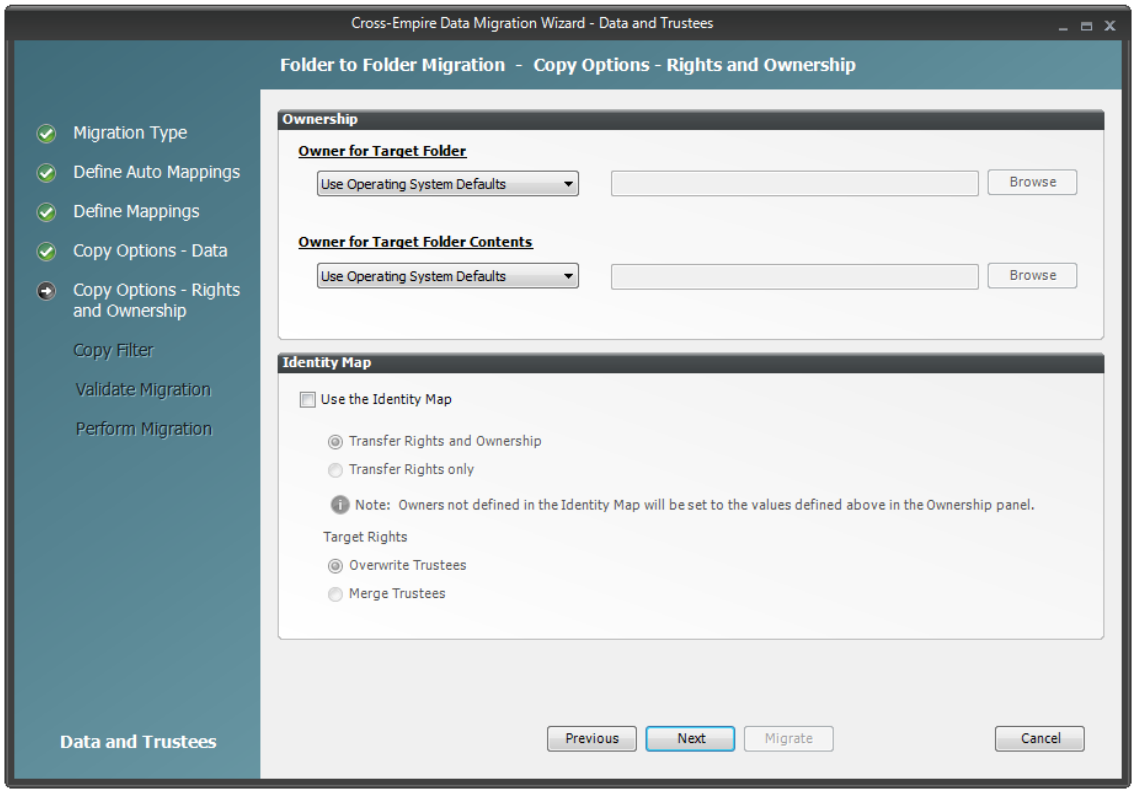


12 Click *OK*.

13 On the Define Mappings wizard page, verify the source folder and the destination folder and click *Next*.



14 On the Copy Options - Data wizard page, from the Option drop-down menu in the *Overwrite Options* region, select *Overwrite if Newer* and click *Next*.



15 (Optional) On the Copy Options - Rights and Owners wizard page, from the drop-down menu of the *Owner for Target Folder* region, select *Set Explicit Owner.*

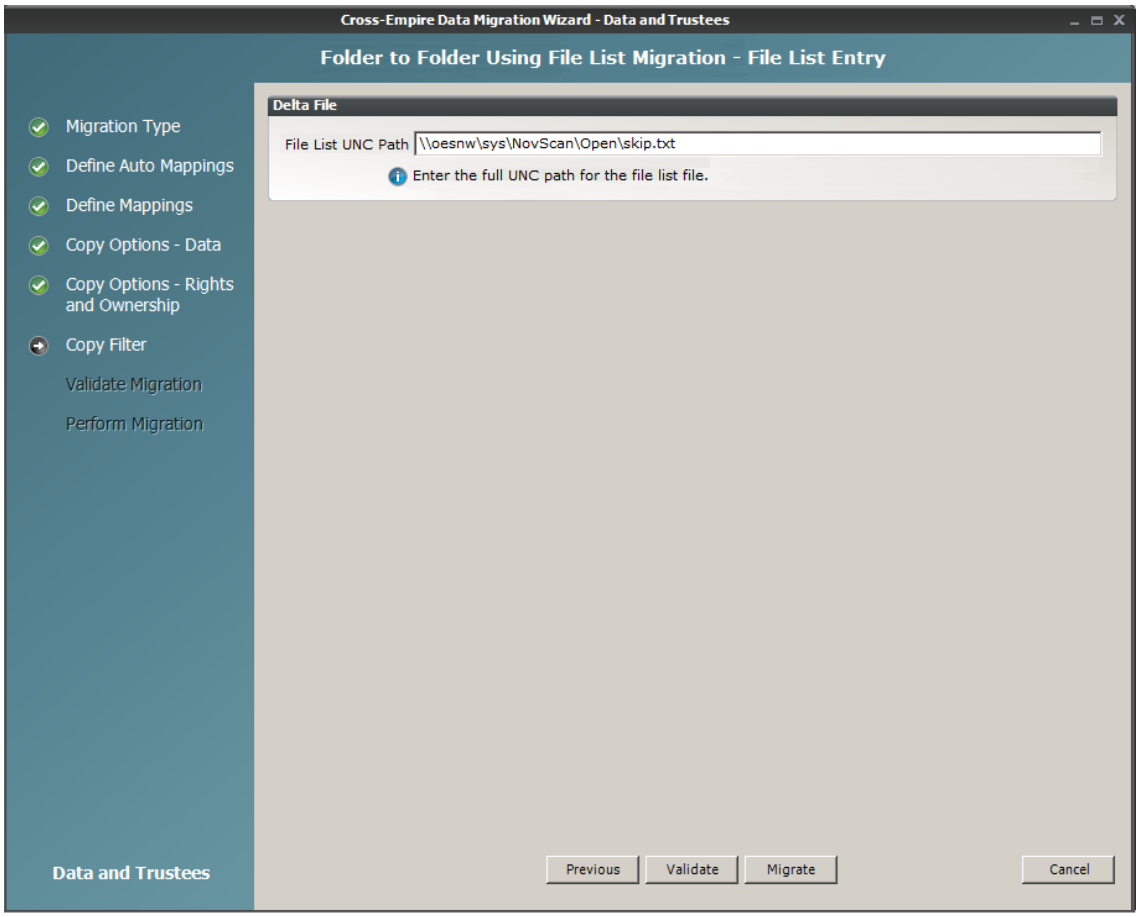
16 (Conditional) If you chose to set an explicit owner for the folder, click the corresponding *Browse* button and browse to specify an owner for the target folder.

17 (Optional) From the drop-down menu of the *Owner for Target Folder Contents* region, select *Set Explicit Owner*.

18 (Conditional) if you chose to set an explicit owner for the folder contents, click the corresponding *Browse* button and browse to specify an owner for the target folder contents.

19 Select the *Use Identity Map* check box and click *Next*.

20 On the Copy Filter wizard page, specify the UNC path to the file you created in Step 16 on page 172.



21 Click *Validate* to confirm that the path is correct.

22 Click *Migrate*.

The skipped files are migrated and the text file that you created in Step 16 on page 172 is deleted.

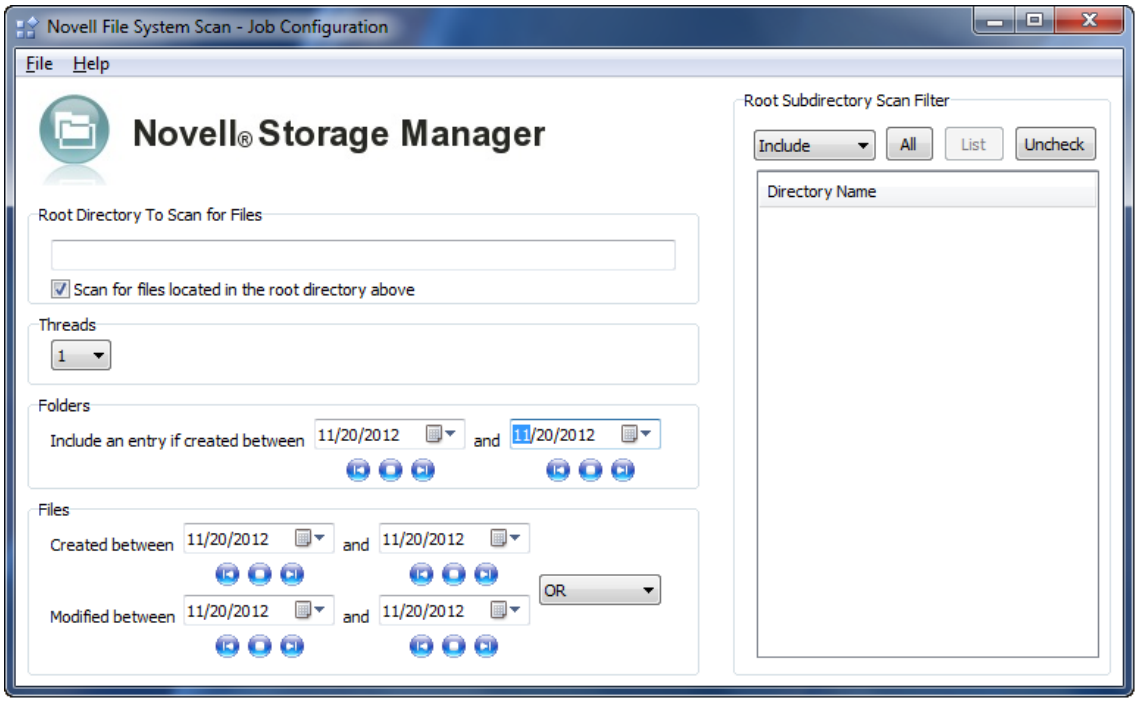
23 Click *Finish*.

24 Continue with "Creating a Job File to Scan the Source Server for New or Modified Folders and Files" on page 179.

Creating a Job File to Scan the Source Server for New or Modified Folders and Files

With the skipped files migrated, you are now ready to create a job file so the NovScanConfig utility can scan the source server.

1 From the `CEDM` folder that you copied in Step 2a on page 167, open the `NovScan` folder and launch the NovScanConfig utility.



2 In the *Root Directory To Scan for Files* field, enter the UNC path to the directory on the NetWare or Open Enterprise Server you want to scan.

   For example: `\\oesnw\vol2\dept shares`

3 In the *Root Subdirectory Scan Filter* region, click the *List* button, then click the *All* button to include all of the subdirectories, including new subdirectories, in the directory you specified in Step 2.

4 Ensure that the drop-down menu listing displays *Include*.

5 From the *Threads* drop-down menu, select the thread count you want for the migration.

6 In the *Folders* region, in the first date entry, select the date when you migrated the closed files.

   This specifies that the job file created by the NovScanCofig utility lists all folders that are new or modified since midnight of the selected date.

7 In the second date entry, select a concluding date for the range.

8 In the *Files* region, in the date entry pertaining to *Created between*, select the date when you migrated the closed files.

   This specifies that the job file lists all files that have been created since midnight of the selected date.

9 In the second date entry for *and*, select a concluding date for the range.

10 Ensure that the drop-down menu listing displays *OR*.

11 In the date entry for *Modified between*, select the date when you migrated the closed files.

   This specifies that the job file lists all files that have been modified since midnight of the selected date.

12 In the second date entry for *and*, select a concluding date for the range.

13 From the *File* menu, select *Save As* and save the file as a text file with a `.job` extension in the `NovScan` folder that you created in Step 2b on page 167.

   For example: `vol2_dept.job`

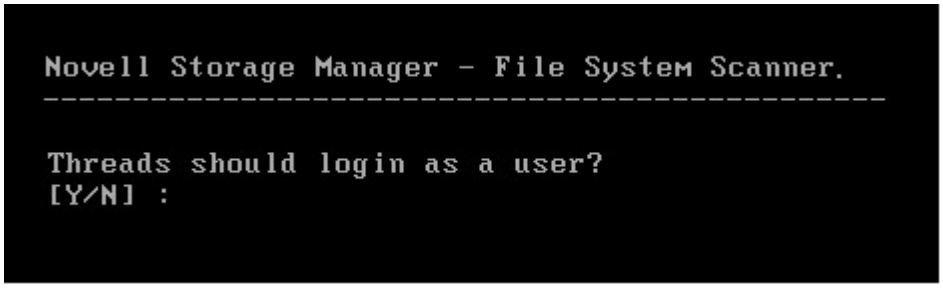
14 When you are notified that the text file has been saved, click *OK*.

15 Close the NovScanConfig utility.

16 Continue with "Using the NovScan NLM to Run the Job File" on page 181.

Using the NovScan NLM to Run the Job File

1 At the NetWare server, load the `novscan.nlm` from the path that you established in Step 2b on page 167.



2 Select either *Y* or *N*.

If you are scanning an Open Enterprise Server, select *Y* and then log in as an administrator so that this NetWare server can make a connection to the remote Open Enterprise Server machine.

If you are scanning a local NetWare server, select *N*.

3 At the NetWare console, run the job file that you created in Step 13 on page 180.

The following commands can be used at the NetWare console command prompt to perform actions with the NovScan NLM:

`JOB=`*`path to job file on local server`*

The following example is a NovScan NLM directive to run a job file:

```
SERVER65: novscan job=sys:novscan\scanvol1.job
```

- `STOPSCAN`

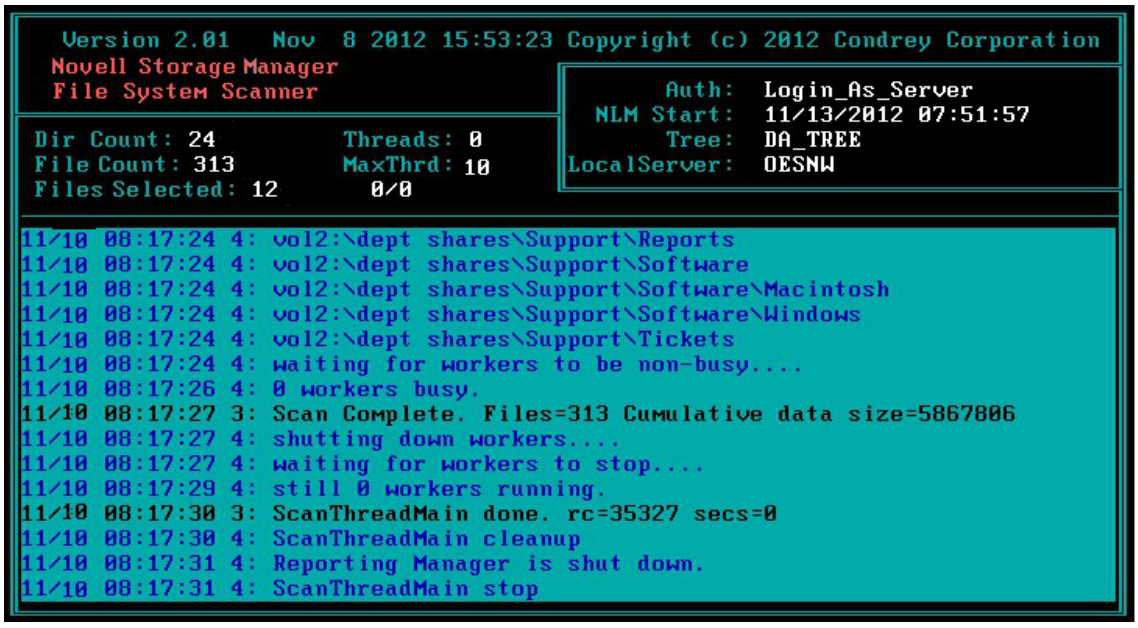
  The NovScan NLM can run one scan job at a time. You might want to stop a scan that is in progress. The following example is a directive for the NovScan NLM to stop a scan that is running.

  ```
  SERVER65: novscan stopscan
  ```

- `SHOW=ON/OFF`

  The NovScan NLM by default shows the names of the directories as they are being scanned. These scanned directories are also logged. You can turn the display and logging on or off by using this parameter. For example:

  ```
  SERVER65: novscan show=on
  SERVER65: novscan show=off
  ```



The *Files Selected* field displays the number of files created or modified since the first phase of the migration.

4 From your Windows workstation, go to the `NovScan` folder that you created in Step 2b on page 167.

5 Observe that a new text file has been created with the same name as the job file that you created in Step 13 on page 180 but with the addition of -FLIST.

This new file is a list of all the new and modified files since the first phase of the migration. If you open this file, do not make any changes, because this causes errors during the next phase of the migration.

6 Save a copy of the text file.

For example, if the file is named `vol2_dept-FLIST.job`, save a copy as `vol2_dept-FLIST_copy.job`.

7 Continue with "Migrating the New and Modified Files" on page 182.

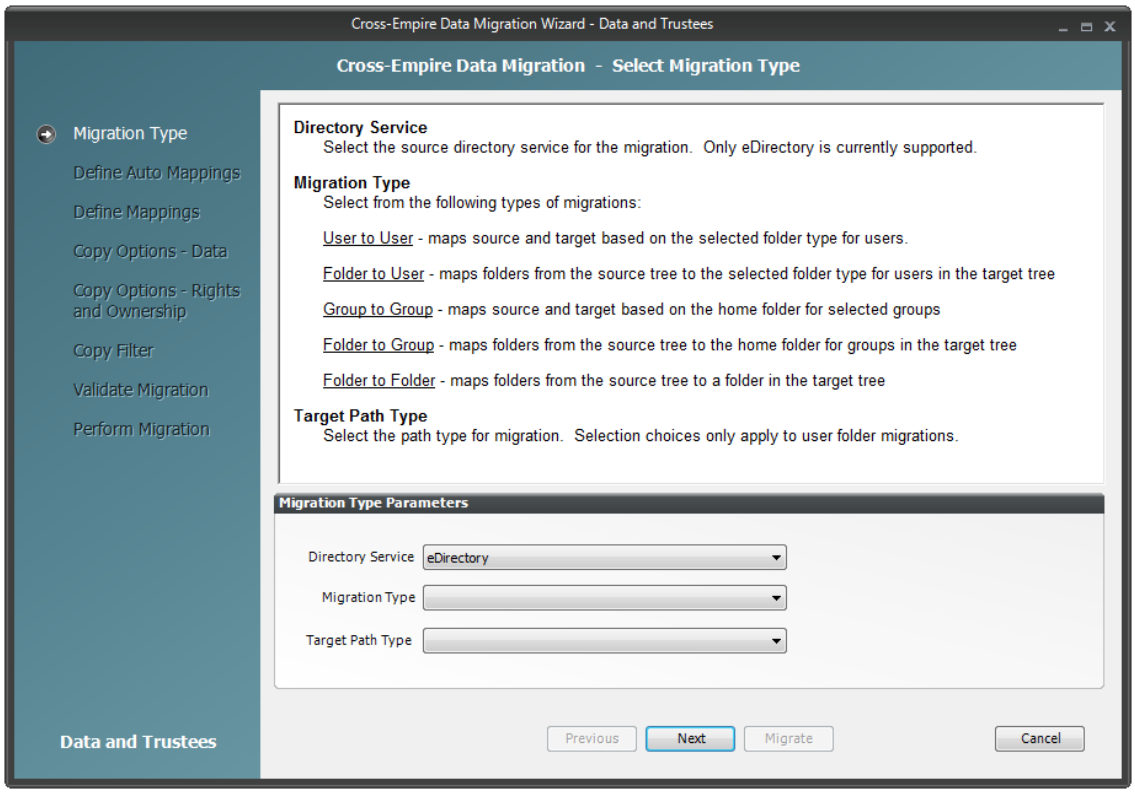
Migrating the New and Modified Files

Migrating all of the files that are new or modified since the first phase of the folder to folder migration follows the same process as migrating the skipped files. The only difference is that you enter a different UNC path.

1 In NSMAdmin, click the *Main* tab.

2 Click *Data Migration*.

3 Click *Migrate Data and Trustees*.



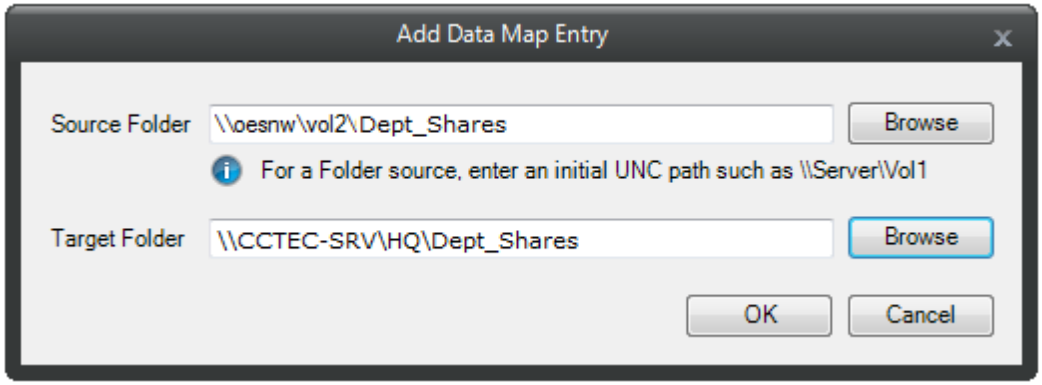
4 From the *Migration Type* drop-down menu, select *Folder to Folder Using File List*.

5 Click *Next*.

6 Skip the Automatic Mappings settings by clicking *Next*.

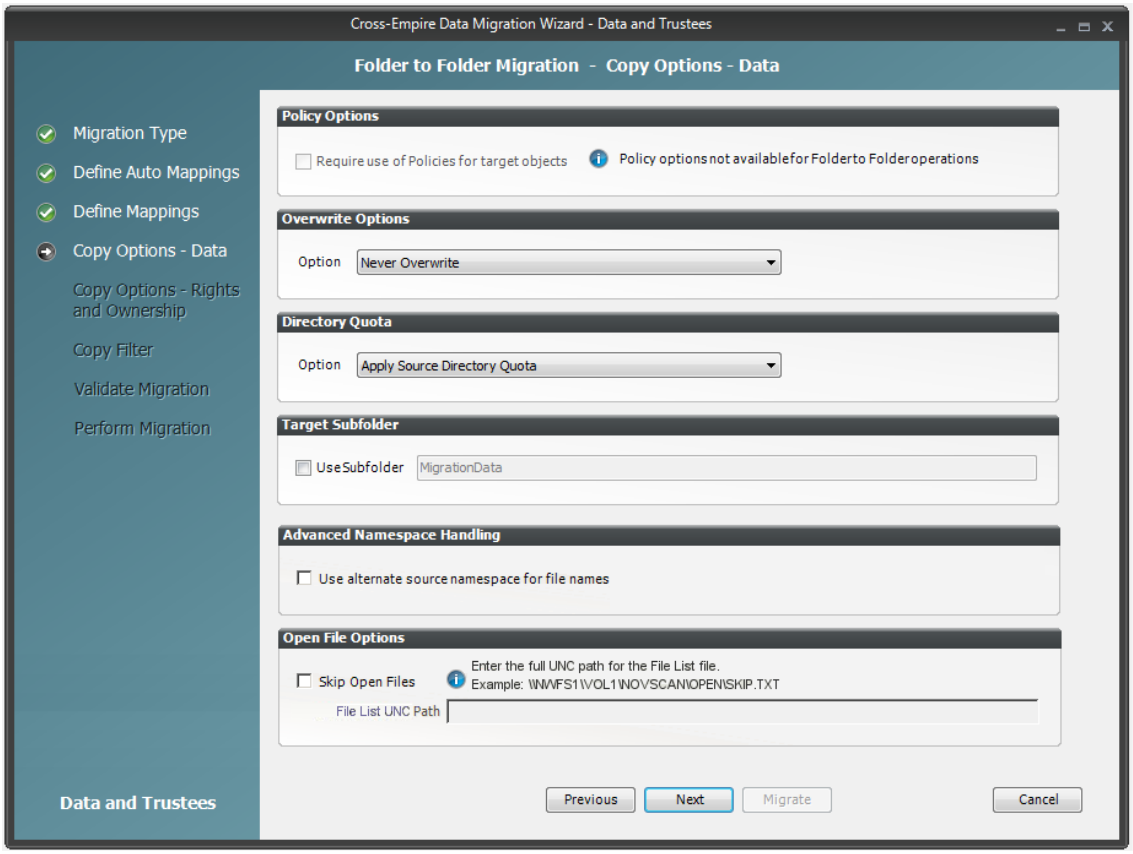
7 On the Define Mappings wizard page, click *Add*.

8 In the Add Data Entry dialog box, browse to and select the source and target.

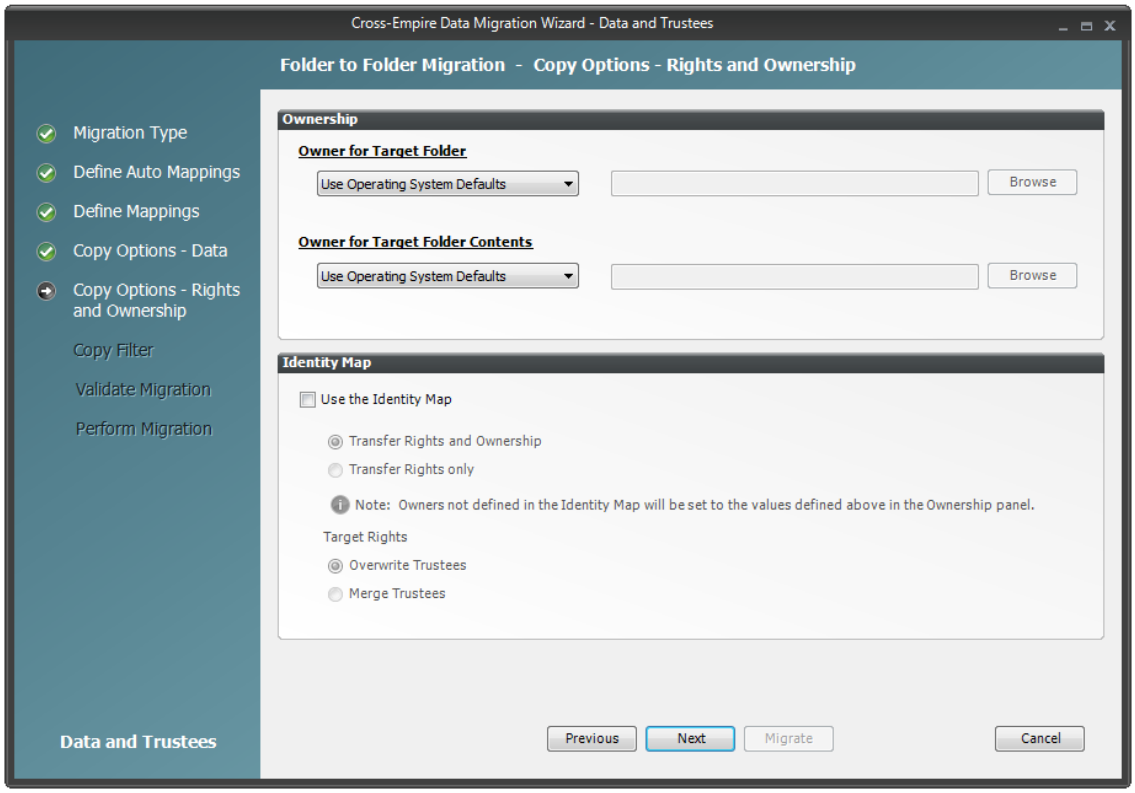


9 Click *OK*.

10 On the Define Mappings wizard page, verify the source folder and the destination folder and click *Next*.



11 On the Copy Options - Data wizard page, from the *Option* drop-down menu in the *Overwrite Options* region, select *Overwrite if Newer*, then click *Next*.



12 (Optional) On the Copy Options - Rights and Owners wizard page, from the drop-down menu of the *Owner for Target Folder* region, select *Set Explicit Owner*.

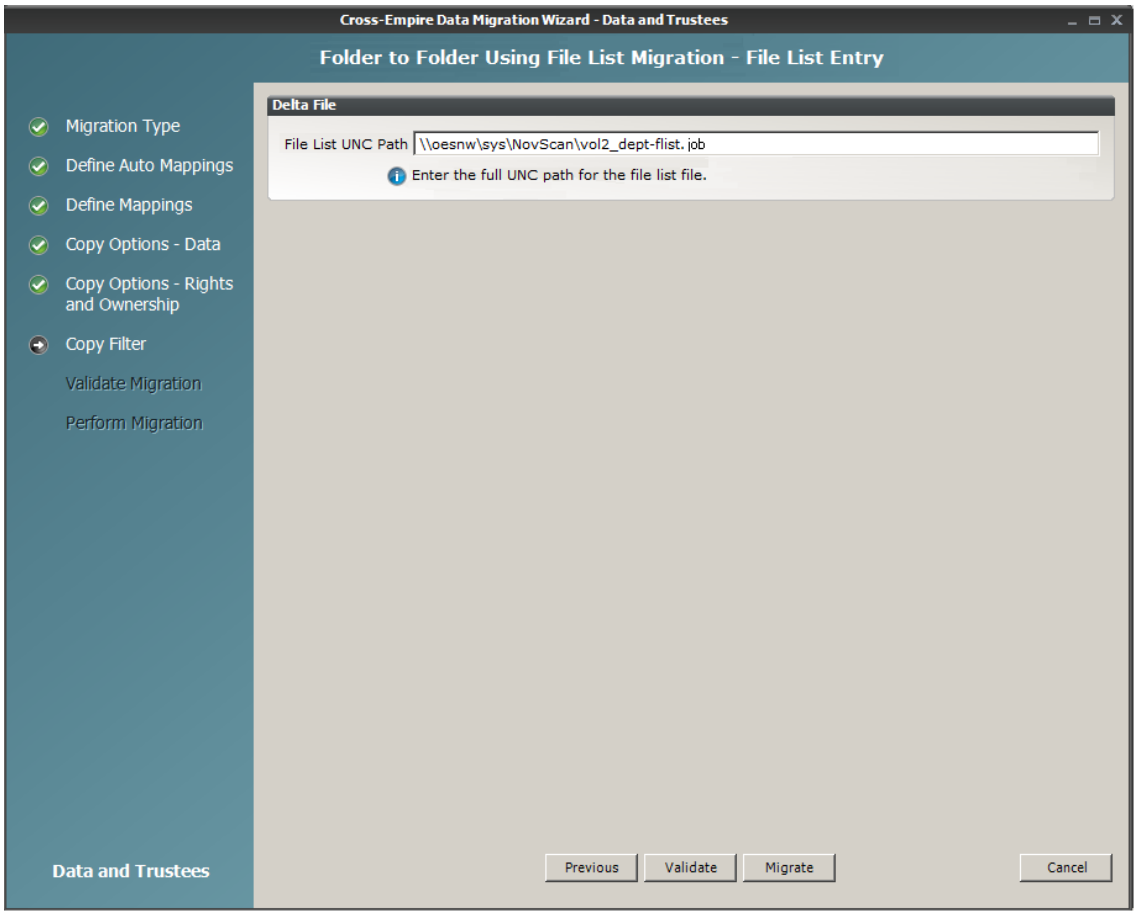
13 (Conditional) If you chose to set an explicit owner for the folder, click the corresponding *Browse* button and browse to specify an owner for the target folder.

14 (Optional) From the drop-down menu of the *Owner for Target Folder Contents* region, select *Set Explicit Owner*.

15 (Conditional) If you chose to set an explicit owner for the folder contents, click the corresponding *Browse* button and browse to specify an owner for the target folder contents.

16 Select the *Use Identity Map* check box and click *Next*.

17 On the Copy Filter wizard page, specify the UNC path to the new text file that you viewed in Step 5 on page 182.



18 Click *Validate* to confirm that the path is correct.

19 Click *Migrate*.

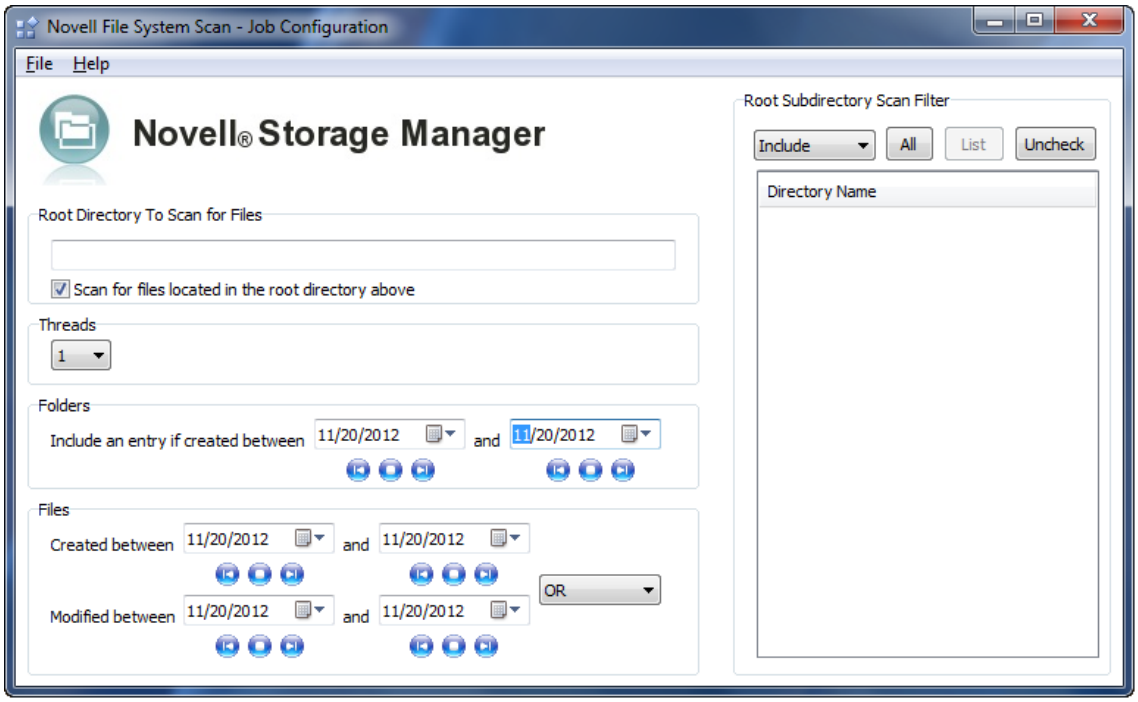
The new and modified files are migrated and the text file that you viewed in Step 5 on page 182 is deleted.

20 Click *Finish*.

21 Continue with "Creating a Job File to Scan the Source Server for All Folders and Files" on page 186.

Creating a Job File to Scan the Source Server for All Folders and Files

1 From the `CEDM` folder that you copied in Step 2a on page 167, open the `NovScan` folder and launch the NovScanConfig utility.



2 In the *Root Directory To Scan for Files* field, enter the UNC path to the directory on the NetWare or Open Enterprise Server you want to scan.

   For example: `\\oesnw\vol2\dept shares`

3 In the *Root Subdirectory Scan Filter* region, click the *List* button, and then click the *All* button to include all of the subdirectories in the directory you specified in Step 2.

4 Ensure that the drop-down menu listing displays *Include*.

5 From the *Threads* drop-down menu, select the thread count you want for the migration.

6 In the *Folders* region, in the first date entry, select the left button, which sets the date to 1/1/1970.

7 In the second date entry, select the right button, which sets the date to 12/31/2036.

   This range of dates ensures that you identify all folders that exist in the specified path.

8 In the *Files* region, in the date entry for *Created between*, select the left button, which sets the date to 1/1/1970.

9 In the second date entry for *and*, select the right button, which sets the date to 12/31/2036.

   Again, this range of dates ensures that you identify all files created in the specified path.

10 Ensure that the drop-down menu listing displays *OR*.

11 Set the date range for modified files to the same dates you used for new folders and new files.

12 From the *File* menu, select *Save As* and save the file as a text file with a `.job` extension in the `NovScan` folder that you created in Step 2b on page 167.

   For example: `vol2_dept-all.job`

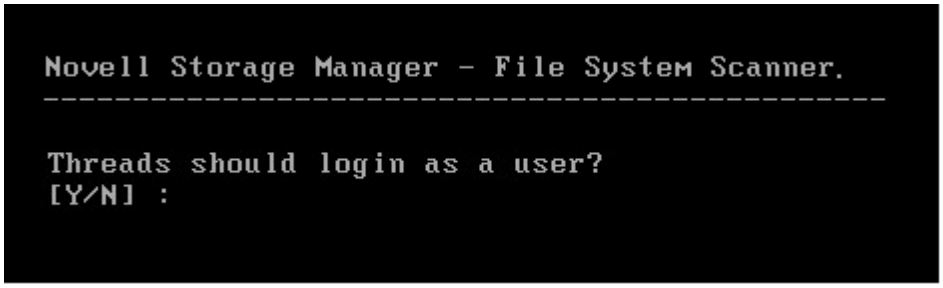
13 When you are notified that text file has been saved, click *OK*.

14 Close the NovScanConfig utility.

15 Continue with "Using the NovScan NLM to Run the Job File" on page 188.

Using the NovScan NLM to Run the Job File

1 At the NetWare server, load the `novscan.nlm` from the path that you established in Step 2b on page 167.



2 Select either *Y* or *N*.

If you are scanning an Open Enterprise Server, select *Y* and then log in as an administrator so that this NetWare server can make a connection to the remote Open Enterprise Server machine.

If you are scanning a local NetWare server, select *N*.

3 At the NetWare console, run the job file that you created in Step 12 on page 187.

The following commands can be used at the NetWare console command prompt to perform actions with the NovScan NLM:

`JOB=`*`path to job file on local server`*

The following example is a NovScan NLM directive to run a job file:

```
SERVER65: novscan job=sys:novscan\scanvol1.job
```

- `STOPSCAN`

  The NovScan NLM can run one scan job at a time. You might want to stop a scan that is in progress. The following example is a directive for the NovScan NLM to stop a scan that is running.

  ```
  SERVER65: novscan stopscan
  ```

- `SHOW=ON/OFF`

  The NovScan NLM by default shows the names of the directories as they are being scanned. These scanned directories are also logged. You can turn the display and logging on or off by using this parameter. For example:

  ```
  SERVER65: novscan show=on
  SERVER65: novscan show=off
  ```

The *Files Selected* field now displays the total number of files.

4 From your Windows workstation, go to the `NovScan` folder that you created in Step 2b on page 167.

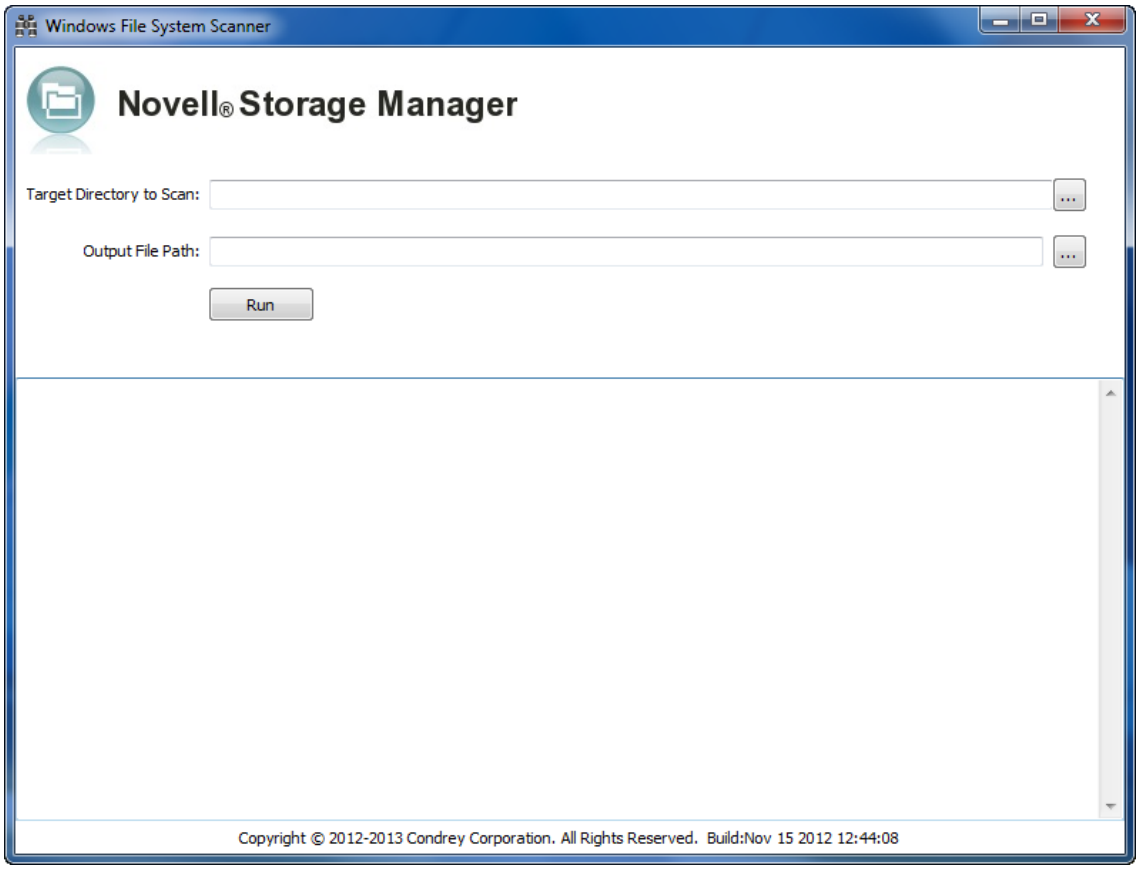
5 Observe that a a new text file has been created with the same name as the job file that you created in Step 12 on page 187 but with the addition of -FLIST.

This new file is a list of all the files from the specified path. If you open this file, do not make any changes, because this can cause errors during the file comparison.

6 Continue with "Scanning the Target Server for All Folders and Files" on page 189.

Scanning the Target Server for All Folders and Files

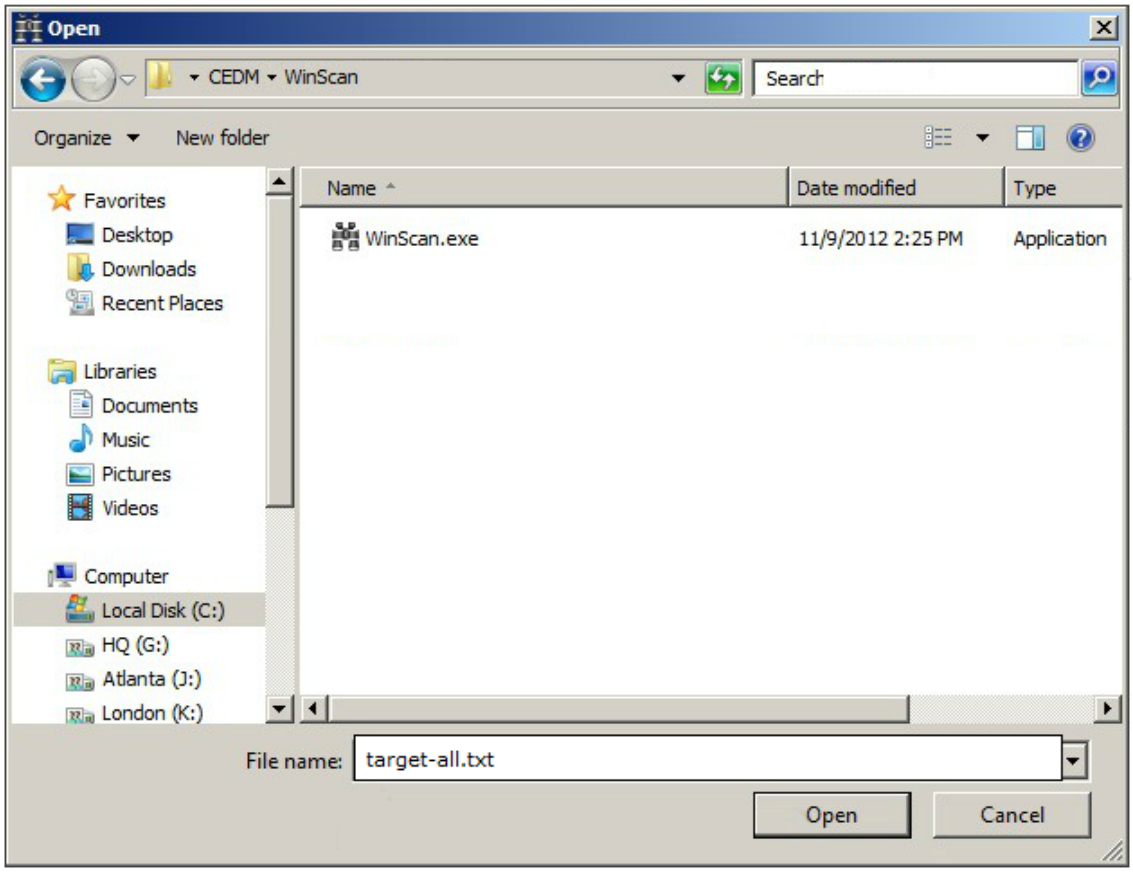
1 From the `CEDM` folder that you copied in Step 2a on page 167, open the `WinScan` folder and launch the WinScan utility.



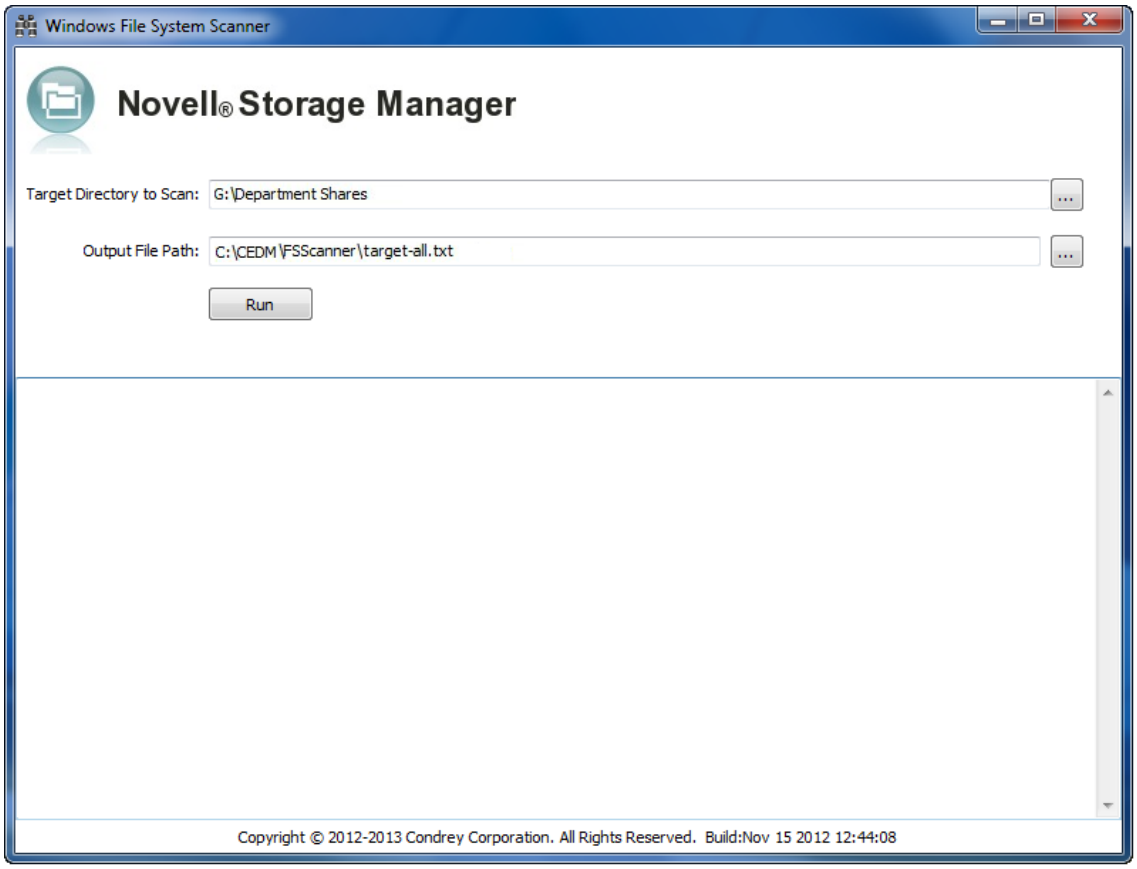
2 Click the browse button for the *Target Directory to Scan* field and browse to select the target folder.

3 Click the browse button for the *Output File Path* field, browse to the `WinScan` folder, and in the *File name* field of the Open dialog box, specify a filename with a `.txt` extension.

For example, `target-all.txt`

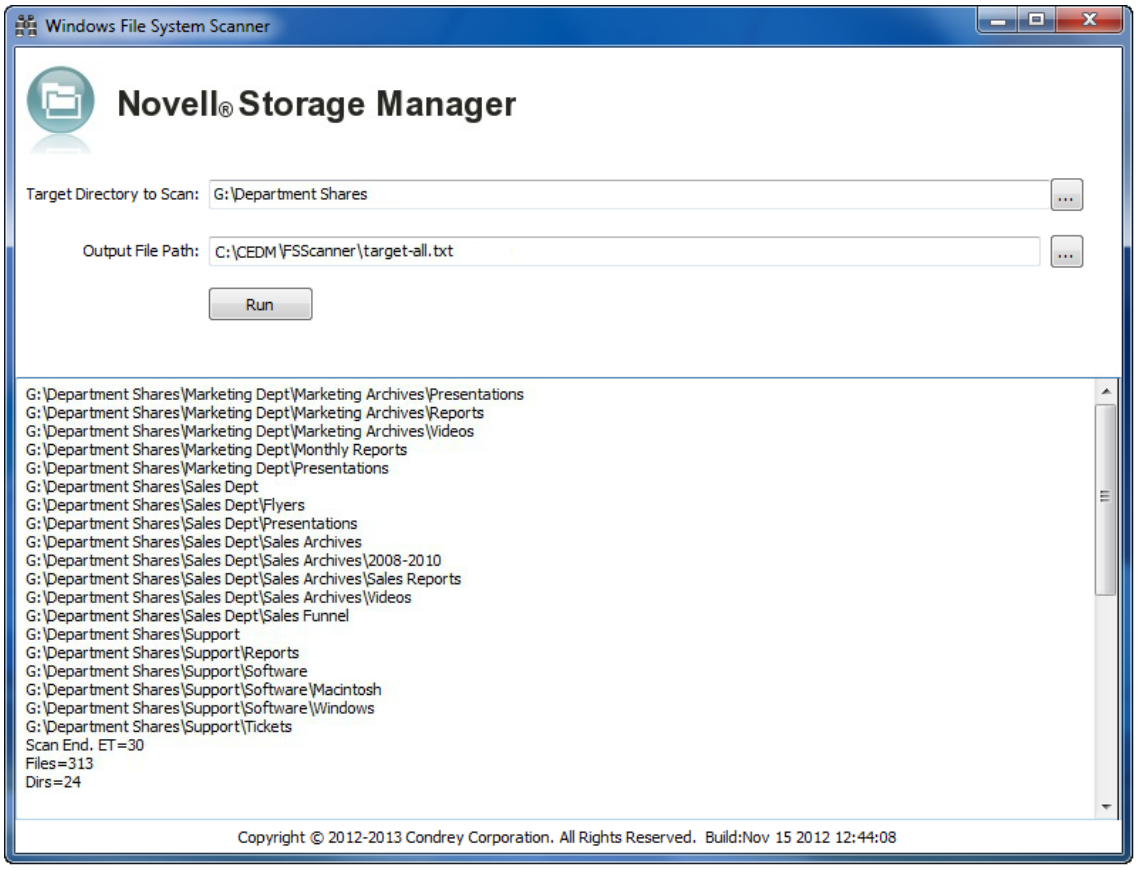

Open
CEDM ▸ WinScan
Search
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
HQ (G:)
Atlanta (J:)
London (K:)
Name
Date modified
Type
WinScan.exe
11/9/2012 2:25 PM
Application
File name:
target-all.txt
Open
Cancel

4 Click *Open*.



5 Click *Run*.

All of the files for the target path are displayed.



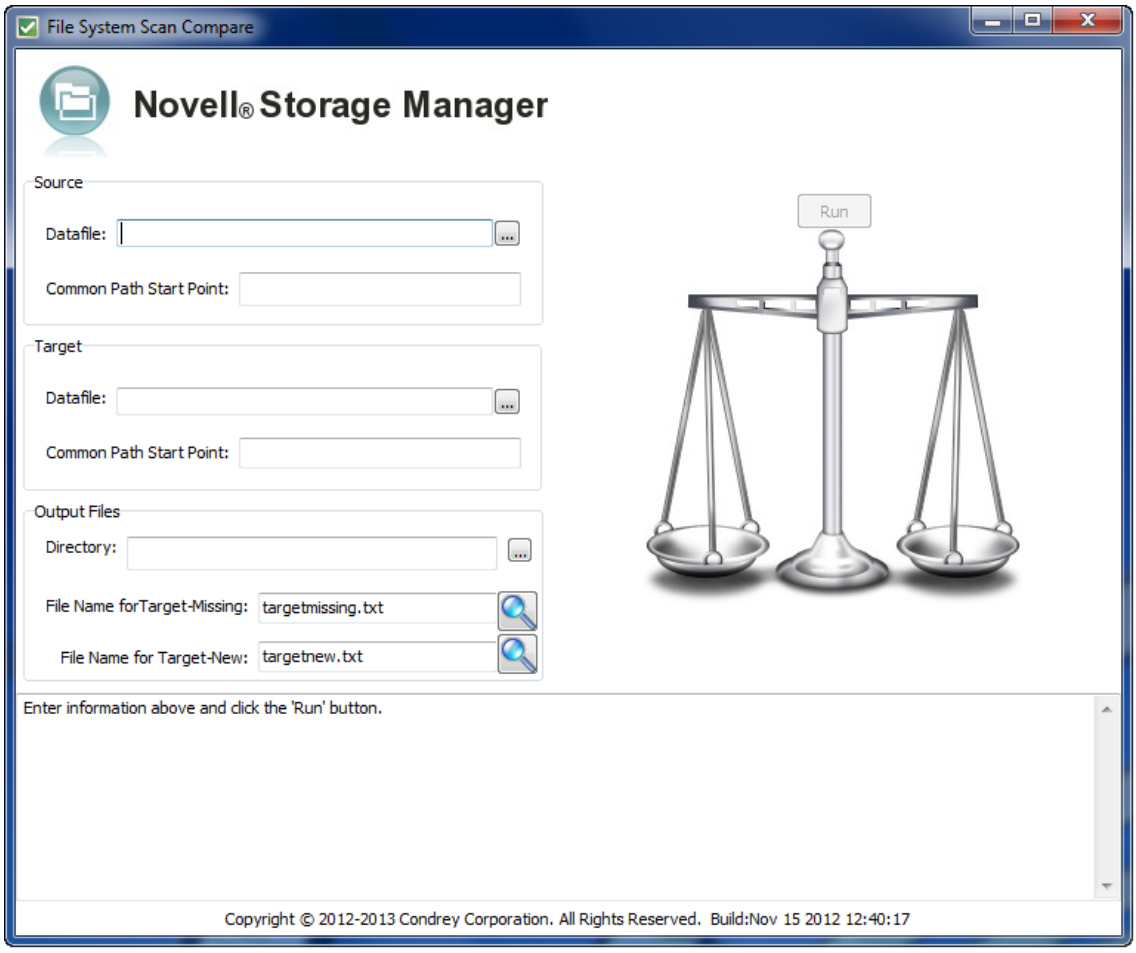
6 Close the WinScan utility.

7 Continue with "Comparing the Source and Target Lists" on page 193.

Comparing the Source and Target Lists

With file lists generated from the source and target servers, you can now compare the two lists by using the ScanCompare utility.

1 From the `CEDM` folder that you copied in Step 2a on page 167, open the `ScanCompare` folder and launch the ScanCompare utility.



2 In the *Source* region, click the browse button for the *Datafile* field, then browse to and select the `.job` text file that you observed in Step 5 on page 189.

3 In the *Target* region, click the browse button for the *Datafile* field, then browse to and select the text file that you created in Step 3 on page 190.

After you have specified the source and target files, the *Common Path Start Point* fields automatically display the first line of each file.

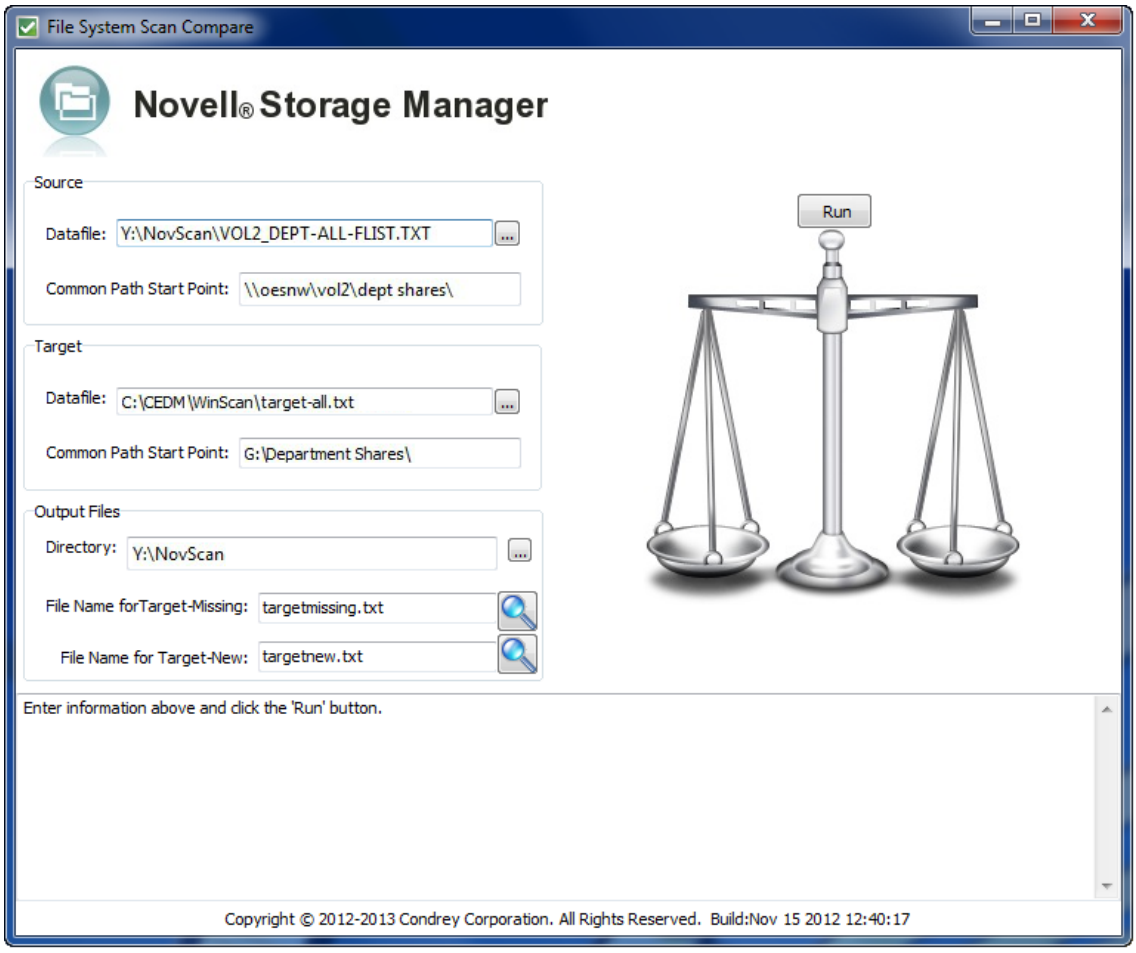
The next task is to specify a common starting point for the file comparison.

4 In the *Source* region, edit the path so that it concludes with the directory name containing the subfolders and files that you migrated earlier.

For example: `\\oesnw\vol2\dept shares`

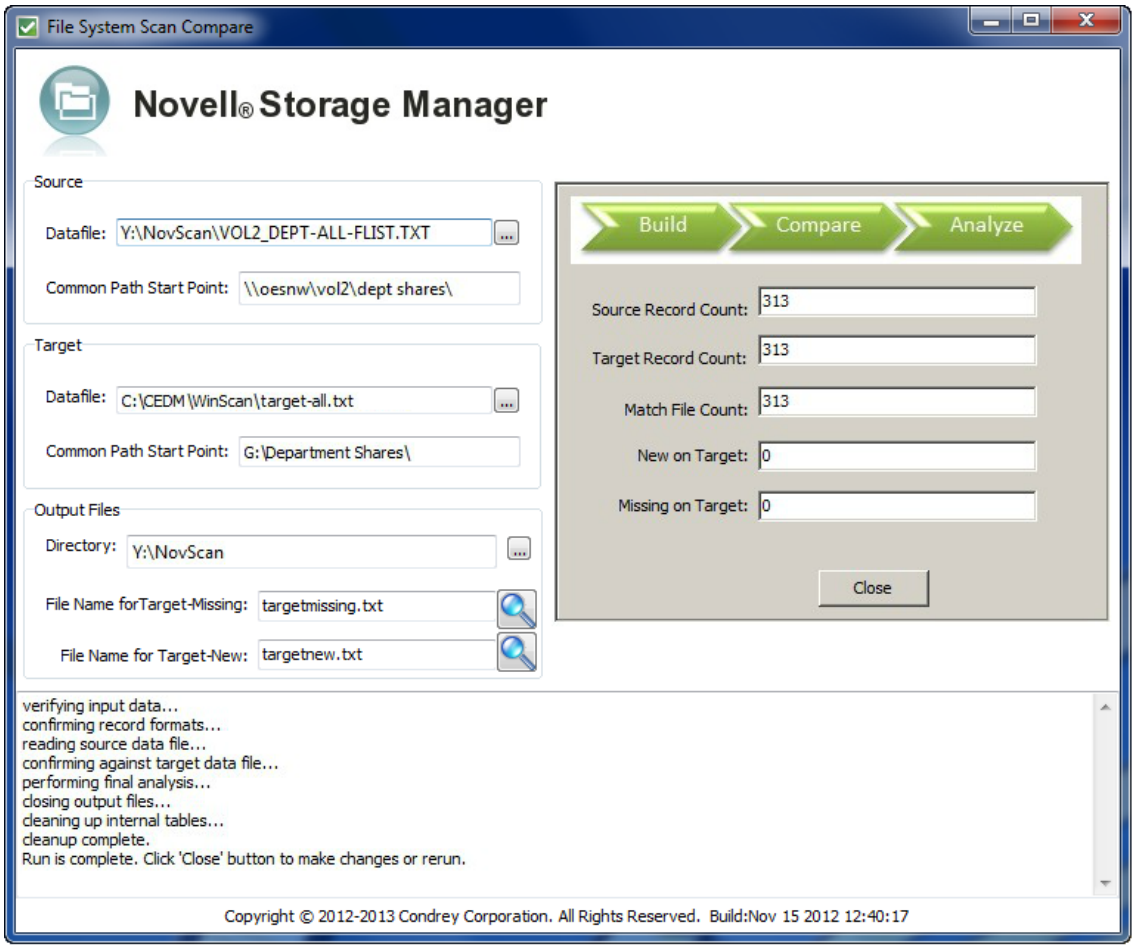
5 In the *Target* region, edit the path so that it concludes with the folder name containing the subfolders and files that were migrated earlier.

For example: `G:\Department Shares\`



6 Click *Run*.

The ScanCompare utility compares the files and displays the findings.



7 Use the findings to verify that all files were migrated.

If the *New on Target* or *Missing on Target* fields display entries other than zero, you will need to review the `targetnew.txt` or `targetmissing.txt` files to determine the cause of the source and target record count discrepancy.

You are now finished with both phases of the folder to folder migration.

11.12.2 Creating a Target Folder in the Data Migration Wizard

1 Make sure you have completed the prerequisites and have created a migration proxy account.

For more information on the prerequisites, see Section 11.3, “Prerequisites,” on page 115. For more information on creating a migration proxy account, see Section 11.4, “Creating the Migration Proxy Account,” on page 117.

2 (Conditional) If you want to migrate closed files now and skip some files to migrate later, complete the following steps:

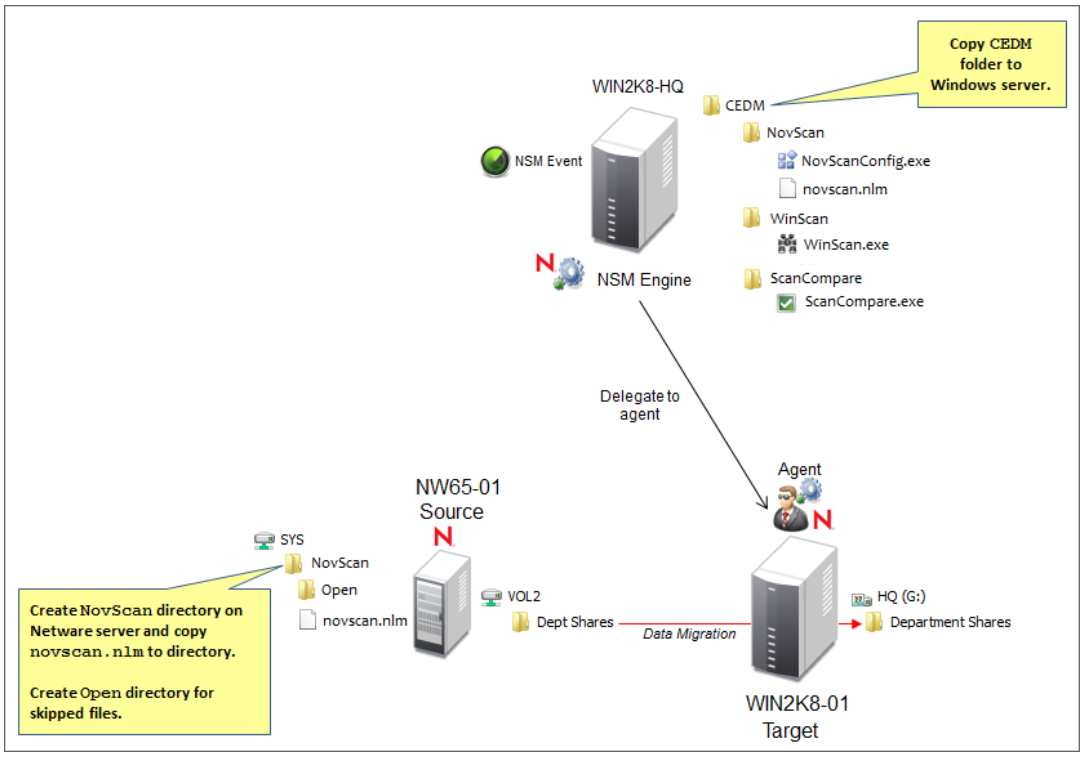
2a From the Novell Storage Manager ISO image, copy the `CEDM` folder to the Windows target server.

2b On each NetWare server from which you are going to migrate data, create a `NovScan` directory.

2c From the Novell Storage Manager ISO image, copy the `novscan.nlm` file from the `Utilities\CEDM\NovScan` folder to the NovScan directory you created in Step 2b.

2d In the new `NovScan` directory, create a new subdirectory and name it `Open`.

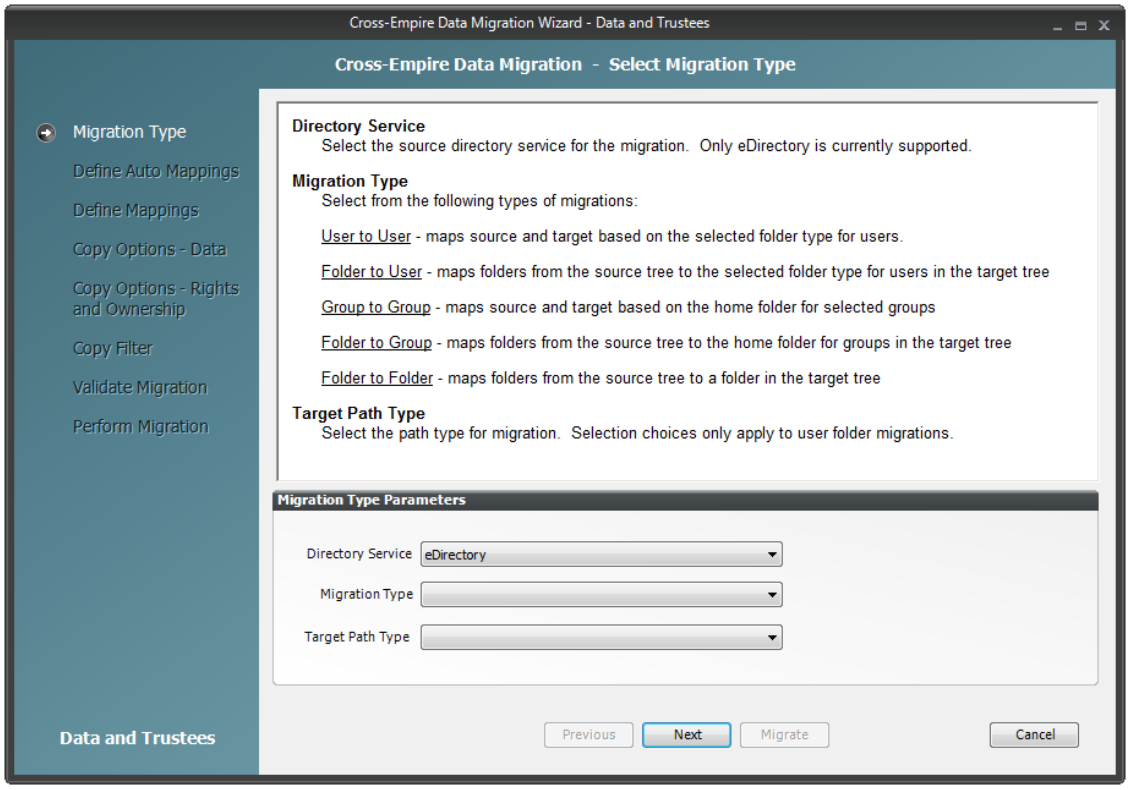
Figure 11-2 *Summary of Substeps to Complete.*



3 In NSMAdmin, click the *Main* tab.

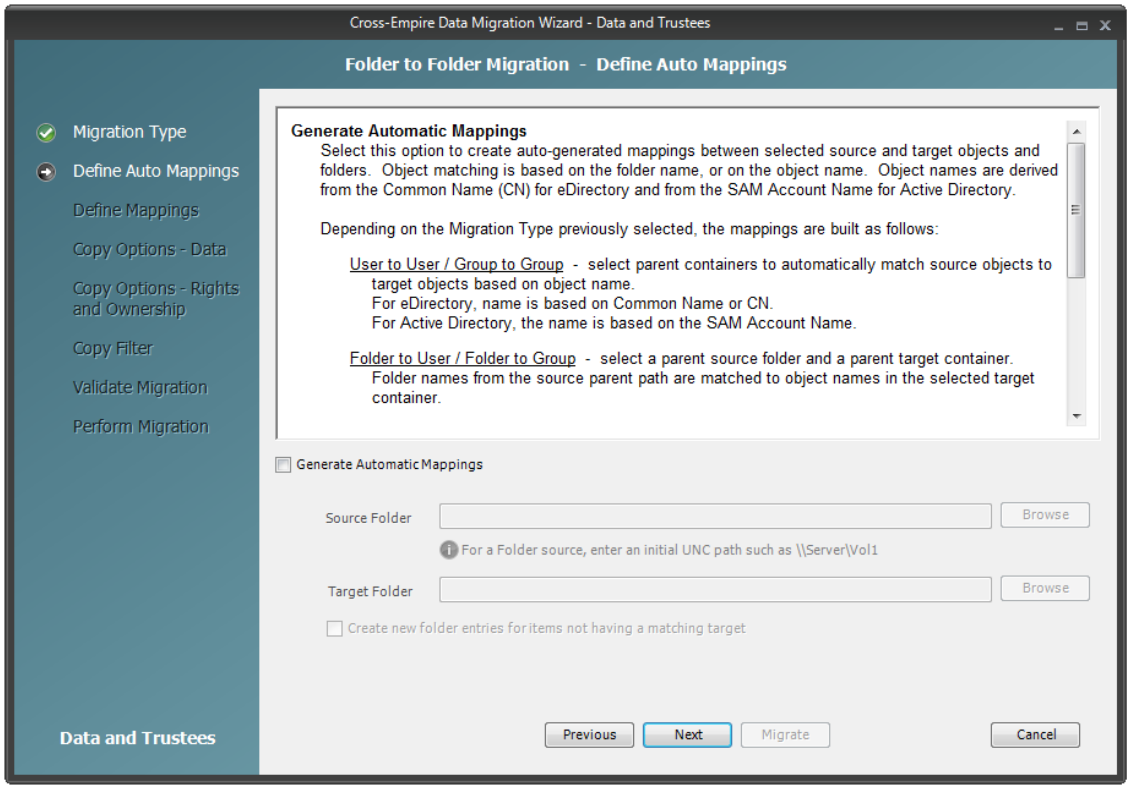
4 Click *Data Migration*.

5 Click *Migrate Data and Trustees*.



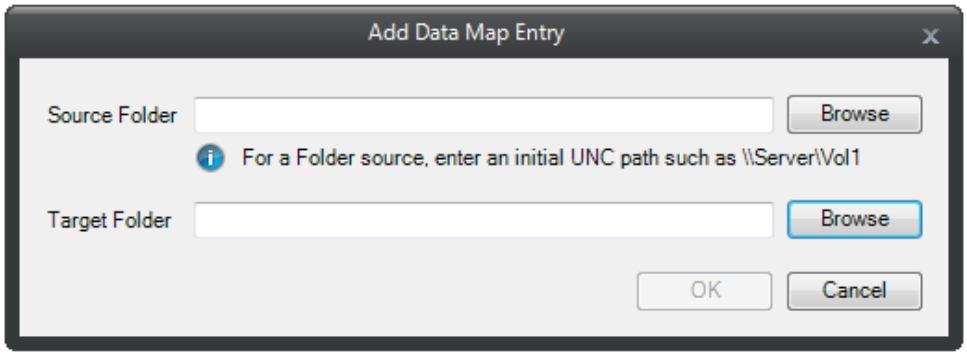
6 From the *Migration Type* drop-down menu, select *Folder to Folder*.

7 Click *Next*.



8 Click *Next*.

9 Click *Add*.



10 In the *Source Folder* field, specify an initial UNC path for a server and volume to browse.

For example, `\\server_name\volume_name\` or `\\ip_address\volume_name`.

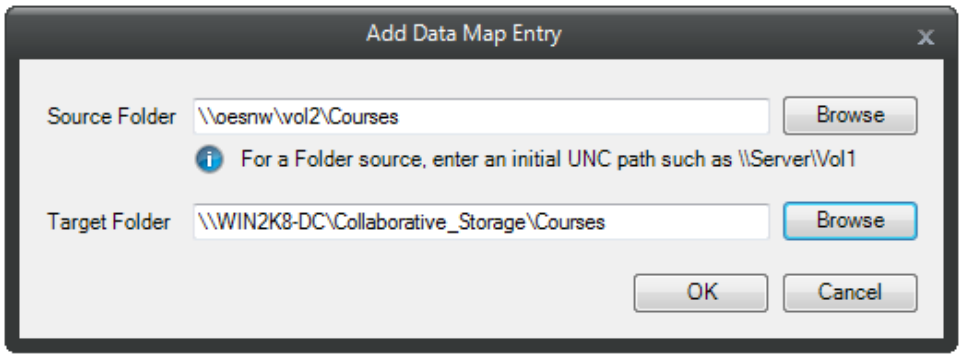
After a path is entered, you can click the *Browse* button to browse to the folder you want.

11 Click the *Browse* button that corresponds to the *Target Folder* field to locate the share where you want to create the new folder for the migrated data.

12 Right-click the share, select *Create Folder*, name the new folder, and click *OK*.

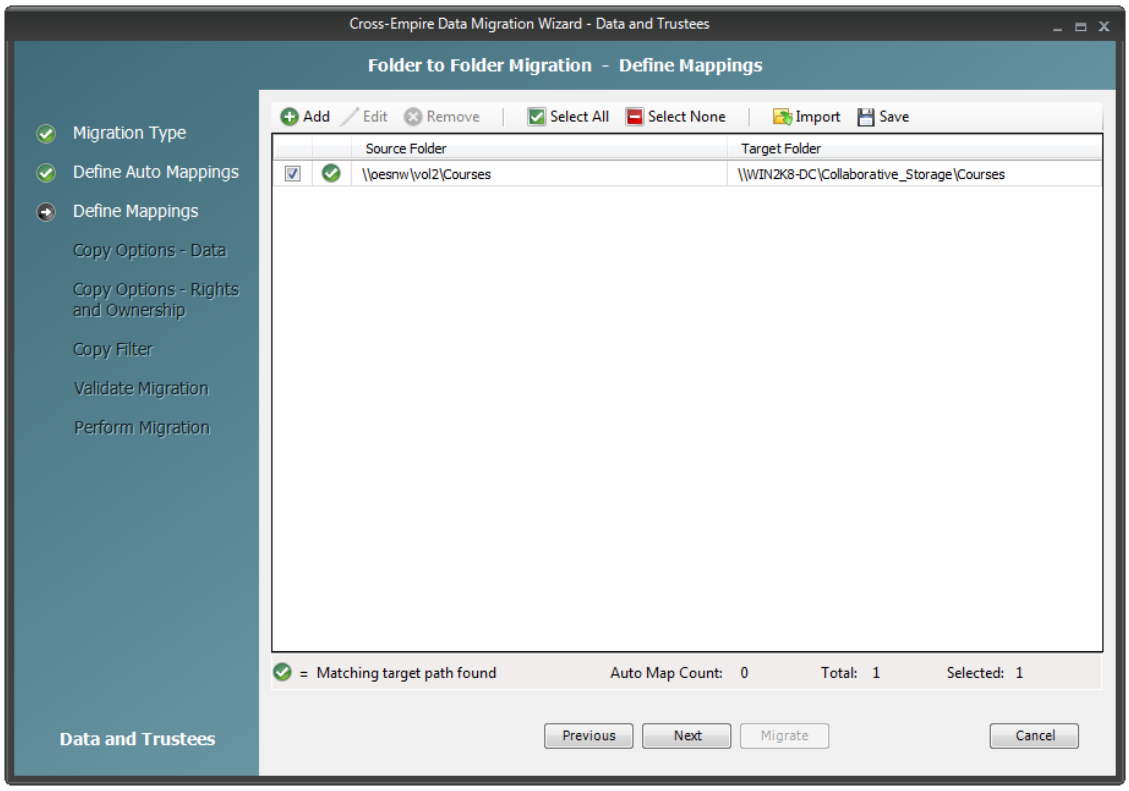
13 Click *OK* to close the Target File System Path Browser.

14 In the Add Data Map Entry dialog box, click the *Browse* button that corresponds to the *Target Folder* field again, browse to and select the new folder, then click *OK*.

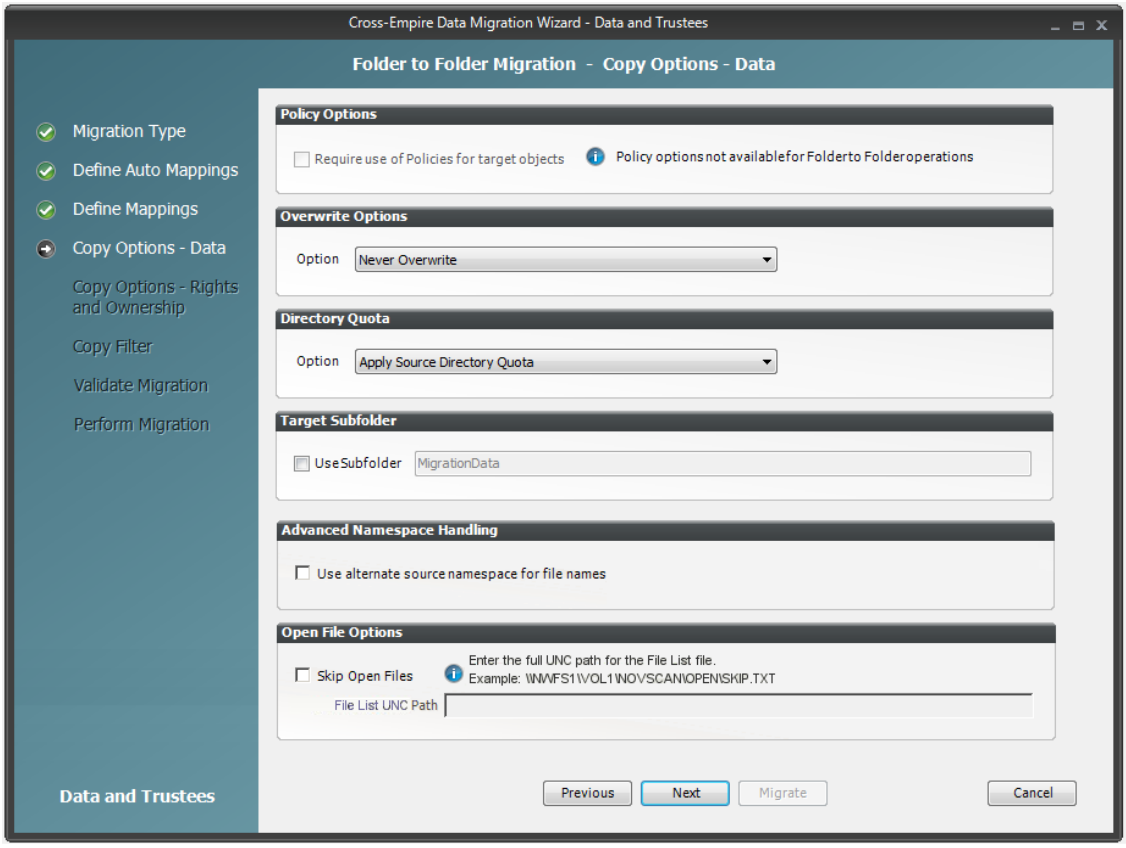


15 Click *OK*.

The defined source and target mappings are displayed.



16 Click *Next*.



17 Fill in the following fields:

Overwrite Options: Indicate what you want to take place when duplicate filenames are encountered in the source and target.

Directory Quota: Specify how quota settings from the source Novell file system should be applied after the migration.

Target Subfolder: If you want migrated data to be placed in a subfolder, select the *Use subfolder* check box and specify the subfolder name in the field.

Advanced Namespace Handling: Selecting this check box allows the Cross-Empire Data Migration subsystem to look for alternate namespaces for files that the Novell file system cannot resolve and therefore cannot migrate.

For example, files originally saved on a Mac or Linux system might use characters that the Novell file system cannot recognize. By looking for an alternative namespace, the Novell file system might be able to resolve the problem and migrate the file.

Open File Options: If you want the Cross-Empire Data Migration subsystem to skip all open files on the network and not migrate them, select *Skip Open Files*.

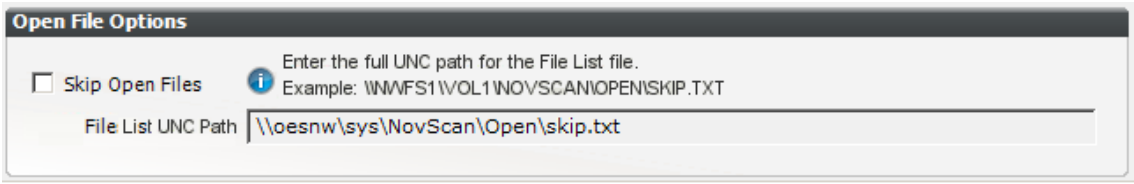
Selecting *Skip Open Files* activates the *File List UNC Path* field where you specify the name and location of the log file listing all of the open files that are skipped during the migration.

Specify the UNC path for the directory you created in Step 2d on page 197 along with a filename for the text file that will list the skipped files.

For example, `\\server_name\volume_name\directory_name\Open\skip.txt`

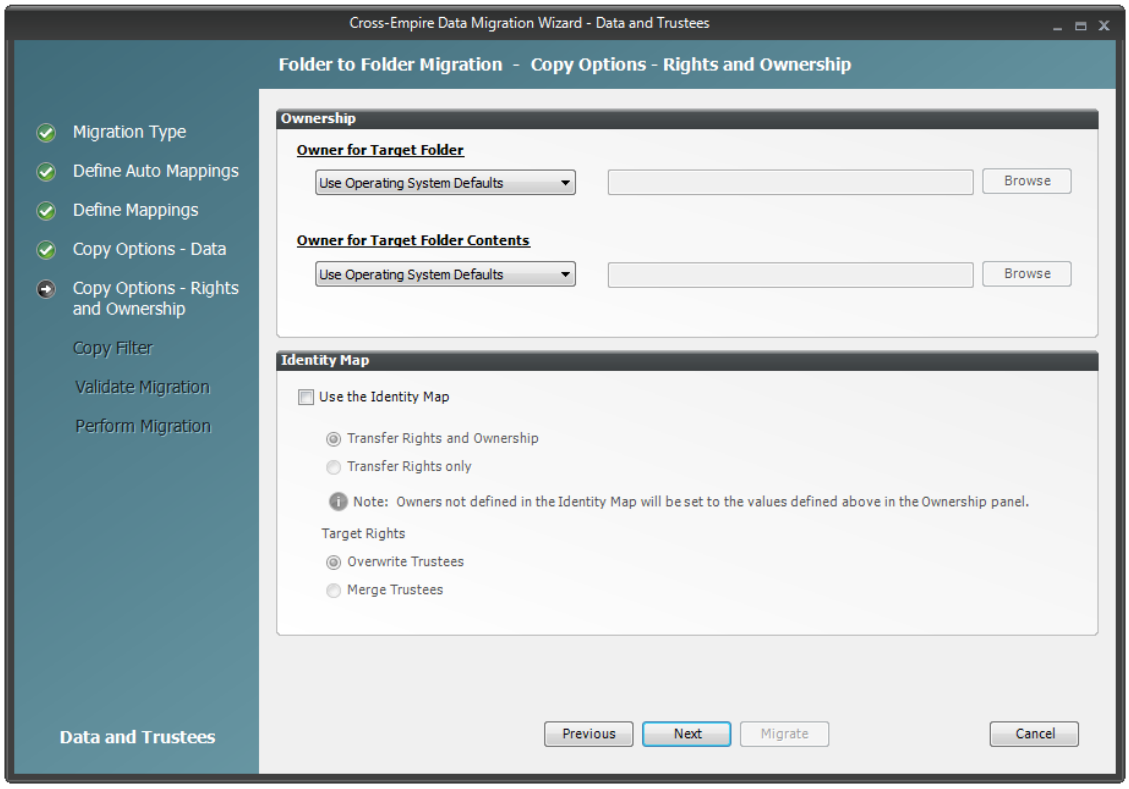
or

`\\ip_address\volume_name\Open\skip.txt`



The Cross-Empire Data Migration subsystem does not validate the path, so you must make sure that the path entered is correct. Otherwise, the migration fails.

18 Click *Next*.



19 Fill in the following fields:

Owner for Target Folder: Use these settings to specify how ownership of the migrated folder is determined.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the setting on the target server.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder.

Owner for Target Folder Contents: Use these settings to specify how ownership of the migrated folder contents is determined.

- **Use Operating System Defaults:** This default setting allows the target Microsoft Windows Server to adjust the file ownership according to the settings on the target server.
- **Set Explicit Owner:** Allows you to browse and select an object as the explicit owner of the migrated folder.

Use the Identity Map: Select this check box if you want Novell Storage Manager to utilize the identity map you created earlier and use the corresponding IDs to copy security rights and file ownership from eDirectory to Microsoft Active Directory.

- **Transfer Rights and Ownership:** Select this option if you want to transfer the file and folder security rights along with the ownership settings.

  Be aware that when you transfer the ownership of a file or folder in a Windows network, you are granting the owner Full Rights, which you might not want to provide.
- **Transfer Rights Only:** Select this option to transfer only the file and folder security rights.
- **Overwrite Trustees:** Select this option to override any existing trustee assignments for a target file or folder with the established Novell eDirectory trustee assignments for those files and folders.
- **Merge Trustees:** Select this option to merge the established Novell eDirectory trustee assignments with those of the target files or folders in Active Directory.

20 Click *Next*.

21 (Conditional) If you want to use a filter to include or exclude specific files, select the *Use Copy Filter* check box and click the *Add* button.

21a Fill in the following fields:

Description: Specify a description of the filter.

Action: From the drop-down menu, select either *Migrate* or *Ignore*, based on whether the filter specifies to migrate files or folders or to ignore them.

Files, Folders: Specify if the filter applies to files or folders.

Masks: List the file types to migrate or ignore.

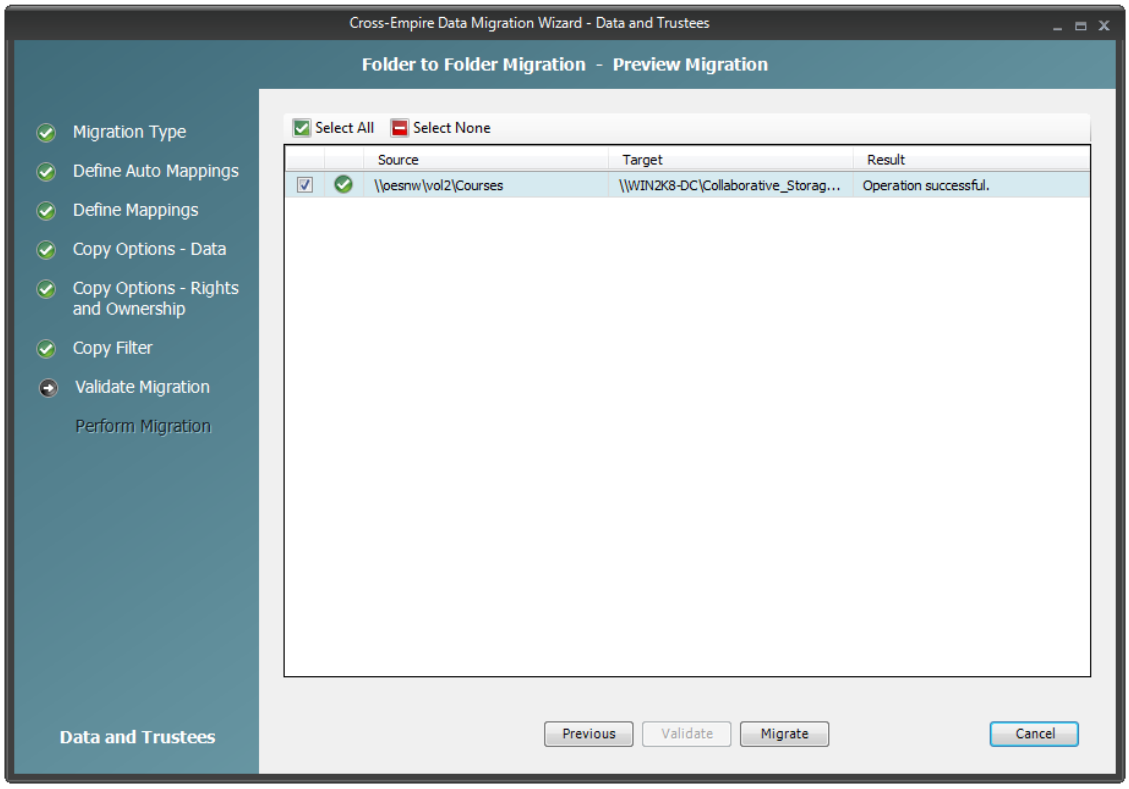
21b Specify any additional filter criteria in the menus and fields that remain.

For a detailed explanation of this region of the dialog box, see Section 5.5.8, “Setting Vault Rules,” on page 49.

21c Click *OK*.

22 Click *Validate*.

Validate shows the result of certain checks that can be run prior to the migration. The *Result* column shows the status of the validation checks. If errors are displayed, you can choose to correct those errors prior to running the migration.



23 (Conditional) Take any necessary action in the Active Directory target and then re-run the Data Migration Wizard.

24 Click *Migrate*.

A page appears with details of the data migration events that are queued for processing. To view the status of migration events, click *Pending Events*. For more information on Pending Events, see Section 12.1.6, "Pending Events," on page 219.

25 Do one of the following:

- If you skipped some files to migrate later, click *Finish* and then continue with "Migrating Skipped Files" on page 175.
- If you have migrated all of you data, click *Finish*.

  You are now finished with the folder to folder migration.

12 Reference

This section presents the tabs and tools in NSMAdmin in a reference format. All of the tools are covered as they are presented in the NSMAdmin interface, beginning with the *Main* tab.

- Section 12.1, “Main Tab,” on page 205
- Section 12.2, “Reports Tab,” on page 224
- Section 12.3, “Configure Tab,” on page 230

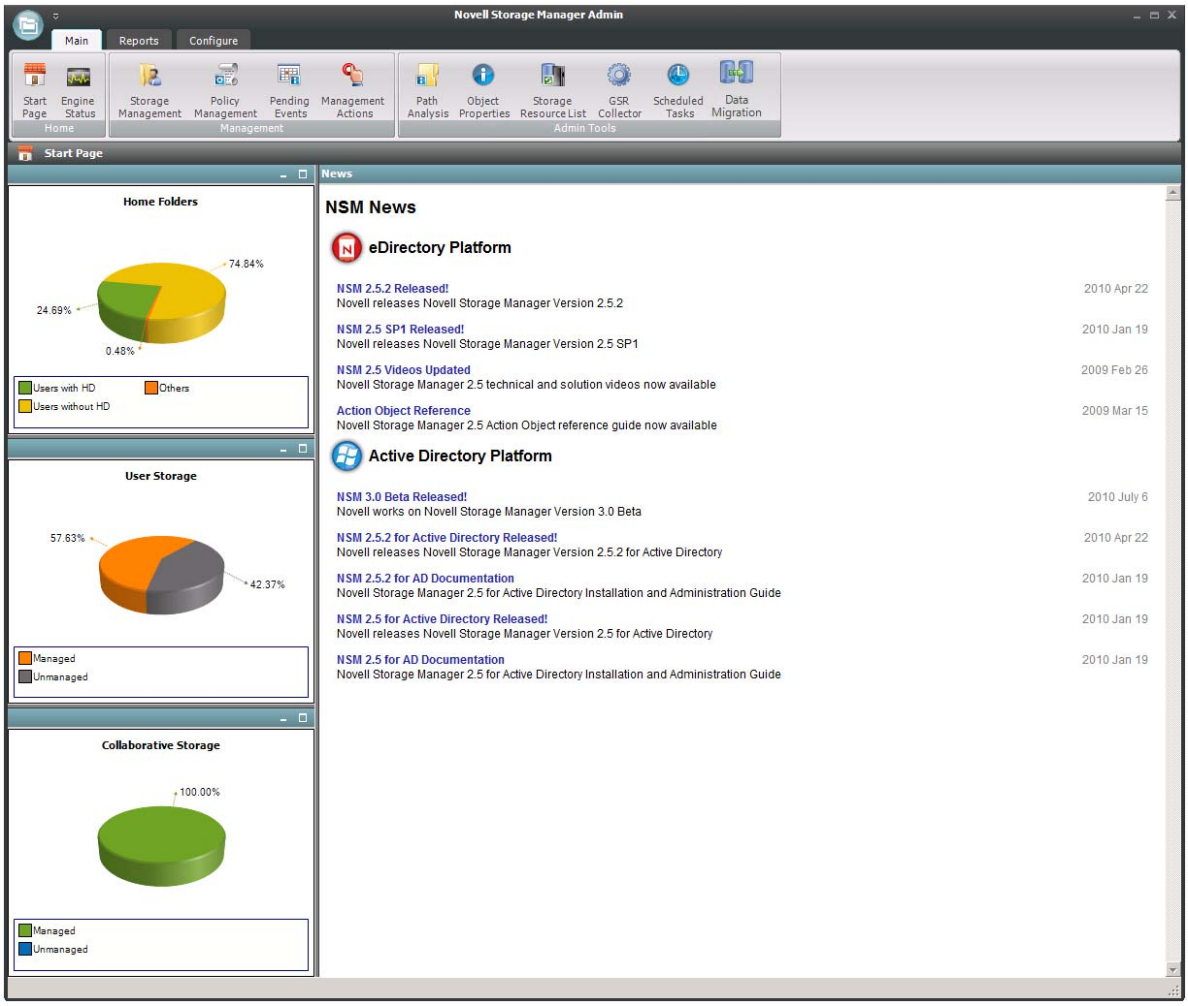
12.1 Main Tab

The *Main* tab provides access to all of the active management interfaces for Novell Storage Manager. You use the *Main* tab to create, edit, deploy, and analyze Novell Storage Manager policies.

- Section 12.1.1, “Start Page,” on page 205
- Section 12.1.2, “Engine Status,” on page 206
- Section 12.1.3, “Storage Management,” on page 207
- Section 12.1.4, “Management Actions,” on page 209
- Section 12.1.5, “Policy Management,” on page 216
- Section 12.1.6, “Pending Events,” on page 219
- Section 12.1.7, “Path Analysis,” on page 220
- Section 12.1.8, “Object Properties,” on page 221
- Section 12.1.9, “Storage Resource List,” on page 221
- Section 12.1.10, “GSR Collector,” on page 223
- Section 12.1.11, “Scheduled Tasks,” on page 224
- Section 12.1.12, “Data Migration,” on page 224

12.1.1 Start Page

The left panes of the Start Page tool display an at-a-glance view of the management status of user storage, collaborative storage, and users and groups that have home folders. The right pane displays links to resources and product news.

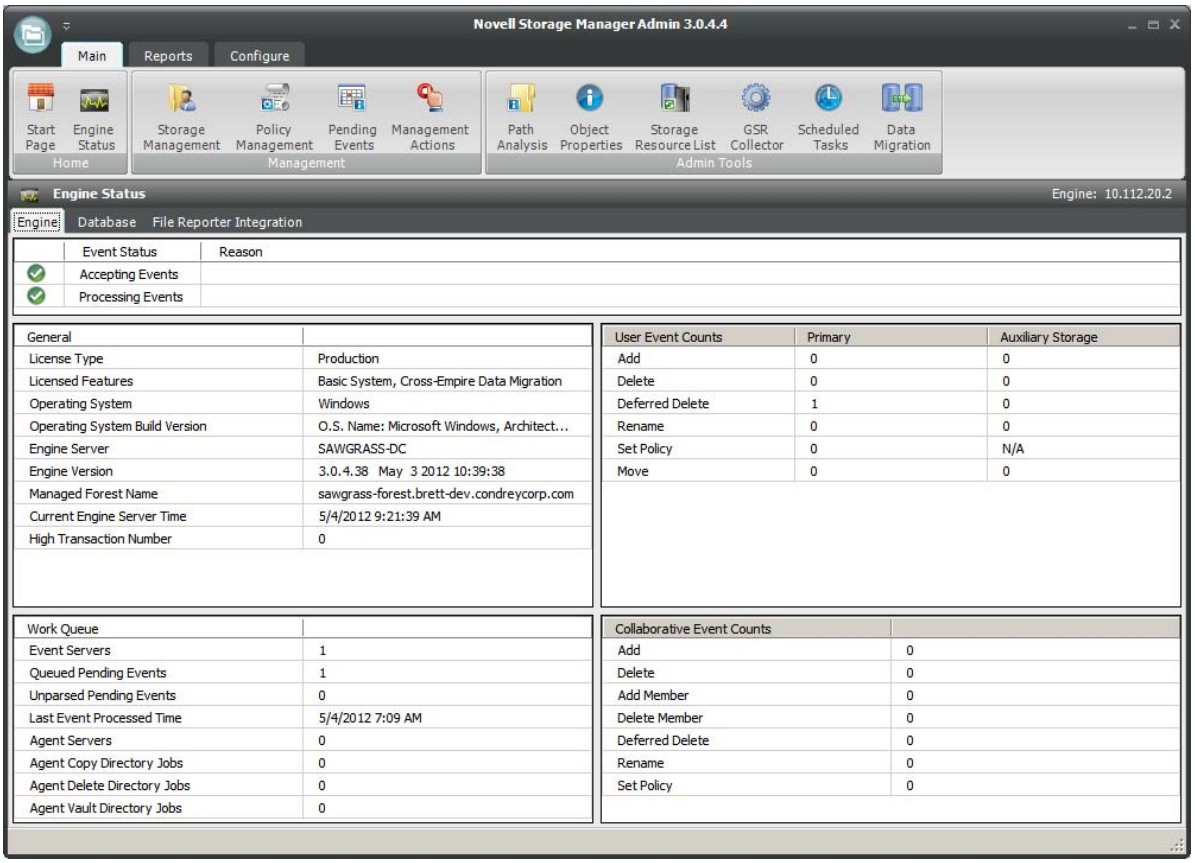


12.1.2 Engine Status

The Engine Status page provides an overview of the current status of the NSM Engine through the *Engine* tab. If you are not seeing Novell Storage Manager enact actions after events in Active Directory take place, viewing whether the NSM Engine is processing and accepting events through this page is a good first step in troubleshooting.

Expanded details pertaining to events are detailed in different regions of the page. The General region provides general details including naming and version numbers. The User Event Counts region displays user storage actions. The Work Queue region provides details on actions yet to be completed. The Collaborative Event Counts region provides collaborative storage actions.

Figure 12-1 *Engine Status Page*



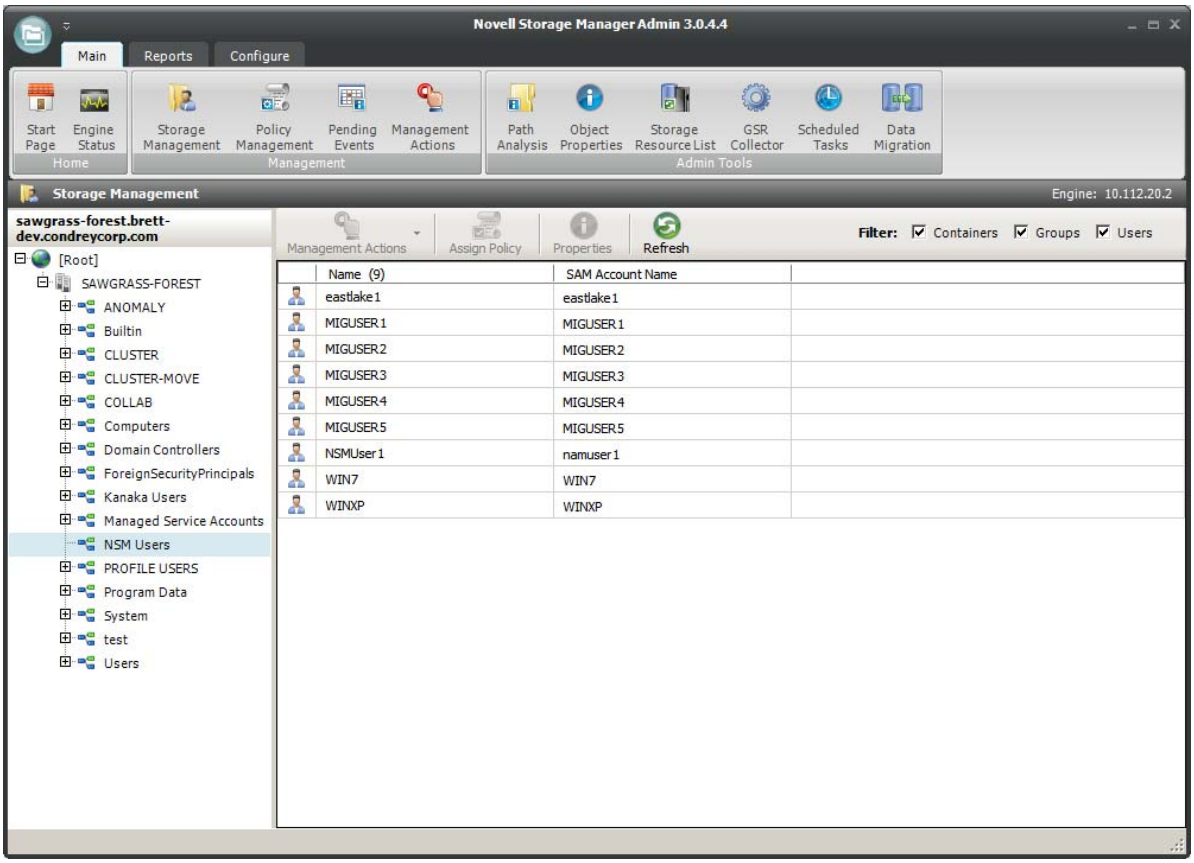
If you have Novell File Reporter installed in your network, you can click the *File Reporter Integration* tab to view the status of the integration between Novell Storage Manager and Novell File Reporter.

NOTE: Novell File Reporter reports on Novell Storage Manager policies through a plug-in installed in NSMAdmin. The plug-in allows administrators to create Novell Storage Manager detailed, policy-based storage reports by reporting on the target paths associated with Novell Storage Manager policies. For more details, see Section 4.6, "Configuring Novell Storage Manager to Work with Novell File Reporter (Conditional)" in the *Novell File Reporter 1.0.1 Installation Guide* (http://www.novell.com/documentation/filereporter10/file_reporter_install/?page=/documentation/filereporter10/file_reporter_install/data/a20gkue.html).

12.1.3 Storage Management

The Storage Management tool lets you manage the associations between Novell Storage Manager policies and Active Directory objects such as organizational units, groups and users. This includes creating organizational units, setting context, viewing properties, performing Management Actions, and assigning policies.

Figure 12-2 *Storage Management Page*



Left Pane

Use the left pane to browse and select organizational units in the directory. Right-clicking an organizational unit in the left pane lets you take additional actions:

- Create an organizational unit (OU)
- Set the directory context in the left pane to display the hierarchy from the root or from the selected organizational unit

Right Pane

Use the right pane to view the objects within a selected organizational unit as well as view properties, perform Management Actions, and assign policies. The right pane displays containers (organizational units), groups, and users, according to what you have selected in the Filter check boxes.

The right pane also provides details such as whether the User or Group object is managed through Novell Storage Manager, if it has an assigned and effective policy, and more.

IMPORTANT: When you perform actions in the right pane, it is important that you know whether you are performing management specific to users, groups, or organizational units (containers).

12.1.4 Management Actions

In managing user and collaborative storage with Novell Storage Manager, there are cases when you need to retroactively apply policies, rights, attributes, and quotas to existing user storage, or perform some administrative corrective action or operation on a large set of users, groups, or containers.

In Novell Storage Manager, performing these types of operations is collectively referred to as performing a Management Action, and is done through the Storage Management page by right-clicking the object and selecting *Management Action*, or clicking the *Management Actions* drop-down menu.

You can perform a Management Action on an organizational unit, a Group object, or a User object. Management Action operations on a Group object apply to users who are members of the group. Management Action operations on an organizational unit apply to users in the organizational unit, and optionally to all subordinate organizational units.

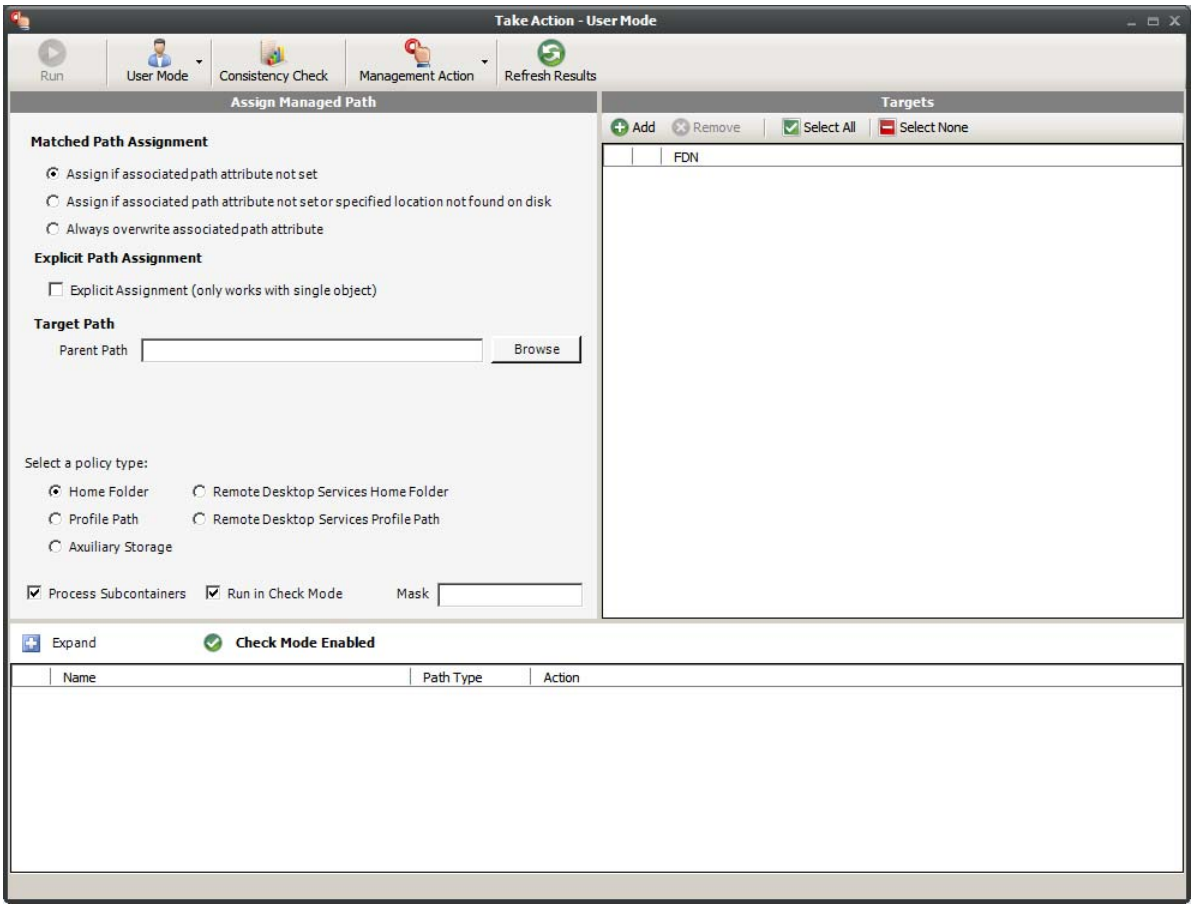
Novell Storage Manager analyzes each User object independently, regardless of whether the Management Action is initiated via organizational unit, Group objects, or User objects.

- "Management Actions Dialog Box" on page 209
- "Available Management Actions" on page 211
- "Assign Policy" on page 215
- "Object Properties" on page 216

Management Actions Dialog Box

Whenever you initiate a Management Action, you work in a dialog box similar to the one below. A description of the components follows the graphic.

Figure 12-3 *Management Action Dialog Box*



Run: Clicking this button executes the management action.

Mode: This drop-down menu lets you indicate if the Management Action is to apply to User, Group, or Container policy.

Consistency Check: This button lets you perform a consistency check before determining what Management Actions to perform. You can also use the *Consistency Check* button to view the results after you perform a Management Action.

Management Action: This drop-down menu lets you change from one Management Action to another while you are in the dialog box.

Refresh Results: This button refreshes the results displayed in the bottom pane of the dialog box.

Top Left Pane: The fields, options, and check boxes in this region vary based on the Management Action you are performing. In some cases, there is nothing in this region, because there are no settings to create. This region includes some powerful options for Management Actions, including the following:

- Process Subcontainers
- Run in Check Mode
- Mask

When you perform a Management Action on an organizational unit, Novell Storage Manager applies the action to all subcontainers. If you do not want the action applied to subcontainers, you can deselect the *Process Subcontainers* check box.

The *Run in Check Mode* check box lets you view the potential outcome of performing a Management Action before you actually perform the action. The action is evaluated and all tasks associated with the action are listed. We recommend that you perform all Management Actions in check mode and observe the outcomes before actually performing a Management Action.

For Management Actions performed on organizational units or Group objects, you can enter a search filter in the *Mask* field to limit the number of objects that Novell Storage Manager analyzes. You can enter standard wildcard characters with multiple strings separated by the "|" character.

Top Right Pane: This part of the dialog box lets you add, delete, or select objects to which the Management Action applies.

Bottom Pane: This part of the dialog box displays the results after the Management Action has taken place. To expand the viewable area, click *Expand*.

Available Management Actions

- "Consistency Check" on page 211
- "Manage" on page 212
- "Enforce Policy Paths" on page 212
- "Groom" on page 212
- "Apply Attributes" on page 212
- "Apply Home Drive" on page 212
- "Apply Members" on page 212
- "Apply Ownership" on page 213
- "Apply Quota" on page 214
- "Apply Rights" on page 214
- "Apply Template" on page 214
- "Recover Managed Path Attribute" on page 215
- "Assign Managed Path" on page 215
- "Directory Merge" on page 215
- "Remove from Database" on page 215

Consistency Check

This Management Action notifies you of inconsistencies or potential problems pertaining to user and group storage being managed through Novell Storage Manager. These potential problems might be missing storage quotas, inconsistent directory attributes, missing home directories, inconsistent file paths, and more.

In addition to reporting on storage issues, consistency check reports let you review current quota assignments and can help you with the design and planning of storage policies. In Section 4.3, "Running Consistency Check Reports on Existing Storage," on page 25, you ran a consistency check before creating your first primary user policy to help you determine how to configure the policy.

Manage

This Management Action catalogs existing network users in Novell Storage Manager, putting them in a managed state.

If the existing users already have established home folders, attributes, and rights, Novell Storage Manager does not change these settings, nor does it enforce policy paths, grooming, and quota management. If you need to change attributes and rights, or enforce policy paths, grooming, and quotas, you can do so through the specific Management Actions.

If these existing users do not have established folders, Manage creates the home folders and sets the rights, attributes, quotas, etc. according to the policies that apply to the users.

Enforce Policy Paths

This Management Action moves data to where the policy's target path specifies. If you decide to move your user home folders from one location to another, you can simply change the target path in the policy and then run Enforce Policy Paths to move the home folders.

Groom

This Management Action carries out file grooming according to the file grooming specifications in the applied policy.

Apply Attributes

This Management Action lets you apply file system attributes. If you decide to modify the file system attributes in a policy, you can select *Apply Attributes* to immediately apply the new attributes for all of the affected users.

If you cataloged existing network users with existing home folders through Manage, the attributes for the home folder are not modified when a user and his or her associated home folder are cataloged (see Manage above). If you want to modify the original attributes for the home folder, you can do so through the settings in the in the left pane of the Apply Attributes dialog box.

Apply Home Drive

When the *Home Folder* check box is selected, this Management Action changes the home drive letter for the user that is assigned under Active Directory, to the drive letter that is specified in the Novell Storage Manager policy.

If you have a Novell Storage Manager Remote Desktop Services home folder policy and you want to apply the drive letter that is established in that policy, you can select the *Remote Desktop Services Home Folder* check box.

NOTE: The new drive letter does not take effect until the user logs out and then logs in again.

Apply Members

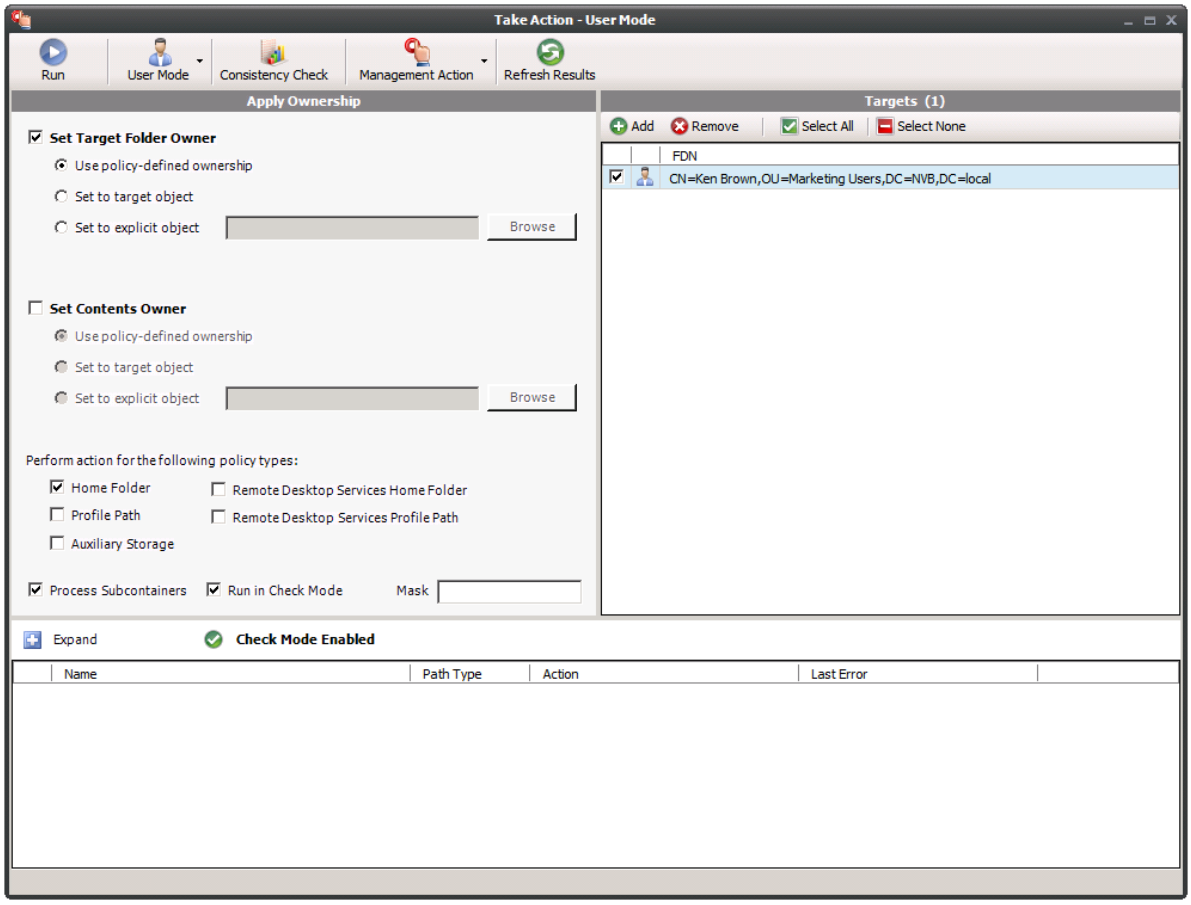
This Management Action is included to create the owner folder and personal folders in a collaborative storage area, where these folders did not exist previously. You must first modify the collaborative storage template in the policy to include -OWNER- and -MEMBER-. For more information, see Chapter 7, "Managing Collaborative Storage," on page 77.

If you do have personal folders in the collaborative storage area and you later change the rights on -MEMBER-, you use the Apply Members Management Action to enforce the new rights.

Apply Ownership

This Management Action lets you set ownership of the home folder and home folder contents.

Figure 12-4 *Apply Ownership Management Action Page.*



NOTE: The ownership specifications you make on the page shown above are applied to folders and files that exist at the time the Management Action takes place. The ownership of files and folders that are created later is not affected by this action. For example, if a user's home folder is moved due to an Enforce Policy Path action, the ownership of the user's home folder will be determined by the settings in the policy.

Set Target Folder Owner: Select this check box to specify that the ownership applies only to the home folder and not to any subfolders.

Use policy-defined ownership: This option sets the home folder owner according to the specified owner in the *Path Owner* field of the policy.

Set to target object: When this option is selected, each of the selected users' home folders is set to have that user object as the owner.

Set to explicit object: This option lets you browse to select a specific owner for the home folder.

Set Contents Owner: Select this check box to specify that the ownership applies to the subfolders and files contained in the home folder.

Use policy-defined ownership: This option sets the home folder contents owner according to the specified owner in the *Path Owner* field of the policy.

Set to target object: When this option is selected, each of the selected users' home folders is set to have that user object as the owner.

Set to explicit object: This option lets you browse to select a specific owner for the contents of the home folder.

Perform action for the following policy types: Specify the policy types you want this Management Action to apply to.

Process Subcontainers: Selecting this option specifies that you want the settings on this page to apply to users that reside in the subcontainers within the container where this policy is applied.

Run in check mode: Selecting this check box lets you view the potential outcome of performing a Management Action before you actually perform it. The action is evaluated and all tasks associated with the action are listed. We recommend that you perform all Management Actions in check mode and observe the outcomes before actually performing a Management Action.

Mask: For Management Actions performed on organizational units or Group objects, you can enter a search filter in the *Mask* field to limit the number of objects that Novell Storage Manager analyzes. You can enter standard wildcard characters with multiple strings separated by the "|" character.

Apply Quota

This Management Action lets you apply home folder and collaborative storage quotas. If you decide to modify the quota settings in a policy, you can select *Apply Quota* to immediately apply the new quota setting to all of the affected users.

If you cataloged existing network users with existing home folders through Manage, there might be no quota settings for the user home folders. Or, the quota settings might be inconsistent with those specified in the policy. If you want to establish or reset the quota for the home folder, you can do so through the settings in the in the left pane of the Apply Quota dialog box.

Apply Rights

This Management Action lets you apply file system rights. If you decide to modify the file system rights in a policy, you can select *Apply Rights* to immediately apply the new rights for all of the affected users.

Apply Template

This Management Action lets you apply a template specifying how to provision user or collaborative storage. If you decide to modify the template in a policy, you can select *Apply Template* to immediately apply the new template structure to all of the affected users. This can be especially useful if you need to quickly provision a new subfolder with a document, such as a new health benefits document for all employees. All you need to do is modify the template to include the new subfolder and document inside the subfolder and then use Apply Template to provision it to everyone.

If you cataloged existing network users with existing home folders through Manage, the file structure created by the template is not modified after the user and his or her associated home folder are cataloged (see Manage above). If you want to modify the original file structure for the home folder, you can do so through the settings in the in the left pane of the Apply Template dialog box.

Recover Managed Path Attribute

If the attribute for a user home folder, profile path, Remote Desktop Services home folder, or Remote Desktop Services profile path ever becomes corrupted, this Management Action can be used to recover an uncorrupted version of the attribute from the Novell Storage Manager database.

Assign Managed Path

You can use this Management Action to assign an attribute to a user folder, profile path, Remote Desktop Services home folder, or Remote Desktop Services profile path.

Directory Merge

This Management Action lets you merge contents of one home folder with those of another. This is especially useful if a user leaves an organization and you want to transition the files from the former user to another user. Another example might be if a user has two home folders and wanted to merge the contents into one.

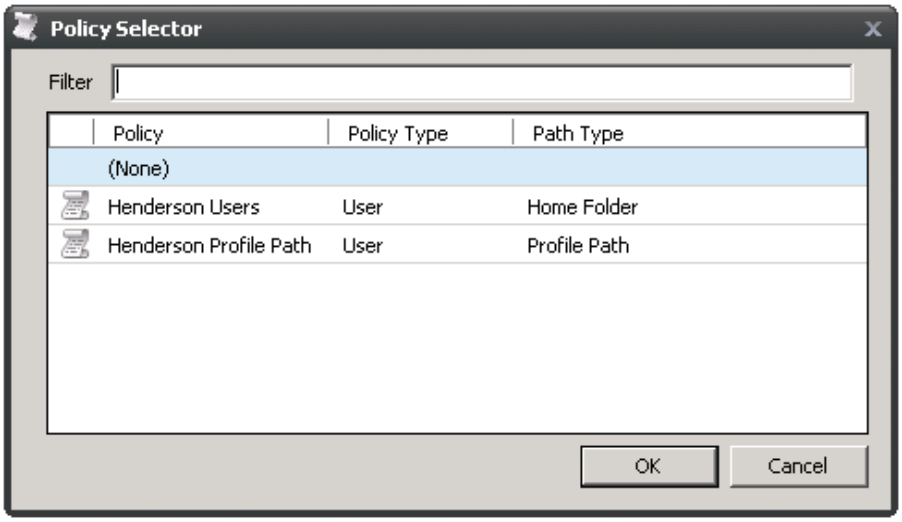
Remove from Database

This Management Action removes object from the Novell Storage Manager database and makes the object unmanaged.

Assign Policy

Lets you easily assign a User, Group, or Organizational Unit object a policy while you are in the Storage Management page. If an effective policy is already assigned to one of these objects, you can assign a new policy, replacing the effective policy with an assigned policy.

Figure 12-5 *Policy Selector Dialog Box*



The *Filter* field filters policy names as you type.

Object Properties

You can easily view an expanded set of object properties in the Storage Management page by right-clicking an object in the right pane and selecting *Object Properties*.

The five tabs display the following information:

Properties: Displays Active Directory values and NSM Engine database values. If you are working with a Novell Support representative to resolve a problem, you might need to provide information from this screen.

Effective Policies: Lists all of the effective policies for the selected object. An effective policy is a policy that affects a user either directly through association or inheritance by membership in a domain, container, group, or domain.

Associated Policies: Lists all of the associated policies for an object. An associated policy is an explicitly assigned policy associated with a domain, container, group, or user.

Transactions: Shows pending events for the selected object. If there are many pending events, but you only want to see those pertaining to a particular user, you can see the pending events for the User object.

History: Shows a history of move and rename events that pertain to the selected User object.

Having historical information can be beneficial for a number of reasons. One in particular is for restoring files. Suppose a project manager was working on a project three years ago and then the company decided to discontinue funding the project. After one year, the project manager decided to delete the project files from her personal folder. Now suppose that two years later, a new executive in the organization wants to renew the project. To locate the original project files from backed up storage would be quite time consuming, but by viewing the information in the History tab, you could easily find the original location of the backed up home folder, if it was moved, and if so, where it was moved to, so that you could retrieve the project files.

12.1.5 Policy Management

The Policy Management page displays all policies, along with a summary of policy details. When you select a policy, applicable tools in the toolbar are activated. A summary of the toolbar follows.

NOTE: All of these tools are also accessible by right-clicking a selected policy.

Manage Policies: Lets you create any of the following policies:

- User Home Folder policy
- User Profile Path policy
- User Remote Desktop Services Home Folder policy
- User Remote Desktop Services Profile Path policy
- Group policy
- Container policy
- Auxiliary policy

Rename Policy: Lets you rename the selected policy.

Delete Policy: Lets you delete the selected policy.

Edit Policy: Brings up the Policy Editor, where you can edit the selected policy.

Import Policies: Provides the ability to import policies that were previously exported through the *Export Policies* menu option.

NOTE: Policy associations are not imported. After policies are imported, you need to associate the policies to containers or groups.

For more information on importing policies, see Section 5.13, "Importing Policies," on page 65.

Export Policies: Provides the ability to export policies so that they can be imported later. For example, many customers first evaluate Novell Storage Manager in a lab environment and create a large number of policies in the process. You can export these policies and later import them into the production environment. All exported policies are saved in a single XML file. For more information, see Section 5.12, "Exporting Policies," on page 64.

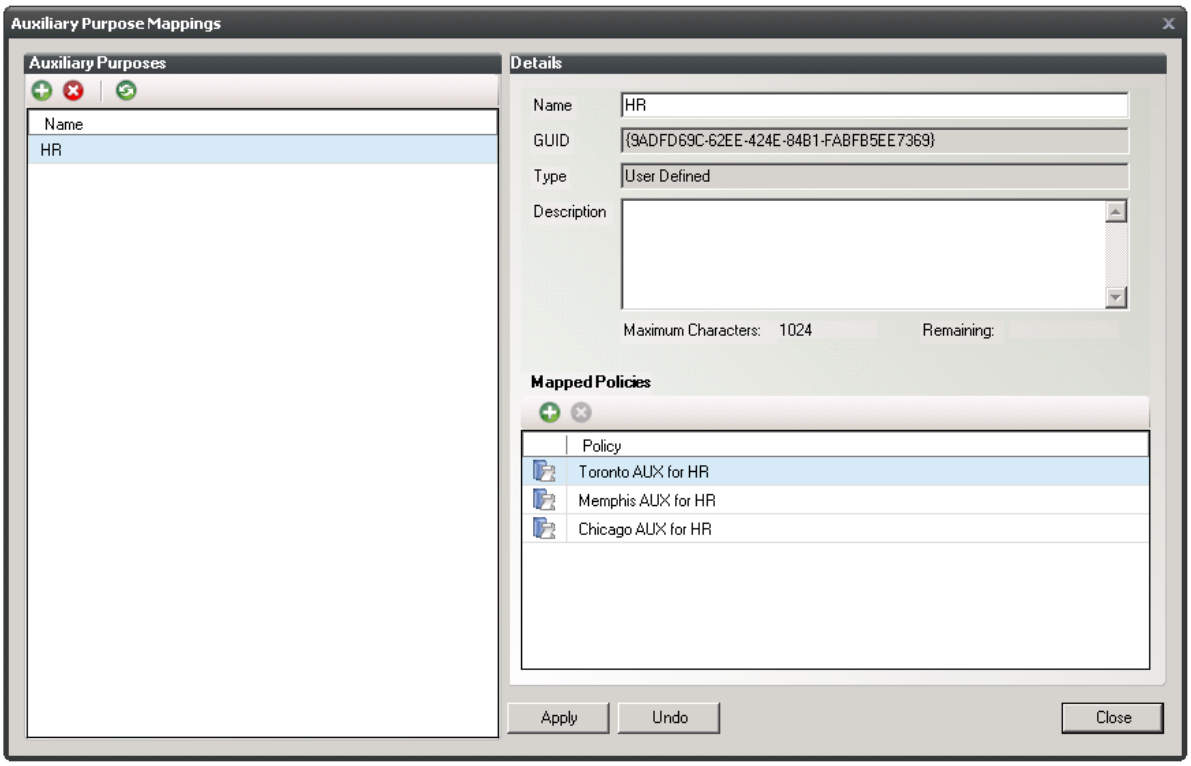
Import Upgraded Policies: Provides the ability to import policies migrated from a Novell Storage Manager 2.5*x* NSM Engine after the NSMAdmin Setup Wizard has been run. This feature is provided in case you chose not to import the policies when you ran the Setup Wizard.

Actions for Auxiliary Policies: Provides menu options that are applicable to Auxiliary policies. To activate this menu, click an Auxiliary policy. Menu options include *Manage*, *Groom*, *Apply Attributes*, *Apply Quota*, *Apply Rights*, and *Assign Auxiliary Attributes*.

Auxiliary Policy Mappings: Auxiliary policy mappings give you the ability to specify a purpose or classification for auxiliary storage policies. For example, you might want to create an HR purpose for all of the auxiliary storage policies that create HR folders for employees. With each of the auxiliary storage policies that create HR folder assigned the same purpose, it makes it possible for Novell Storage Manager to make intelligent decisions for auxiliary storage when a user is moved.

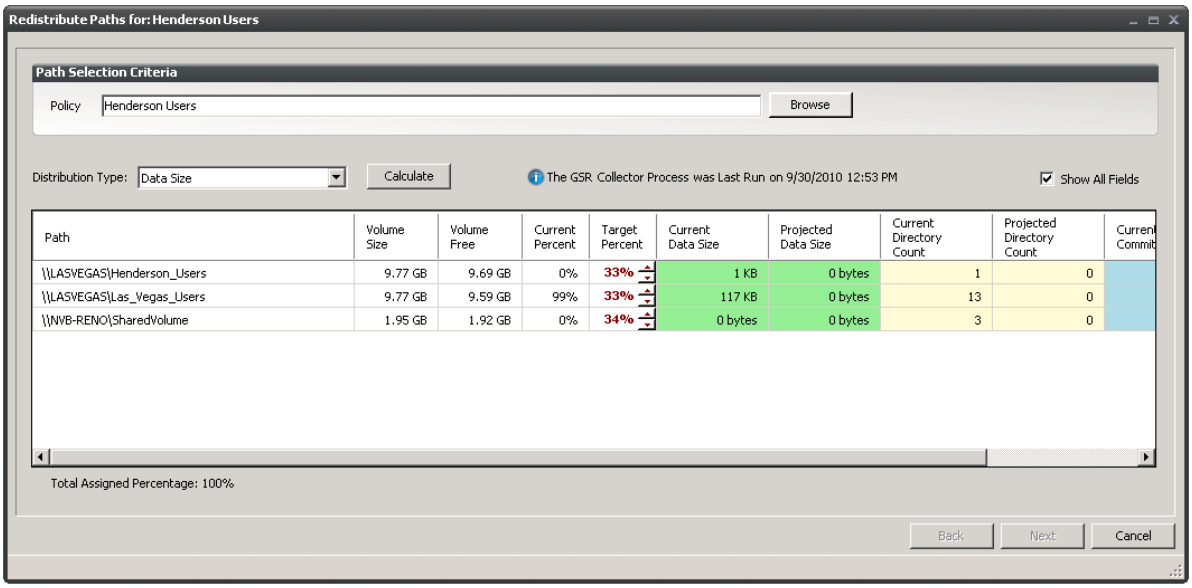
For example, if a user in the Detroit office transfers to the Dallas office, and the user has a home folder and an auxiliary storage folder in the Detroit office's HR department, you want to migrate both the home folder and the auxiliary storage folder to correct locations in Dallas. Having the Detroit auxiliary storage policy and the Dallas auxiliary storage policy identified with the same HR purpose, ensures that the user moved from Detroit to Dallas, will have his auxiliary storage properly established with the move.

Figure 12-6 *Auxiliary Purpose Mappings Dialog Box*



Redistribute Policy Paths: Allows you to define additional target paths in the policy and then redistribute or load-balance the data among the various paths.

Figure 12-7 *Redistribute Policy Paths Dialog Box*



Using the Redistribute Policy Paths dialog box, you can redistribute the user and collaborative storage across the target paths associated with a policy.

NOTE: The data displayed in the dialog box is taken from the most recent report from the GSR Collector.

Use the *Distribution Type* drop-down menu to view your data distribution according data size, directory count, and quota commitment.

Click *Next* to view the current locations of the home folders and collaborative storage folders, and the location where Novell Storage Manager proposes to redistribute the folders. If you want, you can deselect a folder for distribution by deselecting the check box corresponding to the folder. You can also indicate a new target path for the folder by clicking in the *Target Policy Path* column and selecting a new target path.

Clicking *Submit* begins the process of redistributing the folders.

Report on Policy Paths: If your network includes Novell File Reporter, this button is the means of Novell File Reporter reporting on Novell Storage Manager policy paths.

This capability is particularly powerful because it allows you to specify the target paths where user and collaborative storage resides on the network. Because network user and collaborative home folders tend to be the source of most of the stale, redundant, and non-work-related file types, the Policy Path Reporter can quickly and easily be the means of generating reports on the storage areas that you care about most. For procedures, refer to the *Novell File Reporter 1.0 Administration Guide*.

Refresh: Refreshes the list of policies.

NOTE: Refreshing locks the database during the refresh operation. For best performance, do not refresh more than is necessary.

Reload Policy Cache: Reloads your policies from the database. For example, you can use this tool if you have a policy that is not displayed in the list.

Check Boxes: NSMAdmin shows only the policy types that are checked.

Filter: Filters policy names as you type.

12.1.6 Pending Events

This page displays a list of pending events for the NSM Engine. All of the pending events are listed with details on the status of those events. Some events process very quickly and might actually be completed before they can be viewed in the list. Other events might remain in the queue for a long time, waiting for some condition to be met before they can be completed.

Clicking a listed event or events activates the toolbar. The toolbar has the following options:

Properties: Displays event properties such as FDN, ID, Action, and Current Status.

Make Eligible: If an event is deferred, you can click this option to make the event eligible immediately.

Defer: If an event is eligible, you can click this option to manually defer it to a specific date. The chosen deferral date is displayed in a *Notes* field. You can also enter any notes explaining the reason you are deferring the event. Text from the *Notes* field is also displayed in the *Deferred Notes* field of the Properties dialog box.

Bypass: Lets you bypass the status that is holding up the event.

Abort: Lets you terminate the selected event or events.

Refresh: Refreshes the event list.

Previous/Next: The arrows let you move forward or back in the event list according to the *Events Per Page* setting.

Events Per Page: Indicates the number of events you want displayed on each page.

- **Accepting:** A green check mark indicates that Novell Storage Manager is accepting events to process. You can stop accepting events to process by clicking this button. You are prompted to enter text in a field indicating your reason for stopping the acceptance of events. The text you enter is recorded on the Engine Status page.
- **Processing:** A green check mark indicates that Novell Storage Manager is processing events. You can stop processing events by clicking this button. You are prompted to enter text in a field indicating your reason for stopping the processing of events. The text you enter is recorded on the Engine Status page.

12.1.7 Path Analysis

The Path Analysis page shows a tree view of your Novell Storage Manager managed storage and provides various storage reports. These reports are a quick way to determine the trustees of a share or folder, the number of files and file types in a given folder, whether a quota is assigned to a folder and if so, how much, and the trustees of individual files.

NOTE: Whether managed by Novell Storage Manager or not, all of the storage visible in the left panel is eligible for path analysis.

Use the left pane to browse and select network shares and folders. Use the right pane to view the files within a selected folder.

Clicking a share or folder in the left pane activates the toolbar. Options are also available by right-clicking a share or folder. The toolbar has the following options:

Path Analysis: A drop-down menu with the following options:

- *Quota:* Indicates if a quota is set for a folder, the quota size, and the amount of free space remaining in the folder.
- *File Types:* Categorizes the content of the selected folder by displaying the various file types, the total number of each file type, and the total size of each file type. For example, to know if a user is storing non-work related files in his or her home folder and the total size of these files, you could use this feature to quickly determine this information.
- *Trustees:* Opens the View Trustees dialog box, which lists all users and objects that have any type of rights to the selected volume, folder, or file. The View Trustees dialog box also indicates the rights that each of these users and objects have as well as how these rights are obtained.

Path Management: A drop-down menu with the following options:

- *Create Folder:* Lets you create a new folder within a selected folder.
- *Rename Folder:* Lets you rename a selected folder.
- *Delete Folder:* Lets you delete a selected folder.

Rebuild: Rebuilds your volume list. You might need to do this to display the volume structure after it has been modified.

Refresh: Refreshes the view within the Path Analysis page.

12.1.8 Object Properties

You can display the object properties through the Storage Management page, and you can also display them through the Object Properties page.

Use the *Browse* button to select an object from the Object Browser to place the fully distinguished name of the object in the *FDN* field, then click *Submit*. The five tabs display the following information:

Properties: Displays Active Directory values and NSM Engine database values. If you are working with a Novell Support representative to resolve a problem, you might need to provide information from this page.

Effective Policies: Lists all of the effective policies for the selected object. An effective policy is a policy that affects a user either directly through association or inheritance by membership in a domain, container, or group.

Associated Policies: Lists all of the associated policies for an object. An associated policy is an explicitly assigned policy associated with a domain, container, group, or user.

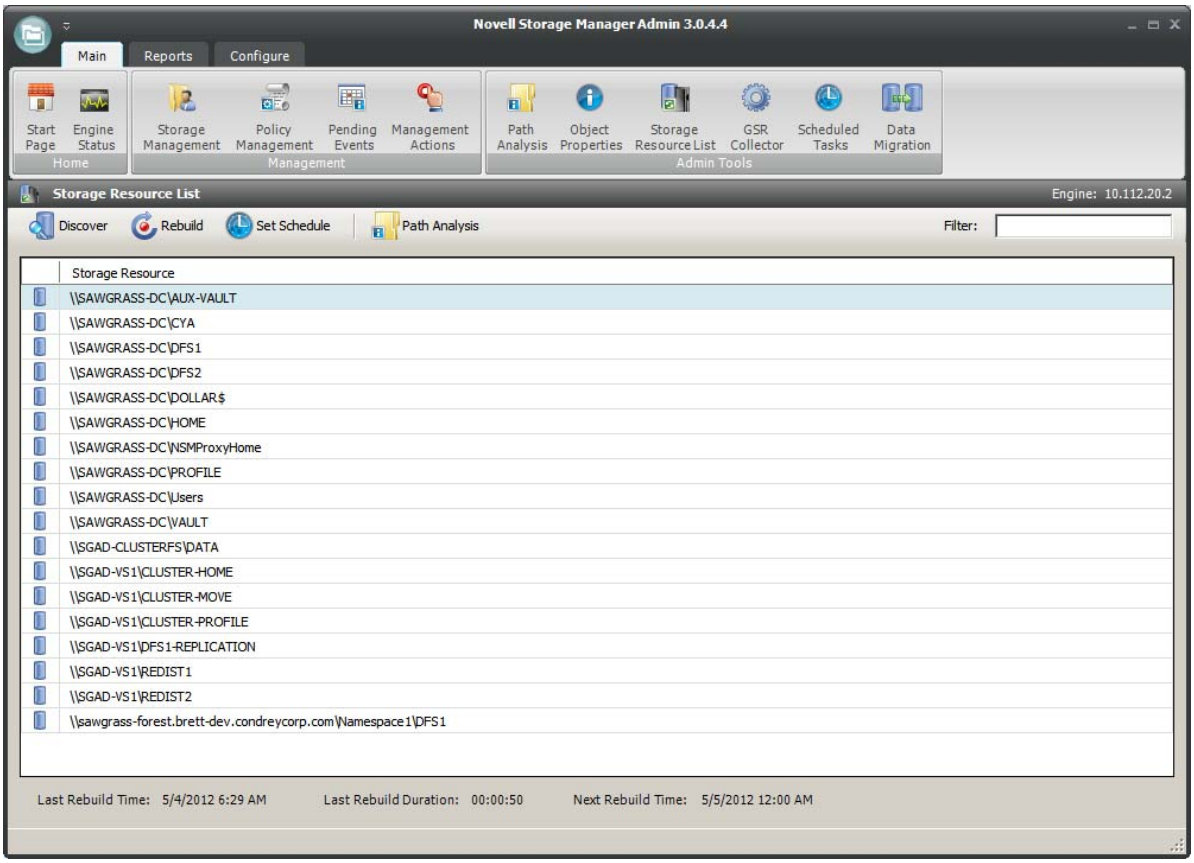
Transactions: Shows pending events for the selected object. If there are many pending events, but you only want to see those for a particular user, you can see the pending events for the User object.

History: Shows a history of the managed storage location that pertains to the selected User object. This information is only available after the GSR Collector has run.

12.1.9 Storage Resource List

This page lets you rebuild the storage resource cache used in Novell Storage Manager. Because Novell Storage Manager uses the storage resource cache to accelerate operations, there might be times when you need to use this page to populate the cache with new shares.

Figure 12-8 *Storage Resource List Page*



Last Rebuild Date: Displays the last date that the storage list was rebuilt.

Last Rebuild Duration: Displays the length of time it took to generate the new storage resource list.

Next Rebuild Scheduled For: Displays the date and time when Novell Storage Manager next rebuilds the storage list. Unless it is rebuilt through the *Rebuild Storage List*, the storage list is rebuilt automatically at midnight each day.

Discover: Clicking this button initiates a search within the entire forest domain for any new shares or DFS namespaces. Depending on the size, configuration, and topology of your network, this can take a significant amount of time.

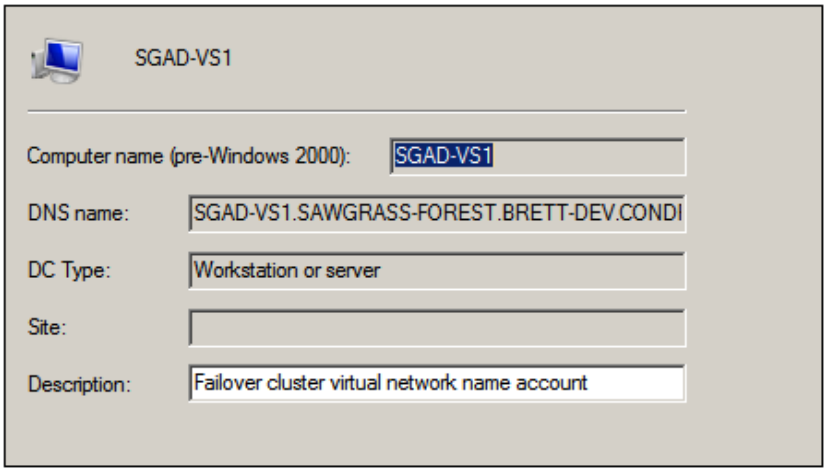
Rebuild: Clicking this button initiates a search within the entire forest domain for all available shares or DFS namespaces. When you create or edit a policy, you might need to rebuild the list if the share or DFS namespace you need does not appear in the storage resource list. Depending on the size, configuration, and topology of your network, this can take a significant amount of time.

Set Schedule: Allows you to set the schedule for rebuilding the storage resource cache.

Path Analysis: Provided to let you determine the trustees of a share or folder, the number of files and file types in a given folder, whether a quota is assigned to a folder and if so, how much, and the trustees of individual files. For more information, see Section 12.1.7, “Path Analysis,” on page 220.

Displaying Windows Server Clusters

If a Windows Cluster File Server Resource is not displayed in the Storage Resource List, verify that the *Description* field of the cluster file server resource includes the words `cluster` and `virtual`. If these two words are not included in the description, Novell Storage Manager cannot see it as a storage resource.



Once you modify the description in the *Description* field, you can click *Discover* to add the resource to the Storage Resource List.

12.1.10 GSR Collector

Formerly known as the "Janitor," the Global Statistics Reporting (GSR) Collector gathers and presents an extensive amount of statistical summaries pertaining to file system data. Running the GSR Collector, provides data for the various reports that you can generate in Novell Storage Manager.

The GSR Collector can be run manually or based on a schedule.

Additionally, the GSR Collector maintains a history of file movements in the Novell Storage Manager catalog. The GSR Collector updates the catalog with time-based data. This means that whenever an administrator moves data managed by Novell Storage Manager, it is recorded in the catalog. This can be especially useful when Novell Storage Manager has archived data. When data is archived, network administrators tend to move data from one storage area to another. With each move, Novell Storage Manager updates the movement in the catalog, so that the data can be easily located; for example, if an audit is necessary.

To view the cataloged data from the Storage Management page, display a User object in the right pane and then double-click it. In the Object Properties dialog box, click the *History* tab to view historical information of data movement pertaining to the User object.

The GSR Collector can be resource intensive. You should be careful when running the GSR Collector during peak traffic load on the NSM Engine.

12.1.11 Scheduled Tasks

You can use Scheduled Tasks to view, edit, and run tasks that are currently scheduled. Scheduled tasks include storage resource discovery, file grooming, and running the GSR Collector. To edit a scheduled task, select the task listing, click *Edit Scheduled Task*, and then select *Edit Schedule* to access the schedule dialog box. You can also access the same dialog box through the GSR Collector page, the Storage Resource List page, and on the Add Scheduled Tasks page to schedule grooming.

12.1.12 Data Migration

Cross-Empire Data Migration is a subsystem within Novell Storage Manager that allows for the movement of file system data between storage infrastructures on different platforms governed by different identity and security frameworks. The Cross-Empire Data Migration architecture is engineered to eventually support multiple types of source platforms and targets, but the current release is limited to a Novell eDirectory source environment and a Microsoft Active Directory target environment.

Clicking Data Migration launches the Data Migration Wizard, which enables the automated movement of data quickly and easily. You have a number of migration options, including moving data for multiple users and or groups directly to its intended location across multiple servers or shares in a single operation, all while preserving critical file system metadata.

For more information, see Chapter 11, “Performing a Cross-Empire Data Migration,” on page 111.

12.2 Reports Tab

The *Reports* tab provides access to existing Consistency and Management Action reports for events and network storage. It also provides access to a Runtime Config report that reports on your Novell Storage Manager configuration, environment, and pending events.

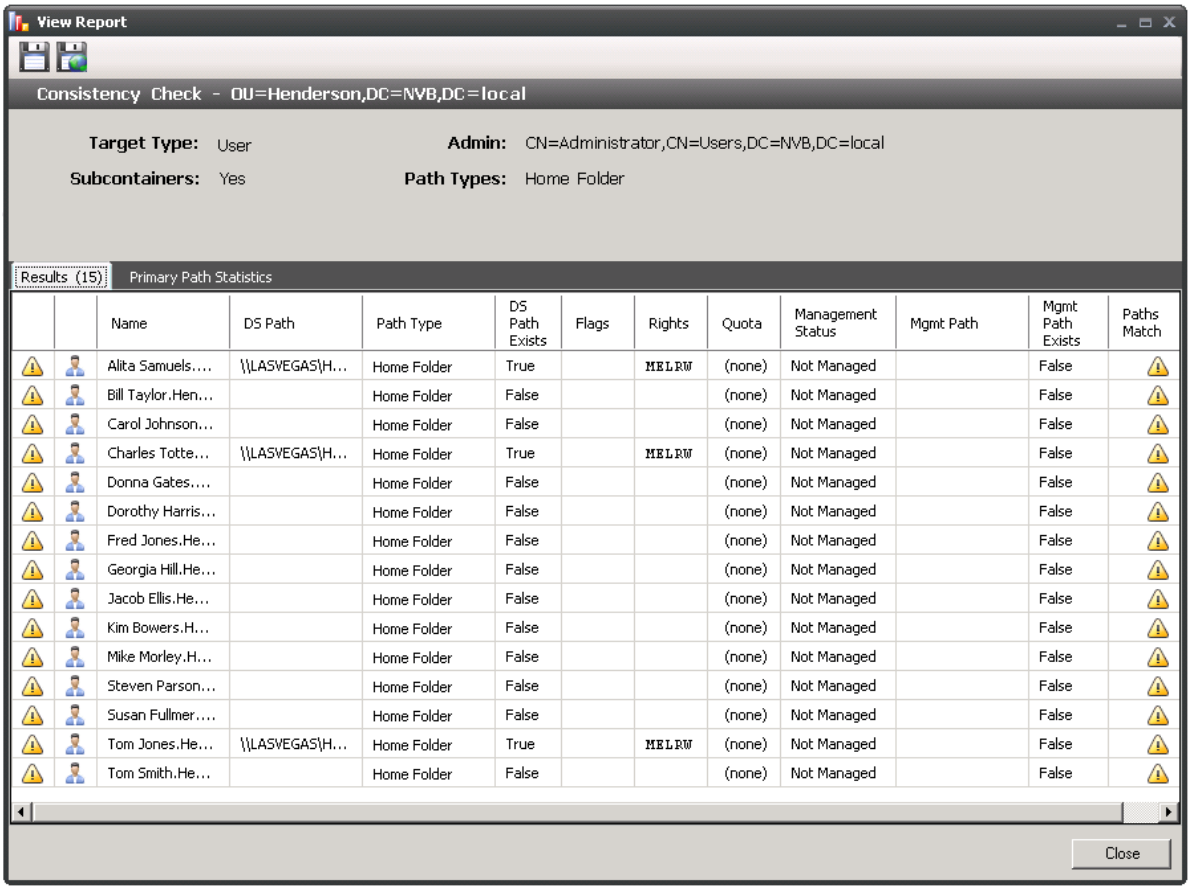
- Section 12.2.1, “Consistency Check Reports,” on page 224
- Section 12.2.2, “Action Reports,” on page 226
- Section 12.2.3, “Anomaly Reports,” on page 227
- Section 12.2.4, “Runtime Config,” on page 228
- Section 12.2.5, “Storage Resource Statistics,” on page 228
- Section 12.2.6, “Global Statistics,” on page 229

12.2.1 Consistency Check Reports

This page is used to access and export stored Consistency Check reports.

To access a report, double-click a report listing to access the View Report dialog box.

Figure 12-9 *Consistency Check Report*

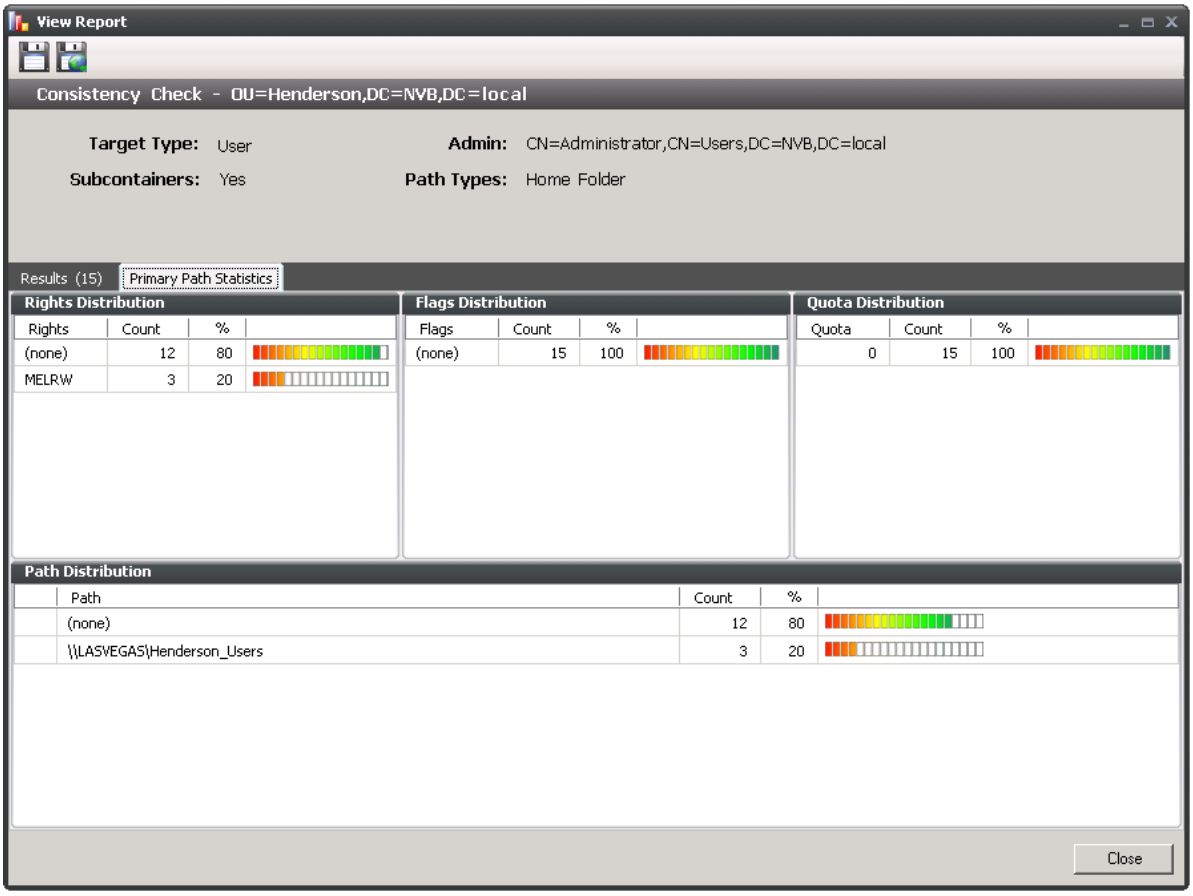


Name	DS Path	Path Type	DS Path Exists	Flags	Rights	Quota	Management Status	Mgmt Path	Mgmt Path Exists	Paths Match
Alita Samuels....	\\LASVEGAS\H...	Home Folder	True		MELRW	(none)	Not Managed		False	
Bill Taylor.Hen...		Home Folder	False			(none)	Not Managed		False	
Carol Johnson...		Home Folder	False			(none)	Not Managed		False	
Charles Totte...	\\LASVEGAS\H...	Home Folder	True		MELRW	(none)	Not Managed		False	
Donna Gates....		Home Folder	False			(none)	Not Managed		False	
Dorothy Harris...		Home Folder	False			(none)	Not Managed		False	
Fred Jones.He...		Home Folder	False			(none)	Not Managed		False	
Georgia Hill.He...		Home Folder	False			(none)	Not Managed		False	
Jacob Ellis.He...		Home Folder	False			(none)	Not Managed		False	
Kim Bowers.H...		Home Folder	False			(none)	Not Managed		False	
Mike Morley.H...		Home Folder	False			(none)	Not Managed		False	
Steven Parson...		Home Folder	False			(none)	Not Managed		False	
Susan Fullmer....		Home Folder	False			(none)	Not Managed		False	
Tom Jones.He...	\\LASVEGAS\H...	Home Folder	True		MELRW	(none)	Not Managed		False	
Tom Smith.He...		Home Folder	False			(none)	Not Managed		False	

The dialog box displays the contents of the Consistency Check report.

The *Primary Path Statistics* tab shows the rights, flag, and path distribution data in text and graphical format.

Figure 12-10 *Primary Statistics in a Consistency Check Report*



To export a Consistency Check report, double-click a report listing to access the View Report dialog box, and then in the upper-left corner of the dialog box, click either the Save CSV Report or Save HTML Report icons.

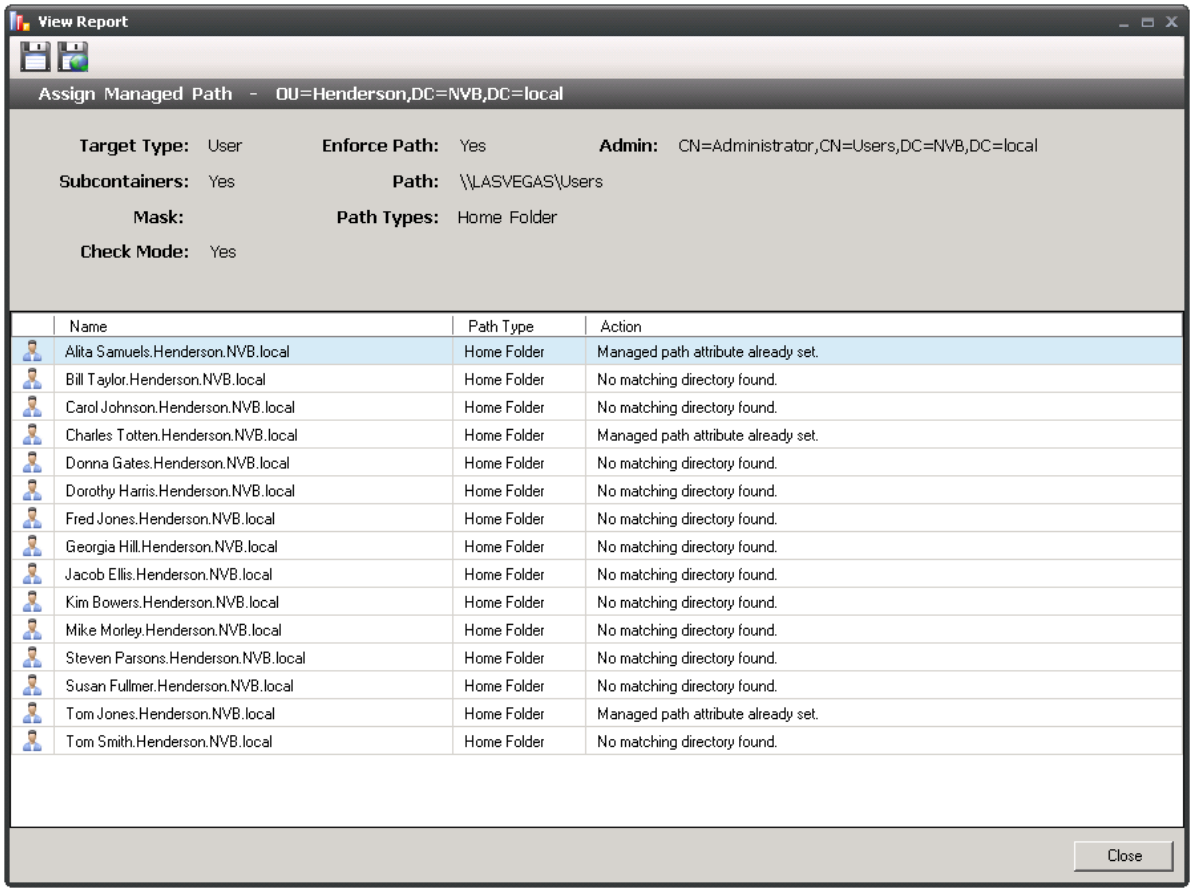
For more information on Consistency Check Reports, see Section 4.3, “Running Consistency Check Reports on Existing Storage,” on page 25 and Section 4.10, “Performing a Consistency Check,” on page 35.

12.2.2 Action Reports

Action reports are stored each time a Management Action is performed. Use this page to view or export to a report, the results of any Management Action performed. A list of available Management Action reports is presented, identifying the report by the Active Directory object it was run on, and the time the report was generated.

Double-clicking any item in the list brings up the individual Management Action report.

Figure 12-11 *Action Report*



To export an Action report, double-click a report listing to access the View Report dialog box, and then in the upper-left corner of the dialog box, click either the Save CSV Report or Save HTML Report icons.

12.2.3 Anomaly Reports

Anomaly reports indicate anomalies that can occur over time as a result of manual storage management practices. See Chapter 4, “Managing Existing User Storage,” on page 23, for information on Management Actions that are based on the anomalies in the Anomaly reports.

Anomaly reports are generated after the first time you run the GSR Collector. Any anomalies the GSR Collector finds are listed in one of the following category reports:

Table 12-1 *Categories for Anomaly Reports*

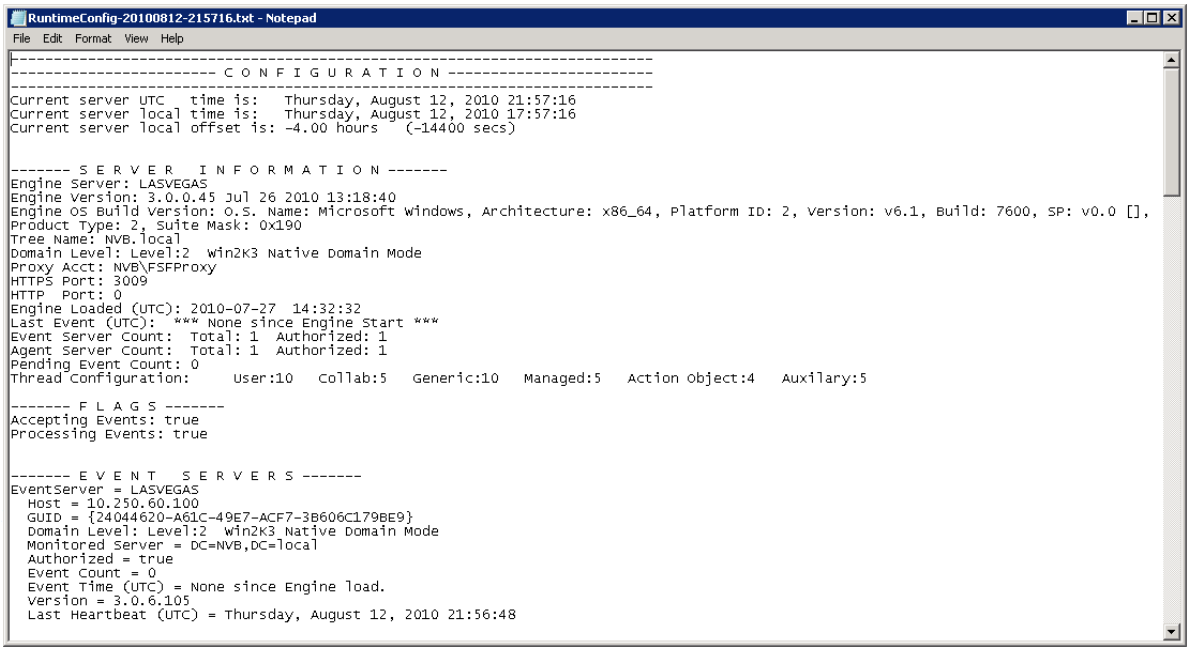
Tab Name	Explanation
Orphan Candidates	Lists home folders that are not currently assigned to a User object in Active Directory.
Name Mismatch	Lists cases where a username and the associated home folder name do not match. This is frequently the case when a User object is renamed, but the corresponding home folder is not.

Tab Name	Explanation
Path Overlap	Lists home folders that are parent paths of other user home folders. For example, a user's home folder attribute in Active Directory is set to \\SERVER\SHARE\HOME\USERS instead of \\SERVER\SHARE\HOME\USERS\JBANKS. This is a potential conflict because if you move an object that resides in the first path, it moves all users below the user.
Duplicate Storage Pointer	Lists users that have identical home folder paths.
Missing Primary Folders	Lists users who do not have assigned home folders.
Missing Auxiliary Folders	Lists users that have auxiliary storage assigned, but the storage is not yet created.
Objects Not Managed	Lists users in Active Directory whose storage is presently not managed through Novell Storage Manager.

12.2.4 Runtime Config

Runtime Config reports are used to build reports on the current configuration and pending events from the NSM Engine. In earlier versions of Novell Storage Manager, these reports were known as DumpConfig reports and they could be quite large because they reported on the entire configuration and status of the NSM Engine. For this reason, you can indicate which configuration data you want included in the report by selecting the desired check boxes.

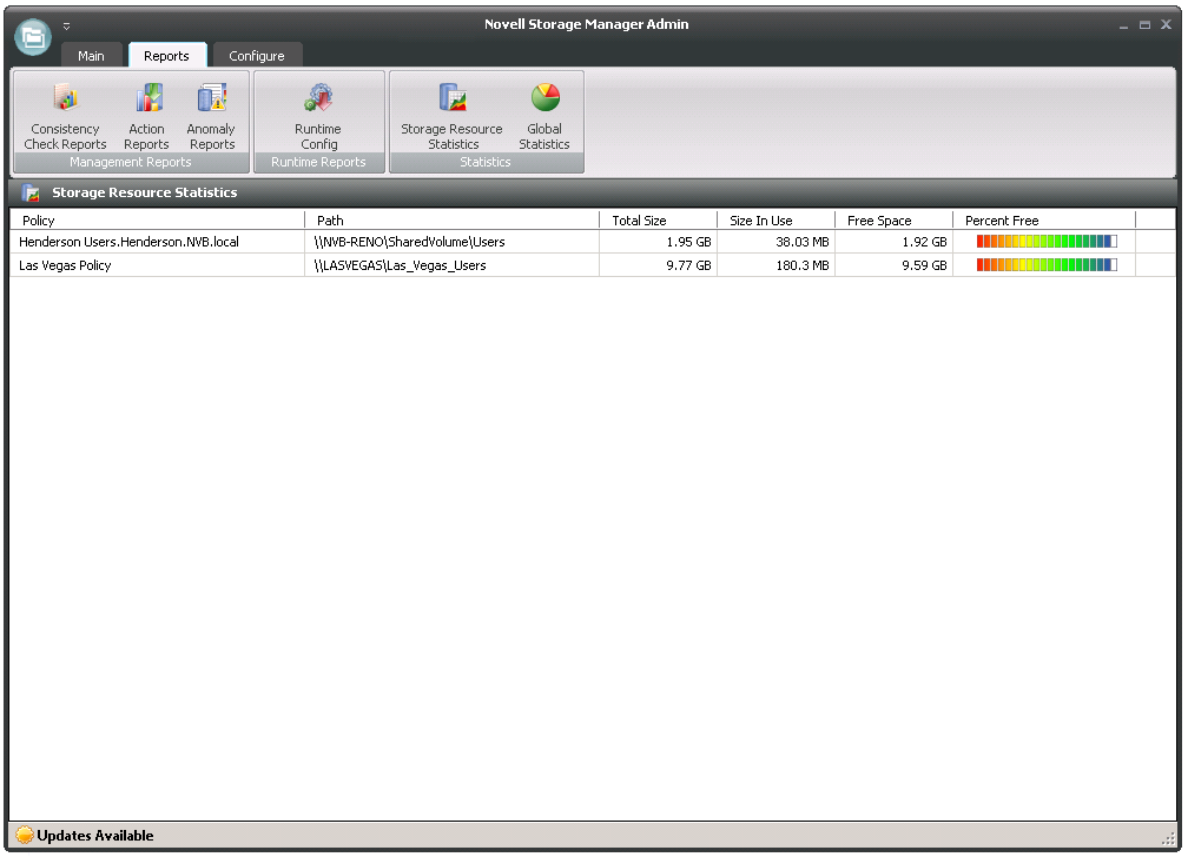
Figure 12-12 *Sample Runtime Config Report*



12.2.5 Storage Resource Statistics

This page shows high-level statistical information pertaining to your policies, their corresponding target paths, and size and free space information.

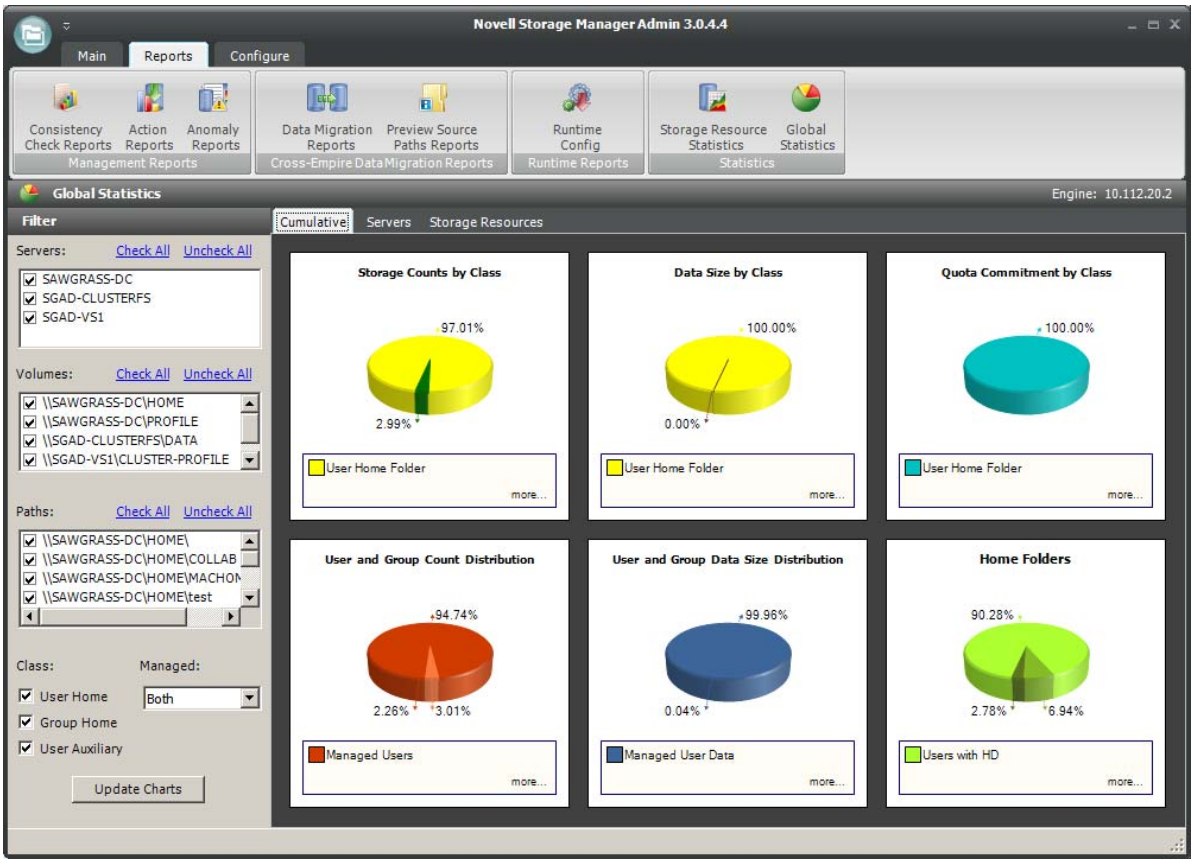
Figure 12-13 *Storage Resource Statistics Report*



12.2.6 Global Statistics

Global Statistics provides a graphic view of the current state of your storage. The reports can be configured to show different servers, shares and paths. The class (user, collaborative, or auxiliary storage) can also be selected.

Figure 12-14 *Global Statistics Report*



Expanding or stretching NSMAdmin increases the size of the charts and the legend under each chart.

12.3 Configure Tab

The *Configure* tab includes all of the operations to set up and configure Novell Storage Manager, as well as integrate Novell File Reporter.

- Section 12.3.1, “Engine Config,” on page 230
- Section 12.3.2, “Event Servers,” on page 234
- Section 12.3.3, “Agent Servers,” on page 234
- Section 12.3.4, “File Reporter,” on page 237
- Section 12.3.5, “Client Config,” on page 237
- Section 12.3.6, “Check Updates,” on page 239

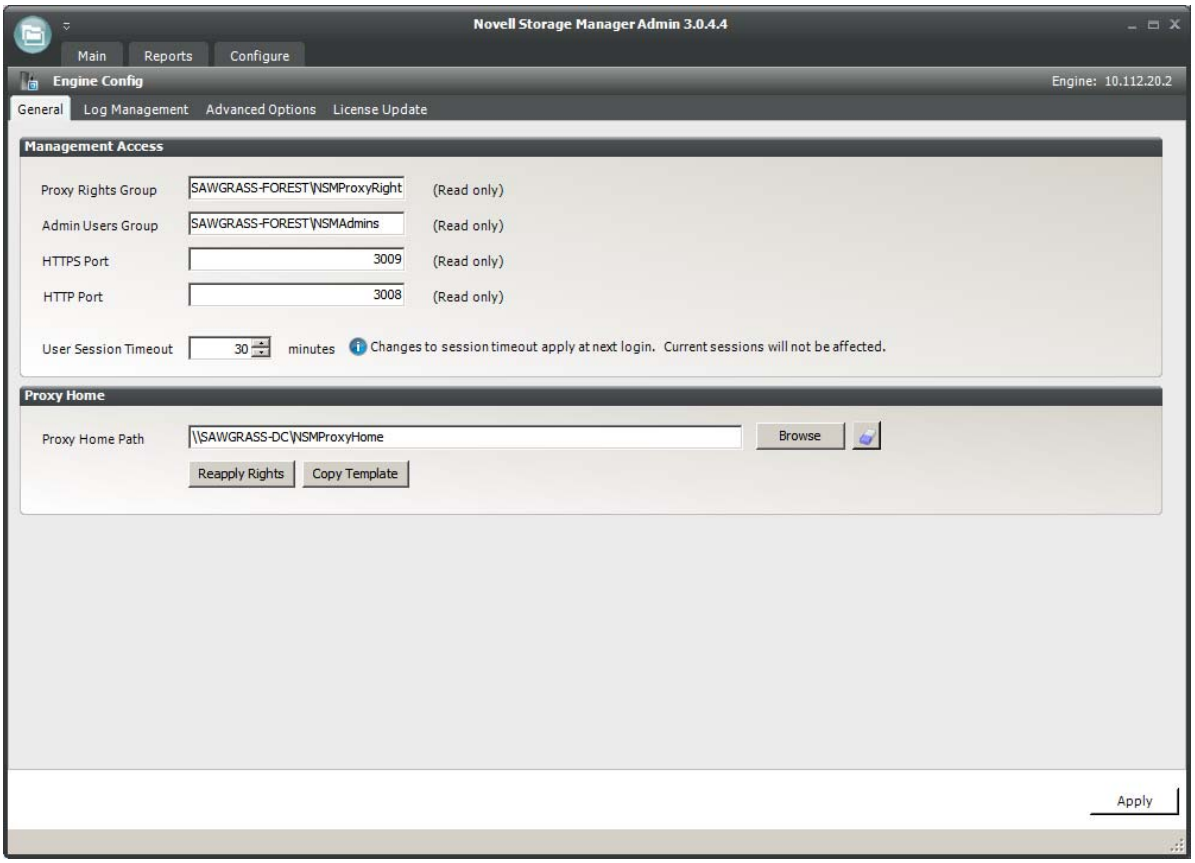
12.3.1 Engine Config

- “Replacing an Unexpired License File” on page 233
- “Replacing an Expired License File” on page 234

This page lets you view and set NSM Engine configuration settings.

The *General* tab includes proxy and management access settings. Each of the fields is described below.

Figure 12-15 *Engine Config General Tab Settings*



Proxy Rights Group: Displays the Proxy Rights Group that you established when you installed Novell Storage Manager.

Admin Users Group: Displays the Admin Users Group that you established during the installation of Novell Storage Manager.

Client Session Timeout: Indicates the number of minutes NSMAdmin can be left dormant before you need to reauthenticate.

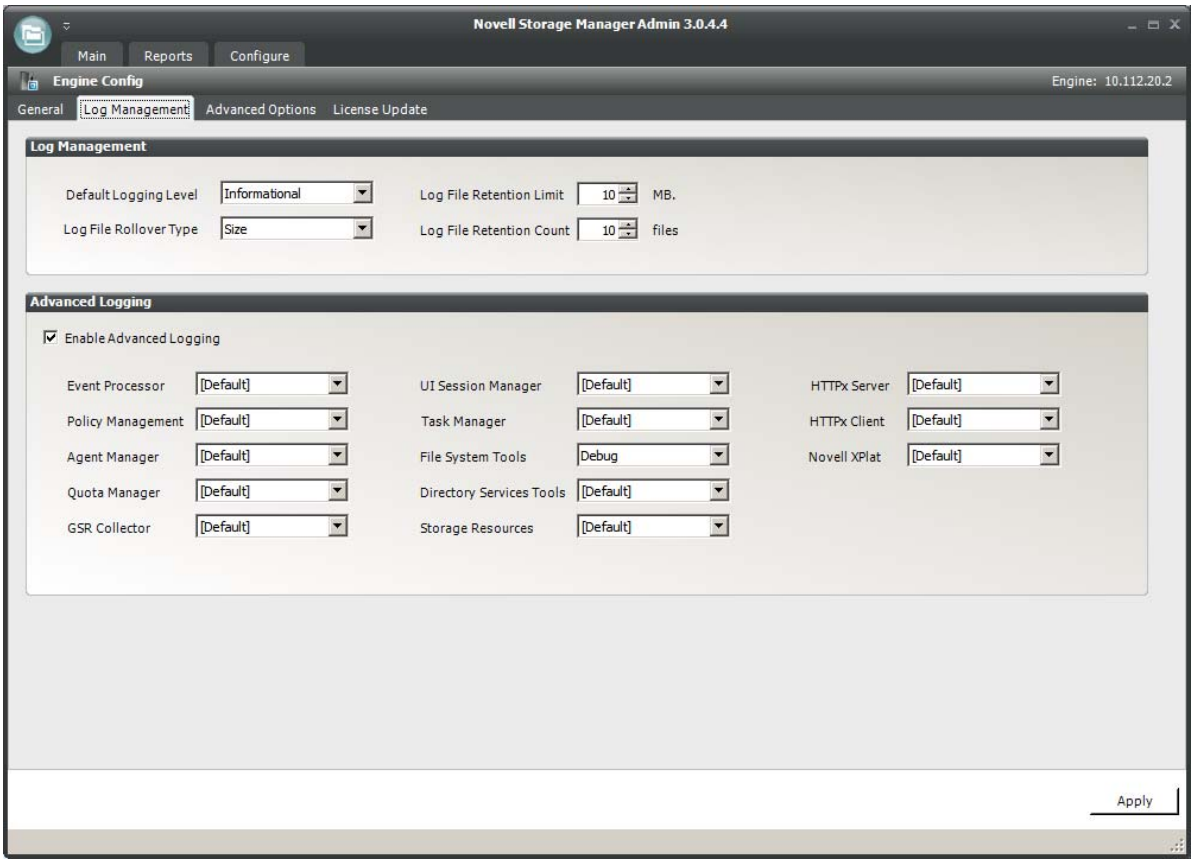
HTTPS Port: Displays the HTTPS port that you chose when you installed Novell Storage Manager.

HTTP Port: If you chose to use an HTTP port during the installation of Novell Storage Manager, the HTTP port is displayed here.

Proxy Home Path: This path was established during the installation of NSMAdmin. If you need to, you can change the path by using the *Browse* button.

The *Log Management* tab includes settings specific to log files, which are accessible only from the server hosting the NSM Engine. Each of the fields is described below.

Figure 12-16 *Engine Config Log Management Tab Settings.*



Global Logging Level: By default, the log records warning level details. You can change the log to record the level you want. Be aware that some settings, such as debug or verbose, record much more information and can potentially make the log file much larger.

Log File Retention Count: By default, Novell Storage Manager retains the 10 most recent log files, according to the Log File Rollover Type setting. For example, if the *Log File Rollover Type* setting is set to *Daily*, the retained log files are from the last 10 days.

Log File Rollover Type: You can choose whether to have log files roll over daily, hourly, when the log has reached a set size limit, or have no rollover setting. If you select *None*, the same log file is opened each time you start the NSM Engine, and log entries are appended to it.

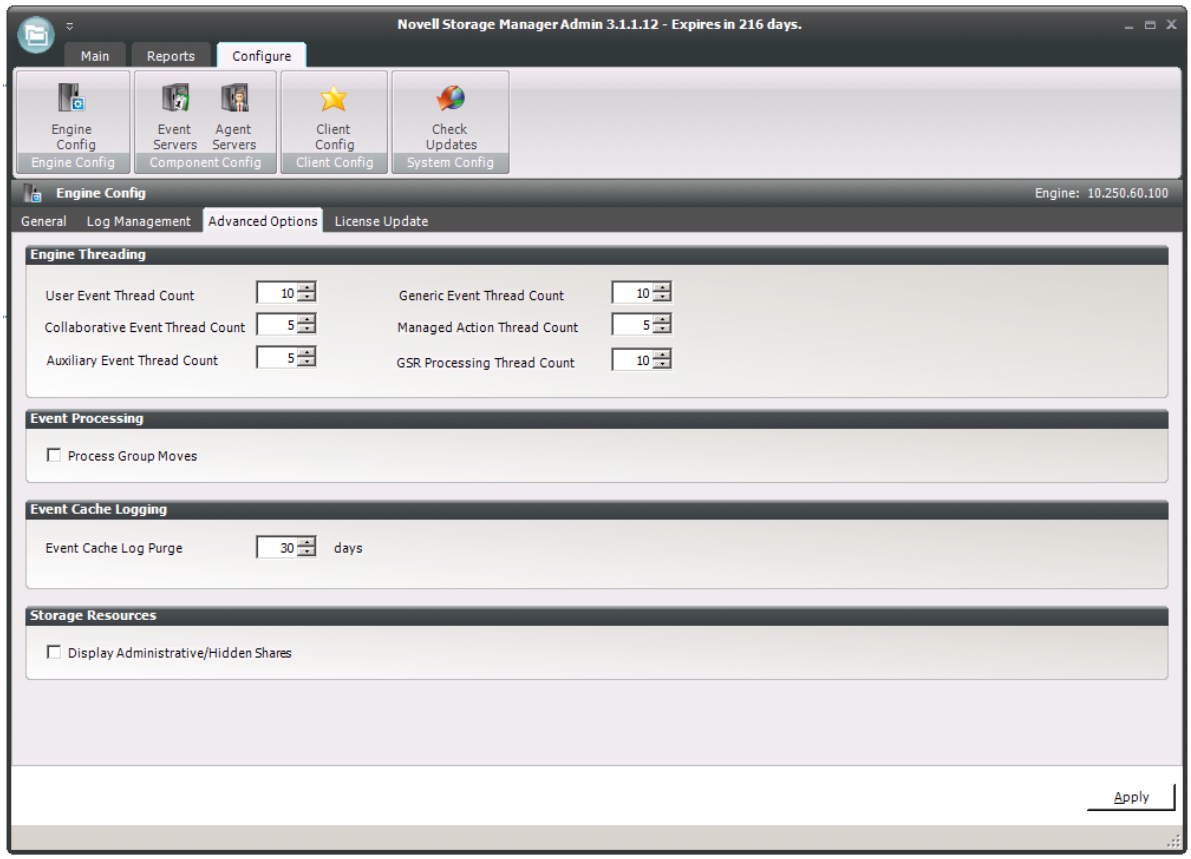
NOTE: If you delete the log file while the NSM Engine is not running, a new log file is created the next time you start the NSM Engine.

Log File Retention Limit: This field appears only when you select *Size* from the *Log File Rollover Type* field. You need to enter the size limit in MB for the log file before it creates a new file.

Enable Advanced Logging: Selecting this check box activates the Advanced Logging region of the page. This region allows you to specify the output of the log file according to the setting you indicate in each of 12 categories.

The *Advanced Options* tab lets you view or reconfigure the thread count settings allocated for the actions that Novell Storage Manager performs.

Figure 12-17 *Engine Config Configure Tab*



These settings are optimized for a normal Novell Storage Manager workload. However, if you are starting a project where you need to add up to 1,000 users, you might want to increase the *User Thread Count* setting.

Event Cache Log Purge: By default, Novell Storage Manager keeps the most recent 30 days of event entries in cache. You can adjust the setting in the *Days* field.

The event cache can be helpful in providing you a recent history of all of the events that were sent from the Event Monitor.

Display Administrative/Hidden Shares: Selecting this check box displays in NSMAdmin, all administrative and hidden shares.

The *License Update* tab lets you replace an unexpired license file.

Replacing an Unexpired License File

1. Click *Browse* to locate and select the new license file.
2. Click *Upload*.

Replacing an Expired License File

You cannot replace an expired license using NSMAdmin. To replace an expired license file:

1. At the server that is hosting the NSM Engine, go to `C:\ProgramData\Novell Storage Manager\Engine\config`.
2. Replace the old `nsm.lic` file with the new one.

12.3.2 Event Servers

The Event Monitor monitors changes to Active Directory based on create, move, rename, and delete events. The host for the Event Monitor is referred to as the Event Server.

You install one Event Monitor per domain, and it can run on a domain controller or a member server. If you install the Event Monitor on a domain controller, the Event Monitor always monitors the local server for changes in the domain. If you install the Event Monitor on a member server, the Event Monitor identifies the closest available domain controller and monitors it for changes in the domain. The Event Monitor runs as a native service on Windows.

The Event Server page lets you:

- Authorize an Event Monitor
- Verify that an Event Monitor is authorized
- View the Event Monitor software version installed
- View Event Monitor statistics
- Remove an Event Monitor

The *Event Count* number indicates the total number of events sent from the Event Monitor to the NSM Engine.

Procedures for authorizing the Event Monitor are located in "Authorizing the Event Monitor"in the *Novell Storage Manager for Active Directory Installation Guide*.

Deleting an Event Monitor

With the release of Novell Storage Manager 3.1.1, functionality has been added within NSMAdmin and the NSM Engine to delete a deauthorized Event Monitor. Only deauthorized Event Monitors can be deleted. If you want to remove an Event Monitor, you must deauthorize it first.

12.3.3 Agent Servers

NSM Agents perform copying, moving, grooming, and vaulting through directives from the NSM Engine. Novell Storage Manager determines which agent to use based on the target destination of the data.

For optimum performance, NSM Agents should be installed on all servers with storage managed by Novell Storage Manager. NSM Agents run as a native service on Windows.

The Agent Server page lets you:

- Authorize an NSM Agent
- Verify that NSM Agents are authorized
- View NSM Agents software versions installed

- View NSM Agent statistics
- Remove an NSM Agent
- Configure a proxy agent

The Agent Server page also indicates:

- Whether the NSM Agent is capable of being utilized in a Cross-Empire Data Migration
- Whether the NSM Agent is functioning as a proxy agent and for which device

Procedures for authorizing an NSM Agent are located in "Authorizing the NSM Agents" of the *Novell Storage Manager for Active Directory Installation Guide*.

Deleting an Agent

With the release of Novell Storage Manager 3.1.1, functionality has been added to NSMAdmin and the NSM Engine to delete a deauthorized NSM Agent. Only deauthorized NSM Agents can be deleted. If you want to remove an NSM Agent, you must deauthorize it first.

NOTE: If an NSM Agent is deauthorized and it hasn't successfully sent a heartbeat within 7 days, it will automatically be removed.

Proxy Agents

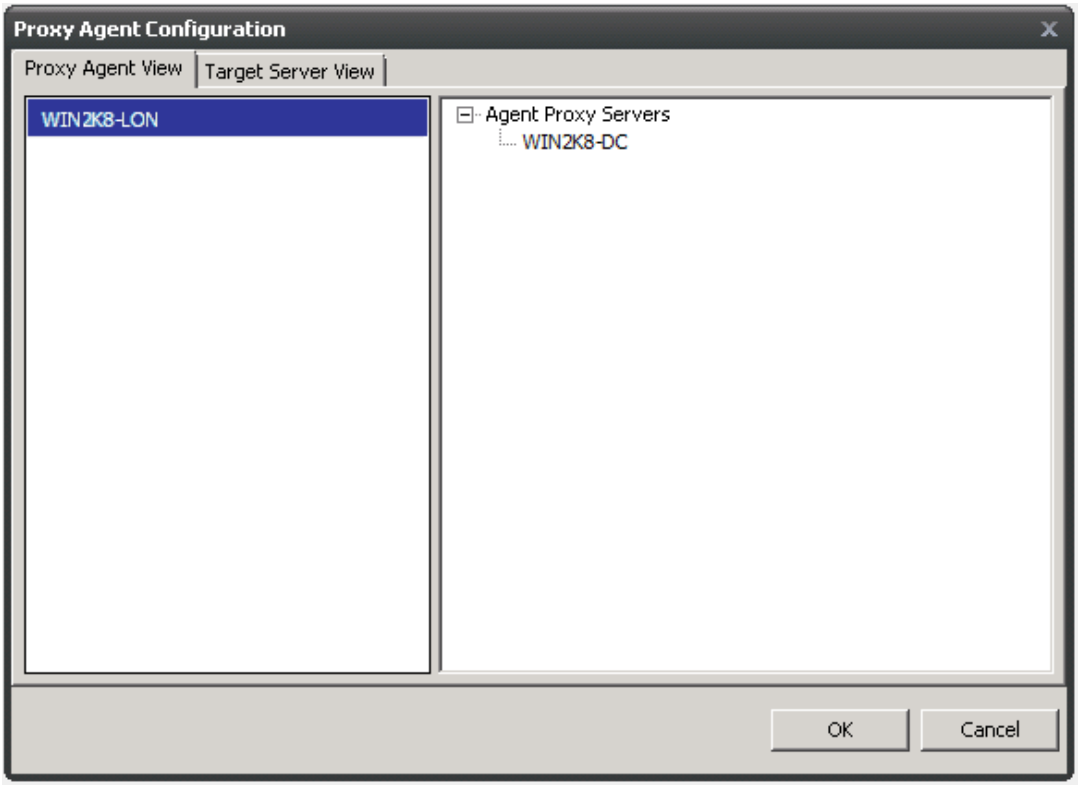
For storage resources that do not or cannot host an NSM Agent, for example a NAS (Network Attached Storage) device, Novell Storage Manager can utilize an NSM Agent running on another server to perform the copying, moving, grooming, and vaulting on the server or NAS device. In this type of scenario, the NSM Agent is serving as a "proxy agent."

A proxy agent can also be set up to reduce the workload on the NSM Engine. For example, a proxy agent can be configured for a server on one side of a WAN environment to move data from one server to another on the same side of the WAN link. This keeps the data from crossing the WAN link only to cross back again.

Configuring an NSM Agent to be a Proxy Agent

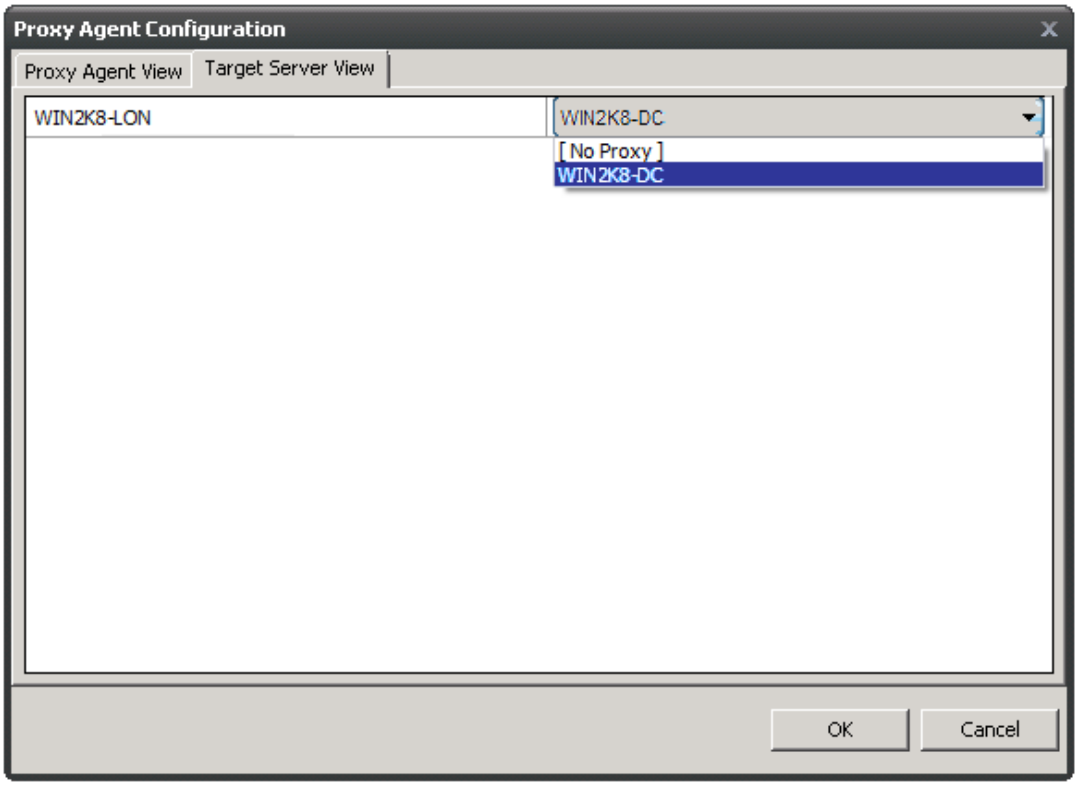
1. Launch NSMAdmin.
2. Click the *Configure* tab.
3. Right-click the NSM Agent you want to authorize to be a proxy agent and select *Configure Proxy*.

   The left side of the Proxy Agent Configuration dialog box shows the list of servers without NSM Agents installed. The right side shows the servers with NSM Agents installed. In the example below, the NSM Agent on the WIN2K8-DC could be set up to be the proxy agent for the WIN2K8-LON server.



4 Click the *Target Server View* tab.

5 From the drop-down list, select the NSM Agent server you want to serve as the proxy agent for the server on the left.



6 Click *OK* to save and close the proxy setting association.

12.3.4 File Reporter

Novell File Reporter helps organizations more effectively manage network storage by providing administrators the ability to access a comprehensive set of information about their network storage so that they can determine the best means of addressing their storage content. The separately sold product is built upon the premise that when organizations know what files are being stored, where they are stored, when they were last accessed, how many versions of a file exist, etc., they are better informed to make decisions about where to store files, what files can be deleted, how to tier their storage, how to plan for storage growth, and more.

NOTE: Novell File Reporter, Novell Storage Manager, and Novell Dynamic File Services are sold together in the Novell File Management Suite.

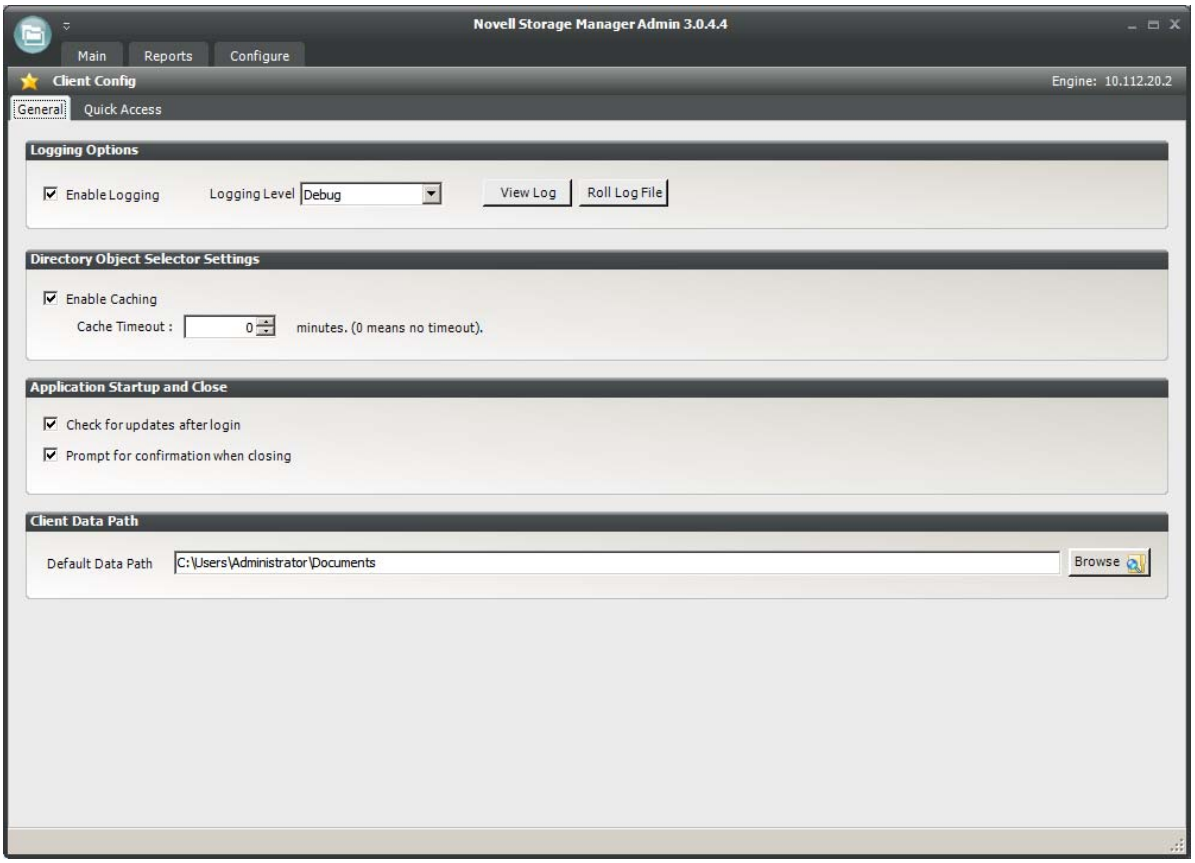
The *File Reporter* button is included in NSMAdmin because it is through NSMAdmin that Novell File Reporter reports on Novell Storage Manager policies. In order to do so, you must configure Novell Storage Manager to work with Novell File Reporter. For procedures on configuring Novell Storage Manager to work with Novell File Reporter, see "Configuring Novell Storage Manager to work with Novell File Reporter (http://www.novell.com/documentation/filereporter10/file_reporter_install/?page=/documentation/filereporter10/file_reporter_install/data/a20gkue.html)" in the *Novell File Reporter Installation Guide*.

12.3.5 Client Config

This page lets you configure various settings within NSMAdmin.

An overview of settings specific to the *General* tab follows the graphic.

Figure 12-18 *Client Config General Tab*



Enable Logging: Selecting this check box enables logging the operations of NSMAdmin and lets you specify the logging level and whether to roll the log or close the old log and start a new log.

Logging Level: This drop-down menu lets you select the classification of entry you want logged.

View Log: Clicking this button opens the log file.

Roll Log File: Clicking this button discontinues entries in the current log file and begins a new log file.

Enable Caching: When you are working in the Storage Management page, selecting this check box enables NSMAdmin to maintain the area of the directory tree that is visible in the right pane, if you move from the page to another. For example, if you locate a Group object in a container and then need to move to another page, when you return to the Storage Management page, you do not need to navigate the directory tree to locate the Group object again.

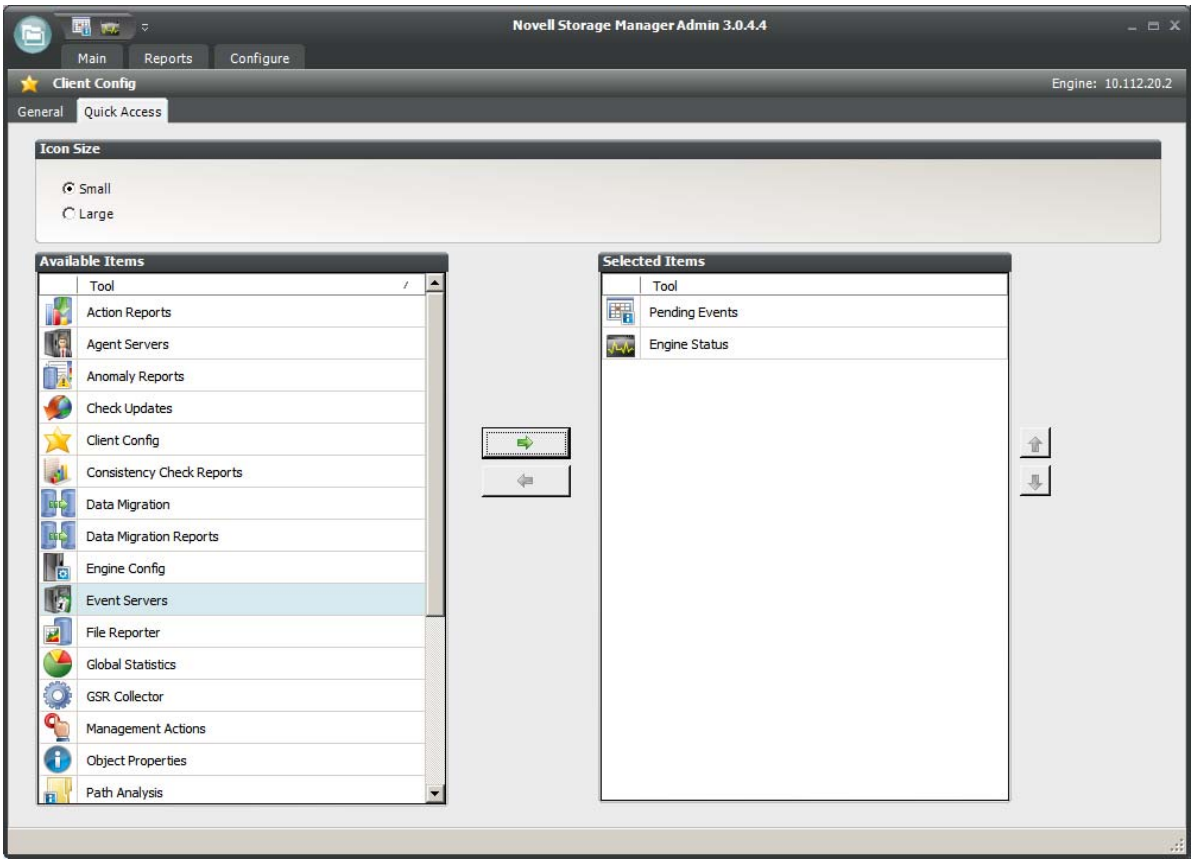
Check for Updates after Login: Selecting this check box allows NSMAdmin to notify you of the availability of newer Novell Storage Manager components.

Check for Confirmation When Closing: Selecting this check box prompts you with a confirmation of your choice when you close NSMAdmin.

An overview of settings specific to the *Quick Access* tab follows:

This page lets you access the items you use most in NSMAdmin from the Quick Access Toolbar. Items can be added or removed from the Quick Access Toolbar by right-clicking the item from its location in the interface, or through the Quick Access page shown below.

Figure 12-19 *Client Config Quick Access Tab*



By default, the Quick Access Toolbar is located in the title bar of NSMAdmin, but the location can be changed by using the menu at the end of the Quick Access Toolbar.

A discussion of the settings in the *Advanced* tab follows.

Settings on this page should be changed only under the supervision of Novell Support.

NOTE: Current values on this page are only active during the current session of NSMAdmin and are reset when NSMAdmin is closed or times out.

Bucket Load Parameters

These parameters are for adjusting the settings for the NSM Engine and NSMAdmin during enumeration operations.

12.3.6 Check Updates

This page compares the version numbers of Novell Storage Manager components that you have installed with the latest versions available. It also provides links for downloading the latest versions of each of the components.

A Security Specifications

This section provides details on configuring your Windows firewall to accommodate the components of Novell Storage Manager 3.1.1 for Active Directory. It also specifies the Local Security Authority (LSA) rights and privileges that must be set.

- Section A.1, “Windows Firewall Requirements,” on page 241
- Section A.2, “LSA Rights and Privileges,” on page 242
- Section A.3, “ProxyRights Group,” on page 243
- Section A.4, “Windows Clustering via Proxy Agents,” on page 244
- Section A.5, “NAS Devices,” on page 244

A.1 Windows Firewall Requirements

The Windows Firewall has different default configurations on Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2. Unless you have disabled the Windows Firewall, you must set the following exceptions:

- The NSM Engine must be permitted to make outbound connections.
- The NSM Engine must be able to listen on ports 3008 and 3009. These are the default port choices that are presented during the installation and configuration. If you use different values, you must adjust the firewall port exceptions to match the port values.
- The NSM Agent must be permitted to make outbound connections.
- The NSM Agent must be able to listen on ports 3010 and 3011. These are the default port choices that are presented during the installation and configuration. If you use different values, you must adjust the firewall port exceptions to match the port values.
- The Event Monitor component must be permitted to make outbound connections.
- On each server running Windows Server 2008 or later and hosting user or collaborative storage with managed quota, you must enable the `Remote File Server Resource Manager Management - FSRM Service (RPC-In) firewall rule.`

On servers running Windows Server 2008, the firewall settings are applicable to each of three different categories of network interfaces that are identified based upon their IP address range (public IP addresses versus private IP addresses) and whether or not the computer is a member of a domain. Depending upon the specific environment where Novell Storage Manager 3.1.1 for Active Directory is installed, the firewall might need to have these exceptions enabled in one or more of the following categories:

- Domain
- Private
- Public

A.2 LSA Rights and Privileges

The following table identifies the security principals, sets of rights and privileges and the computers on which the rights and privileges must be granted for Novell Storage Manager 3.1.1 for Active Directory to function properly.

Right/Privilege	Applies to	Security Principle
"Access this computer from the network" [SeNetworkLogonRight]	All systems hosting folder shares that are to be managed by the product; all domain controllers in all managed domains; all systems on which the Engine, Agent or Event Monitor components are installed.	"ProxyRights"
"Create a token object" [SeCreateTokenPrivilege], "Impersonate a client after authentication" [SeImpersonatePrivilege], "Act as part of the operating system" [SeTcbPrivilege]	All systems on which the Engine, Agent or Event Monitor components are installed.	"ProxyRights"
"Back up files and directories" [SeBackupPrivilege], "Bypass traverse checking" [SeChangeNotifyPrivilege], "Manage auditing and security log" [SeSecurityPrivilege], "Restore files and directories" [SeRestorePrivilege], "Take ownership of files or other objects" [SeTakeOwnershipPrivilege]	All systems hosting folder shares that are to be managed by the product; all domain controllers in all managed domains; all systems on which the Engine, Agent or Event Monitor components are installed.	"ProxyRights"
"Create symbolic links" [SeCreateSymbolicLinkPrivilege] Only on Vista / Win2K8 & newer.	All systems hosting folder shares that are to be managed by the product; all domain controllers in all managed domains; all systems on which the Engine, Agent or Event Monitor components are installed.	"ProxyRights"

Right/Privilege	Applies to	Security Principle
"Synchronize directory service data" [SeSyncAgentPrivilege]	All domain controllers in all managed domains; the system on which the Event Monitor component is installed.	"ProxyRights" f this group has been granted Read access to all attributes of all objects in a managed domain, then this privilege is not needed on any domain controllers in that same domain.
"Log on as a batch job" [SeBatchLogonRight]	The system on which the Engine component is installed.	The administrative user whose credentials are used to log in to the Setup Wizard during configuration of the NSM Engine. By default, the build-in NSMAdministrators group is granted this right on all domain controllers and member servers.
"Log on as a batch job" [SeBatchLogonRight]	The system on which the Engine component is installed.	"Admins", File / Storage Reporting Users

As indicated in the table above, installing any of the product components grants the appropriate rights and privileges on the server on which the component is installed. However, in certain situations, the security changes that are configured automatically during the installation process are not sufficient to meet all of the security requirements needed to monitor events and manage storage across an entire domain or multiple domains.

A.3 ProxyRights Group

By default, whenever any of the components of Novell Storage Manager 3.1.1 for Active Directory are installed on a computer in a domain, the NSMProxyRights universal security group is granted membership in that domain's Administrators built-in security group. This grants the product all of the necessary permissions to read and write attribute values on objects in the domain. This also eliminates the need for the *Synchronize directory service data* privilege to be granted to the NSMProxyRights group on each domain controller in the domain.

By default, whenever any of the components of Novell Storage Manager 3.1.1 for Active Directory are installed on a member server in a domain, NSMProxyRights is granted membership in the built-in Administrators group on the member server.

On other servers in the domain that are hosting user or collaborative storage managed by Novell Storage Manager 3.1.1 for Active Directory, you must also grant NSMProxyRights group membership in the built-in Administrators group. This is necessary because there are many storage management actions performed that require membership in this group regardless of the LSA privileges that the user has been granted—in particular, managing file shares and directory quotas.

Additionally, the other servers in the domain that are not hosting components, but are hosting user or collaborative storage, must have the rights and privileges described in the table above, along with some file share and NTFS permissions. The easiest way of granting these rights and privileges is through Group Policy objects in Active Directory.

As explained in "Setting Rights and Privileges on Managed Storage" and of the *Novell Storage Manager 3.1.1 for Active Directory Installation Guide*, you must grant Full Control sharing and security privileges to the NSMProxyRights group for each share that Novell Storage Manager 3.1.1 for Active Directory will manage.

A.4 Windows Clustering via Proxy Agents

Novell Storage Manager 3.1.1 for Active Directory supports clustering of Windows Server 2003 and later through proxy agents. Configuring a cluster to be managed through a proxy agent is similar to configuring an individual server to be managed by a proxy agent. In particular, the NSMProxyRights group must be granted membership in the built-in Administrators group and it must also be granted all of the LSA rights and privileges, that are granted at each cluster node. When this is done, the folder share permissions and NTFS permissions that are required must be granted to the NSMProxyRights group for all shares and NTFS volumes that will be managed by Novell Storage Manager 3.1.1 for Active Directory.

A.5 NAS Devices

Novell Storage Manager 3.1.1 for Active Directory also supports Network Attached Storage (NAS) devices as hosts for managed user or collaborative storage. NAS device support testing has been conducted exclusively on EMC Celerra and NetApp filer, which is also known as a NetApp fabric-attached storage (FAS) device. Although Novell Storage Manager 3.1.1 for Active Directory might be able to manage storage on other NAS devices, no other testing had been conducted at the time of this publication.

For a NetApp filer device, configuration is very simple because the device does not fully emulate a Windows Server at the operating system level. Use the NetApp filer administration utility to join the NAS device to a domain that is being managed by Novell Storage Manager 3.1.1 for Active Directory. Then grant the NSMProxyRights group membership in the NAS device's built-in Administrators group. When this is done, grant the NSMProxyRights group the folder share and NTFS permissions that are required to manage the storage. There are no LSA rights and privileges to grant on a NetApp filer NAS device.

For an EMC Celerra NAS device, configuration is similar to configuring a server in the domain to be managed by a proxy agent. Join the NAS device to a domain that is being managed by Novell Storage Manager 3.1.1 for Active Directory. Then grant the NSMProxyRights group membership in the NAS device's built-in Administrators group. When this is done, grant the NSMProxyRights group the folder share and NTFS permissions that are required to manage the storage. Finally, grant the LSA rights and privileges to the NSMProxyRights group, except the rights and privileges that don't exist on the EMC Celerra NAS device.

NOTE: If the EMC Celerra NAS device is set up to simultaneously support Windows clients via CIFS and UNIX or Linux clients via NFS, it is necessary for all Windows user accounts to have valid non-zero values configured in their UID and GID attributes within Active Directory. This UID/GID requirement becomes effective when the NAS device is configured to simultaneously use both CIFS and NFS.

B Distributed File System (DFS)

Previous versions of Novell Storage Manager 3 supported Windows Distributed File System (DFS) namespaces, with some significant limitations. With the release of Version 3.0.4, Novell Storage Manager provided complete support for DFS.

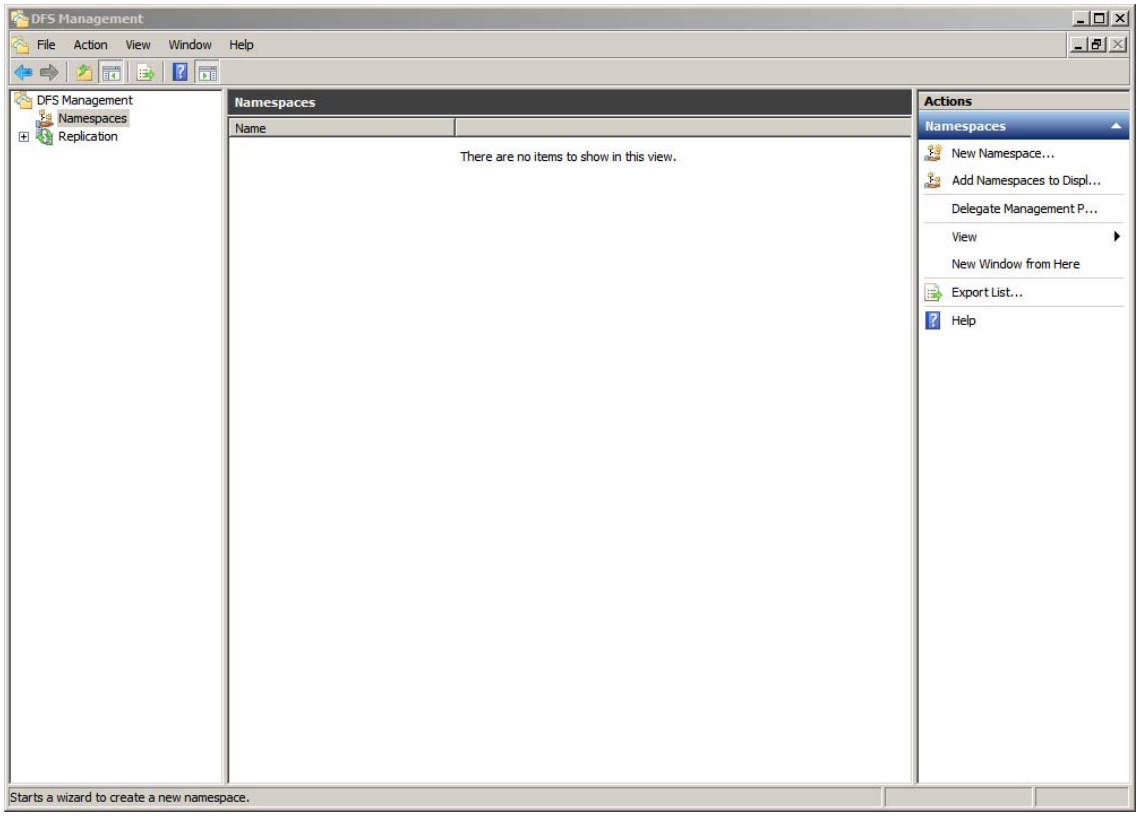
This section provides procedures for configuring the DFS namespaces to work with Novell Storage Manager.

- Section B.1, “Creating DFS Namespace Permissions,” on page 245
- Section B.2, “Configuring DFS Folders,” on page 251

B.1 Creating DFS Namespace Permissions

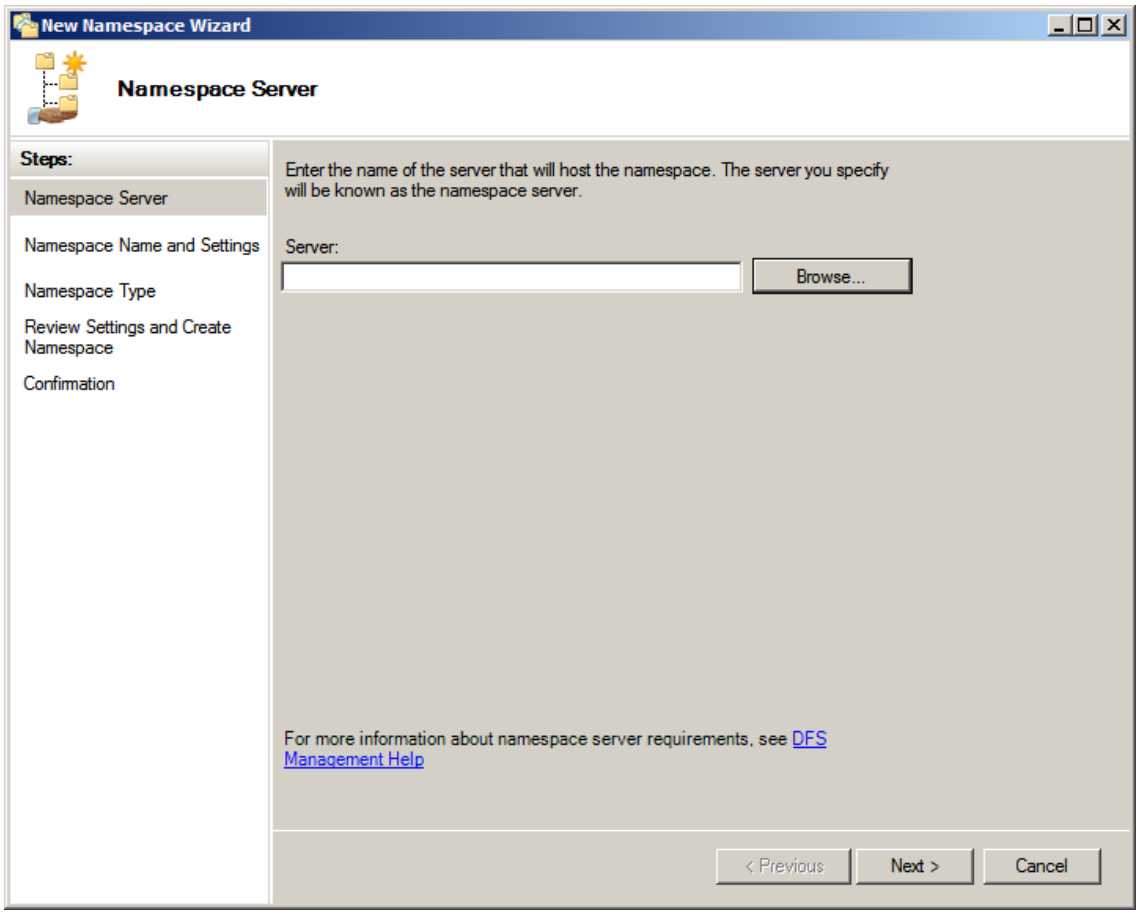
The Novell Storage Manager Proxy Rights Group (named NSMProxyRights by default) requires Full Control in the CIFS permissions on the root share of the DFS namespace.

1 Click *Start* > *Administrative Tools* > *DFS Management* to launch the DFS Management console.



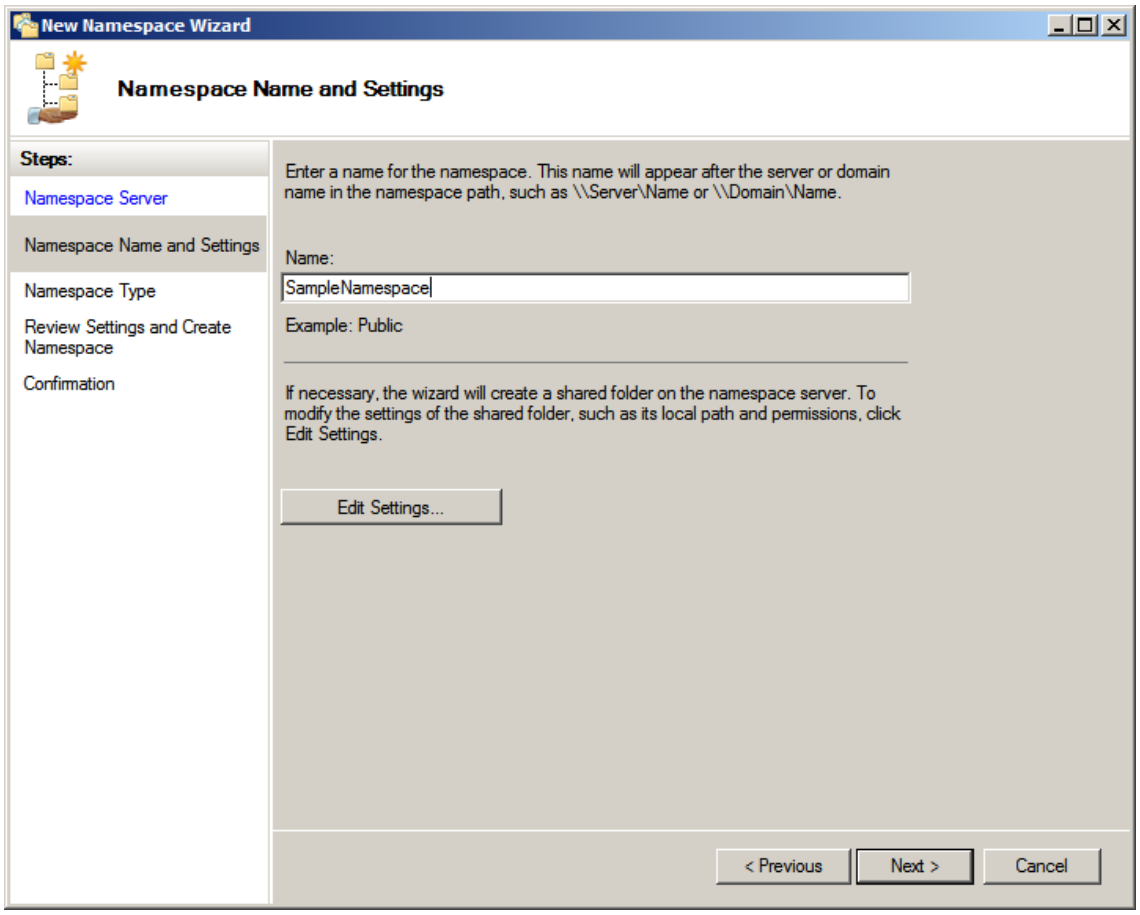
2 Right-click the *Namespaces* node and select *New Namespace*.

This launches the New Namespace Wizard.



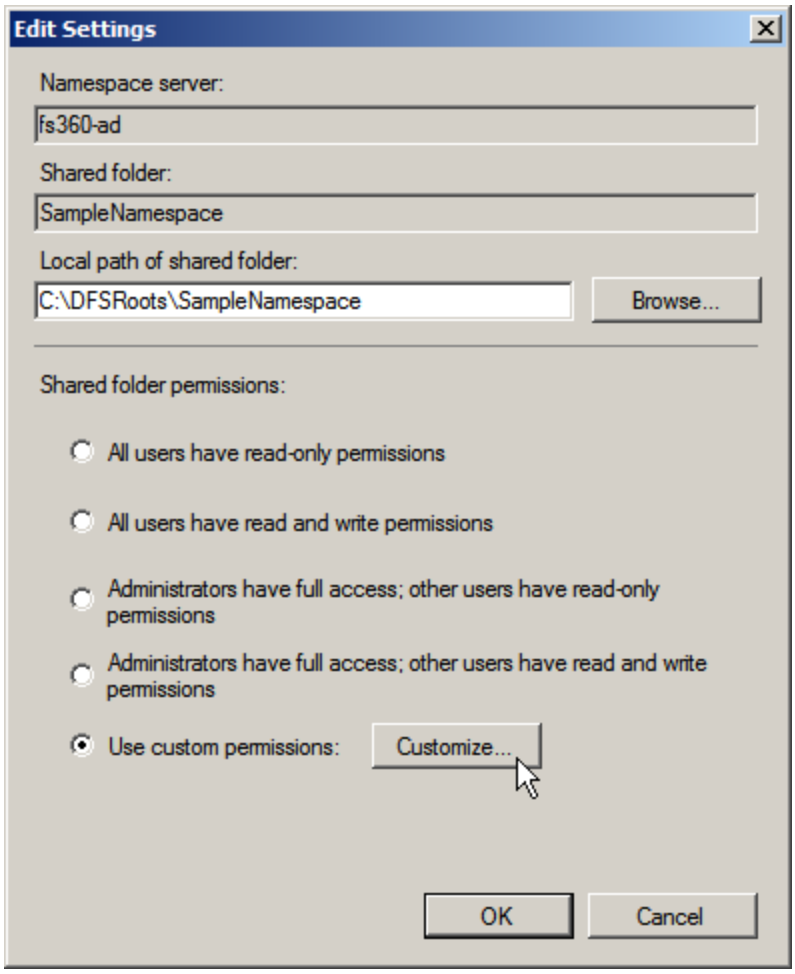
3 Use the *Browse* button to specify the server that will host the namespace.

4 Click *Next*.

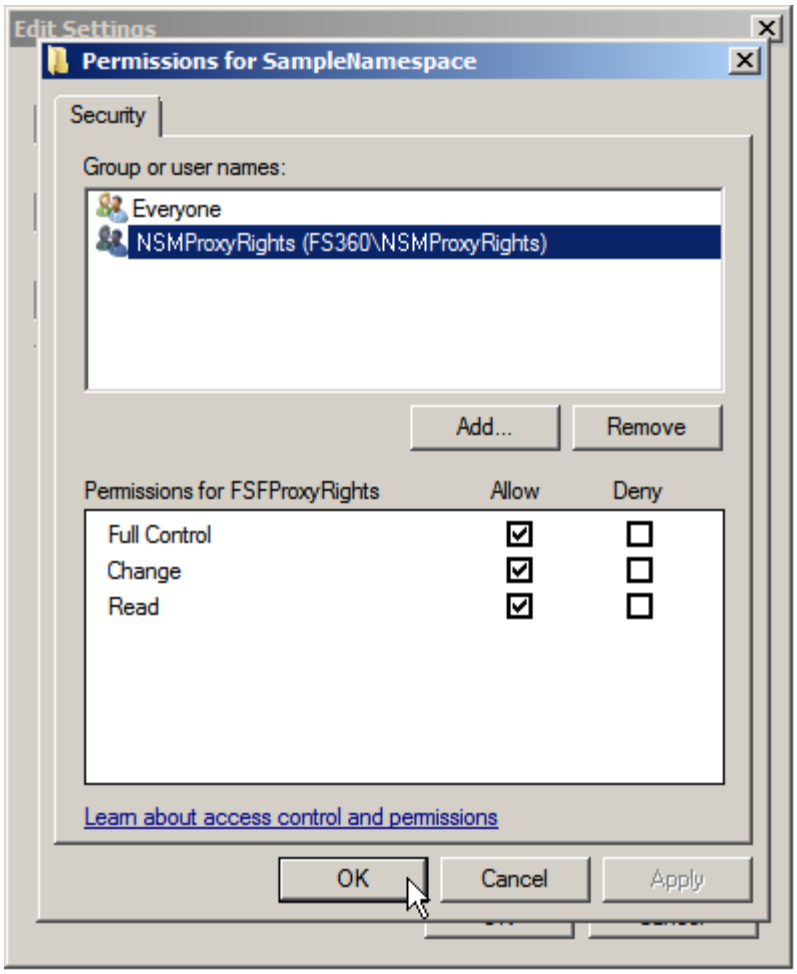


5 In the *Name* field, specify the name of the namespace.
For example, HomeNamespace or Public.

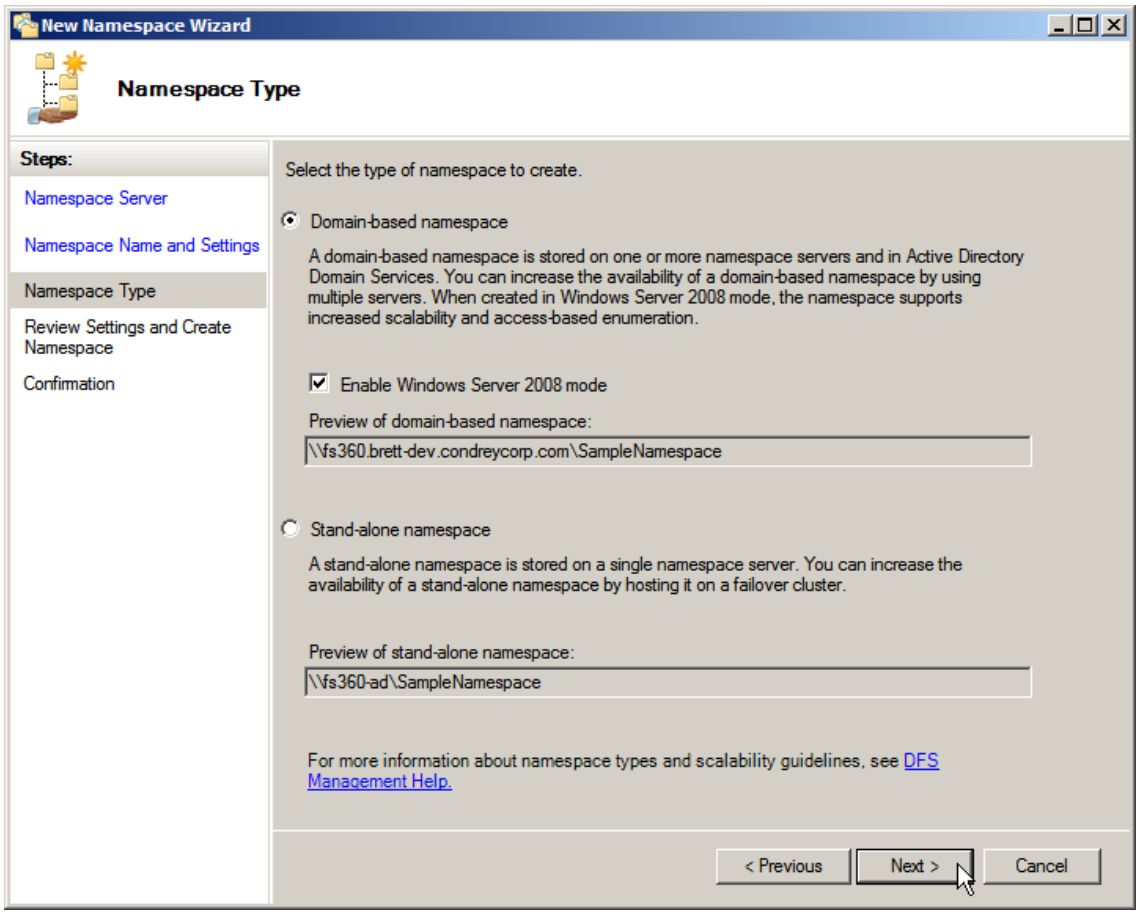
6 Click *Edit Settings*.



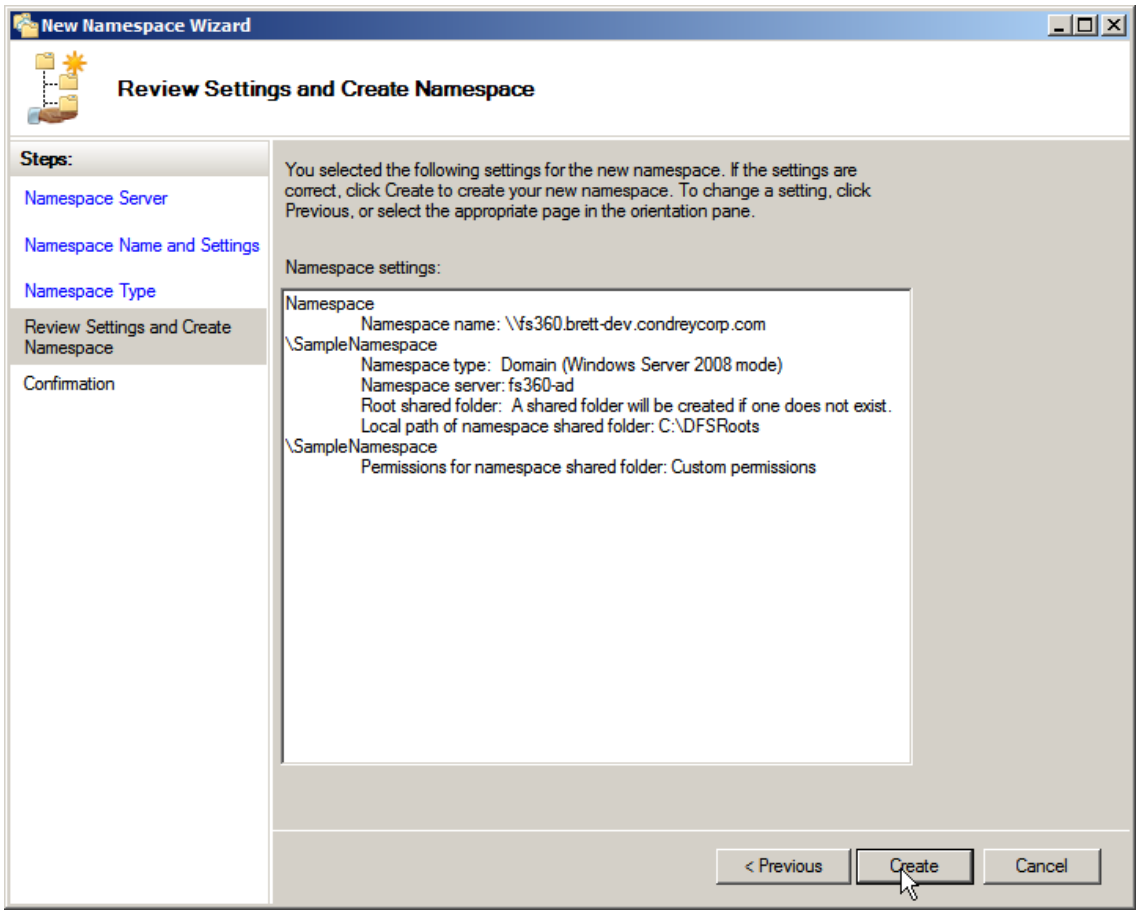
7 Select *Use custom permissions* and click *Customize*.



8 In the Permissions dialog box, select the proxy rights group, select the *Full Control* check box, then click *OK*.



9 In the *Namespace Type* wizard page, select the type of namespace to create, then click *Next*.



10 Review settings and click *Create*.

11 Click *Close* to close the wizard.

B.2 Configuring DFS Folders

Novell Storage Manager 3.1.1 for Active Directory requires definite paths in its policies. Because namespaces can provide multiple targets for DFS links and thereby introduce ambiguity, a DFS namespace must be configured with one of the following three options:

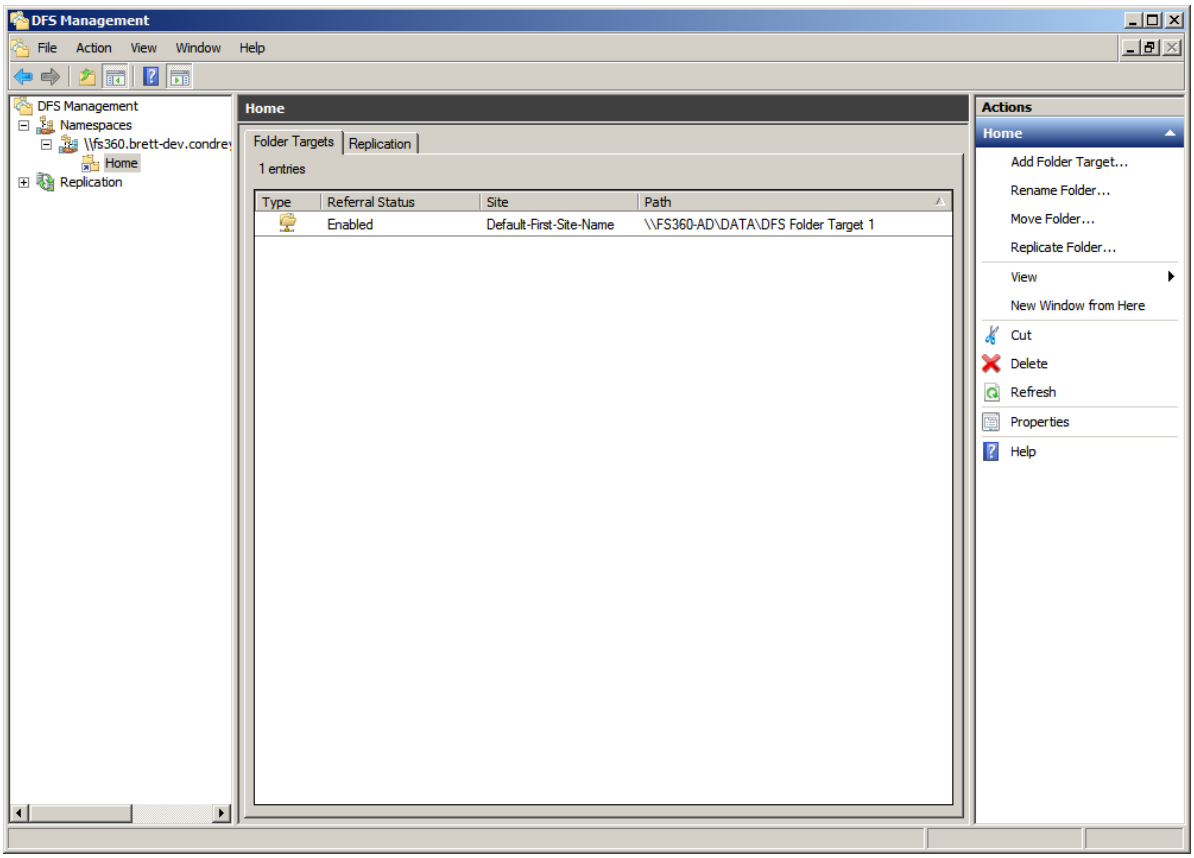
- Section B.2.1, "Providing Only One Target Per DFS Link," on page 251
- Section B.2.2, "Disabling All but One Target Per DFS Link," on page 252
- Section B.2.3, "Enabling Multiple Target Paths," on page 253

B.2.1 Providing Only One Target Per DFS Link

The simplest way to guarantee that NSM has unambiguous DFS paths is to give each DFS link a single target.

In the following graphic, there is just one target path and it is enabled.

Figure B-1 *One Target Path*

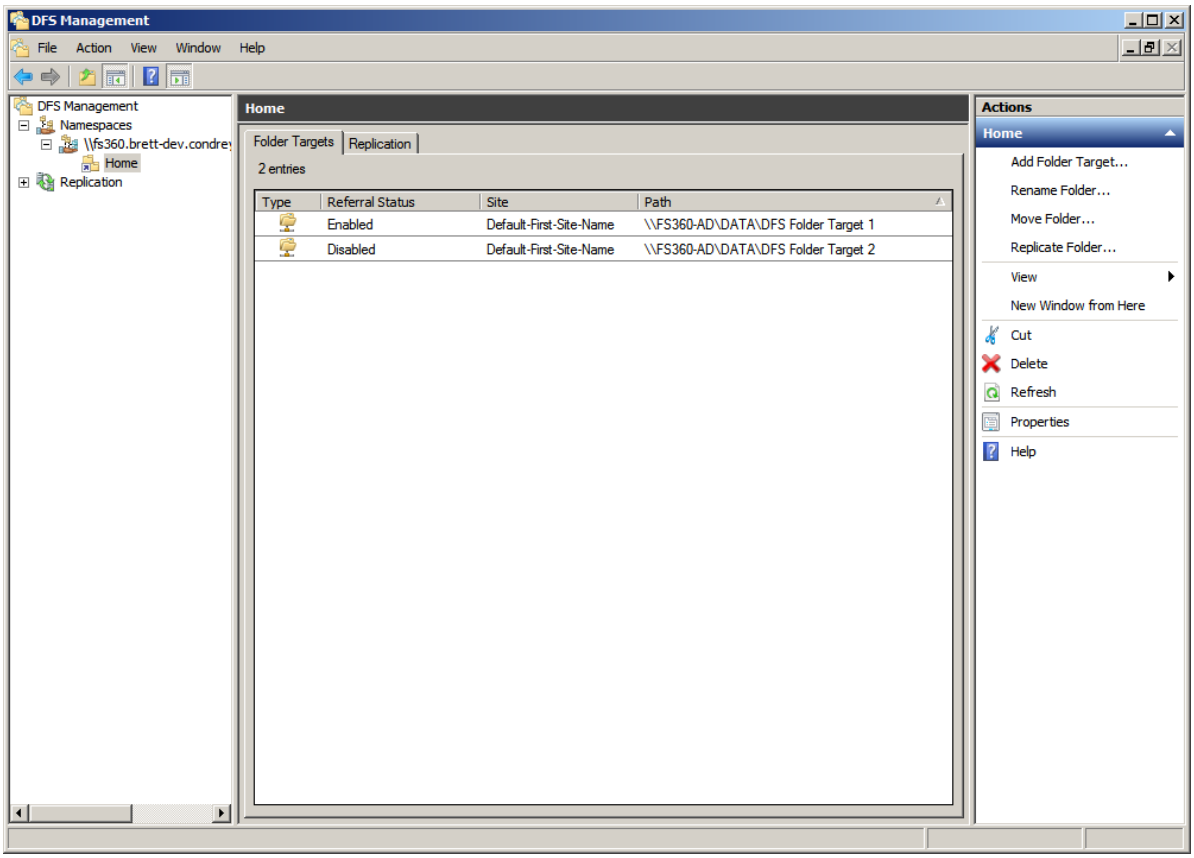


B.2.2 Disabling All but One Target Per DFS Link

If a DFS namespace is used for high availability, such as ensuring that users can access a replicated copy of their data, it might be appropriate to create multiple targets in a DFS link and disable all but one. If the enabled link target becomes unavailable, an administrator can disable the downed target and enable a replication target. As long as only one target is enabled for a given DFS link, Novell Storage Manager can successfully provision and manage storage through the DFS path.

In the following graphic, there are multiple target paths, but only one is enabled.

Figure B-2 *Multiple Target Paths with One Enabled*



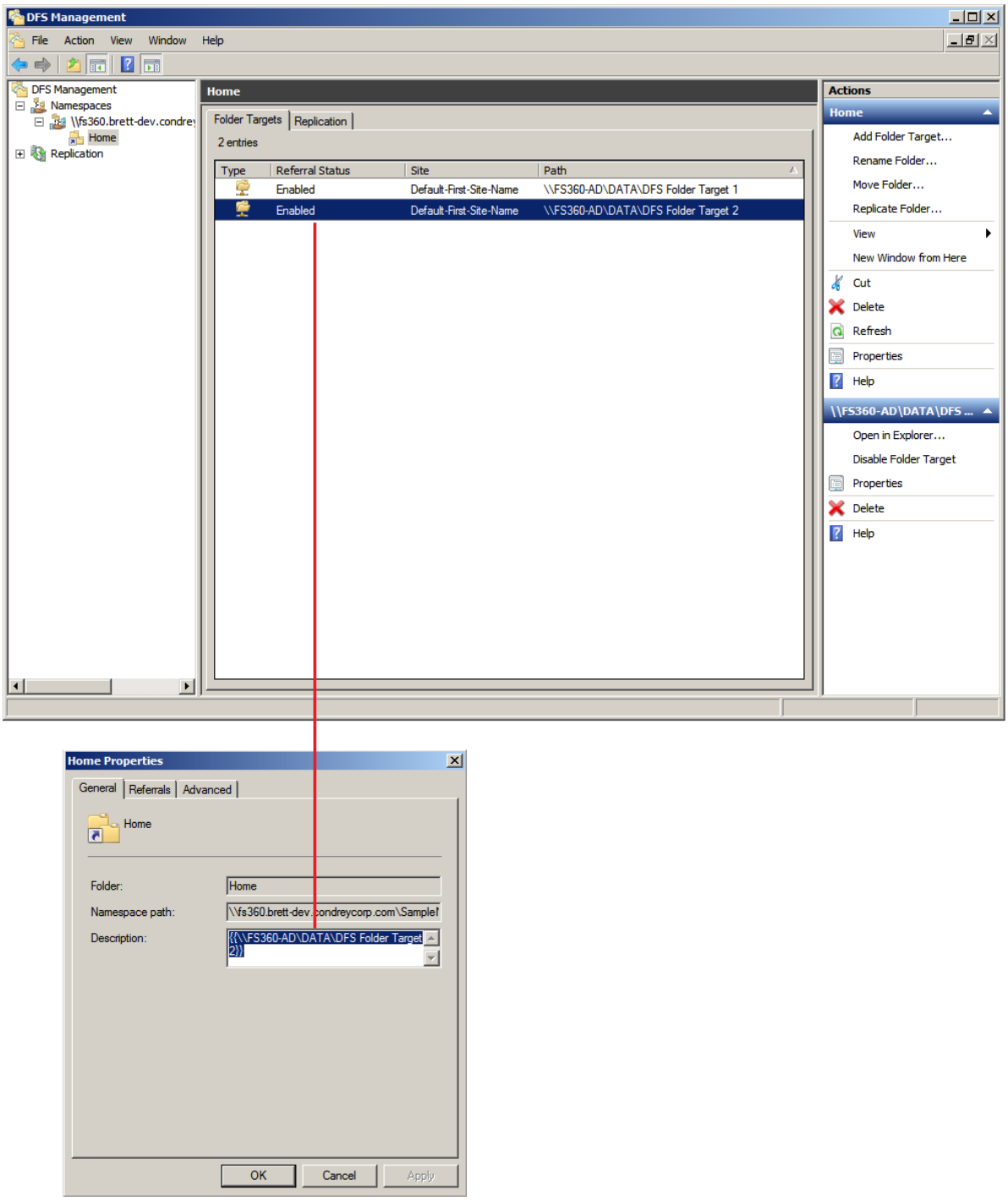
B.2.3 Enabling Multiple Target Paths

Novell Storage Manager can parse the description field on a DFS folder to determine which of several enabled targets is the primary, unambiguous target. This allows Novell Storage Manager to manage namespaces with multiple enabled targets in a DFS link.

To do this, the description for the DFS link must enclose the complete UNC path of the path Novell Storage Manager should use in double curly braces. For example, {{\\Server\Share\Path}}. This must be identical to the UNC path in the target link; it cannot be a subdirectory.

In the following graphic, there are two target paths enabled.

Figure B-3 *Two Target Paths Enabled*



The Home Properties dialog box is accessed by double-clicking the listing in the DFS Management console.

C Active Directory Schema Extensions

Novell Storage Manager 3.1.1 for Active Directory extends the Active Directory schema by adding two new attributes and one new class. These are:

- Section C.1, “Attributes,” on page 255
- Section C.2, “Classes,” on page 256

C.1 Attributes

- Section C.1.1, “ccx-FSFAuxiliaryStorage,” on page 255
- Section C.1.2, “ccx-FSFManagedPath,” on page 256

C.1.1 ccx-FSFAuxiliaryStorage

A list of one or more paths pointing to managed auxiliary storage associated with this object

Table C-1 *ccx-FSFAuxiliaryStorage Specifications*

Active Directory Attribute Property	Value
Name	ccx-FSFAuxiliaryStorage
LDAP Display Name	ccx-FSFAuxiliaryStorage
Admin Display Name	ccx-FSF-Auxiliary-Storage
Admin Description	List of one or more paths pointing to managed auxiliary storage associated with this object
ASN.1 ID	1.3.6.1.4.1.35052.1.1.100.1.1
Syntax	ADSTYPE_CASE_IGNORE_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	False
Schema ID GUID	c4bacb95-075e-11df-bcab-eee40b817f62
Search Flags	-
System Flags	-
Link ID	-

Active Directory Attribute Property	Value
Attribute Security GUID	cd55682f-3987-446d-a18e-cfd8d53b95f2
Partial Attribute Set Member	False

C.1.2 ccx-FSFManagedPath

The managed path attribute for objects (such as groups and containers) that do not inherently have a home folder attribute.

Table C-2 *ccx-FSFManagedPath Specifications*

Active Directory Attribute Property	Value
Name	ccx-FSFManagedPath
LDAP Display Name	ccx-FSFManagedPath
Admin Display Name	ccx-FSF-Managed-Path
Admin Description	Managed path attribute for collaborative objects
ASN.1 ID	1.3.6.1.4.1.35052.1.1.100.2.1
Syntax	ADSTYPE_CASE_IGNORE_STRING
Sized – Lower Limit	-
Sized – Upper Limit	-
Single Valued	True
Schema ID GUID	c4bacb96-075e-11df-bcab-eee40b817f62
Search Flags	-
System Flags	-
Link ID	-
Attribute Security GUID	cd55682f-3987-446d-a18e-cfd8d53b95f2
Partial Attribute Set Member	False

C.2 Classes

- Section C.2.1, “ccx-FSFManagedAttributes,” on page 256

C.2.1 ccx-FSFManagedAttributes

An auxiliary class holding common attributes managed by Novell Storage Manager 3.1.1 for Active Directory.

Table C-3 *ccx-FSFManagedAttributes Specifications*

Active Directory Class Property	Value
Name	ccx-FSF-Managed-Attributes
LDAP Display Name	ccx-FSF-Managed-Attributes
Admin Display Name	ccx-FSF-Managed-Attributes
Admin Description	Auxiliary class holding common attributes managed by Novell Storage Manager
ASN.1 ID	1.3.6.1.4.1.35052.1.1.2.1.1
Schema ID GUID	c4bacb93-075e-11df-bcab-eee40b817f62
Class Type	Auxiliary
Parent Class	top
Default Object Category	ccx-FSFManagedAttributes
Naming Attribute	-
Mandatory Attributes	-
Optional Attributes	ccx-FSFAuxiliaryStorage
	ccx-FSFManagedPath
Possible Superiors	-
System Possible Superiors	-
System Flags	-
Default Security Descriptor	-

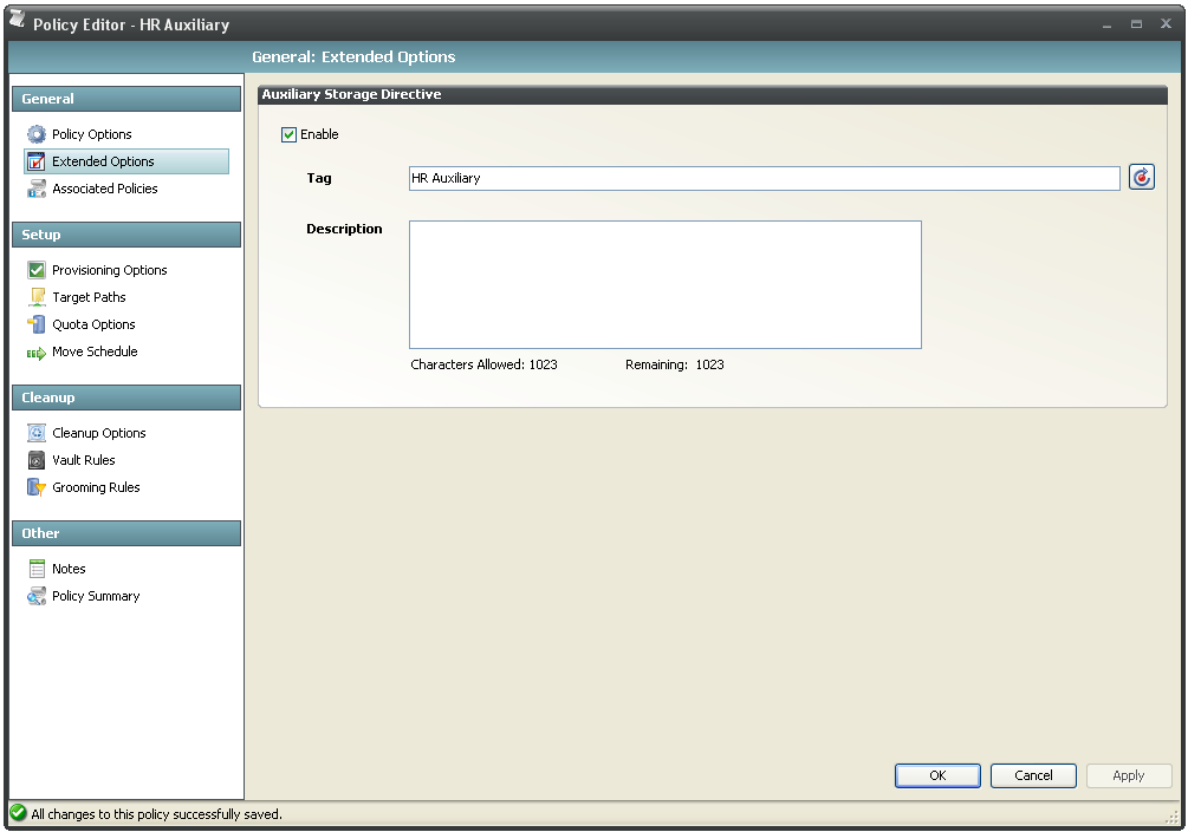
D AuxMap

The AuxMap utility lets you map drive letters to a user's auxiliary storage folders through command line parameters in a Windows logon script. When the user logs in to Active Directory, AuxMap reads the auxiliary attribute associated with each auxiliary storage folder assigned to the user and then enables the drive mappings.

AuxMap is supported on Windows XP SP2 and later, Windows Vista, Windows Server 2008, and Windows 7.

You must have the *Enable* check box checked, and an entry in the *Tag* field of the Extended Options of an auxiliary storage policy.

Figure D-1 *Extended Options Page of an Auxiliary Storage Policy*



For more information, see "Enabling Auxiliary Storage Extended Options" on page 62.

At the root of the ISO, go to the applicable path to locate AuxMap:

- `\Windows\x86\AuxMap.exe`
- `\Windows\x86_64\AuxMap.exe`

Example Usage:

```
AuxMap --drive=<drive-letter> --storage=<storage-name>

AuxMap -d=<drive-letter> -s=<storage-name>

AuxMap --delete --drive=<drive-letter>

AuxMap --list-mappings
```

The following command line switches are supported:

Table D-1 *AuxMap Command Line Switches*

`--help`
or
`-?`
	Displays command line switch help information for AuxMap.

`--list-mappings`
or
`-lm`
	Lists all currently mapped network drives.

`--drive=<drive-letter-or-path>`
or
`-d=<drive-letter-or-path>`
	This must be a single uppercase letter in the range A through Z. The storage referred to in the storage parameter will be mapped to the chosen drive letter.

`--storage=<storage-name>`
or
`-s=<storage-name>`
	This must be the name of an auxiliary storage area that has been provisioned for the user and is currently enabled and specified in the *Tag* field of the Extended Options page of an auxiliary storage policy. If the string in the *Tag* field contains a space, you must have quotes around the auxiliary storage area name.

`--delete`	Performs a map delete on the specified drive letter or path. Use with the `--drive` or `-d` switches.
`--debug`	If present, this causes AuxMap to produce more detailed diagnostic logging as it executes.

The following command line switches are ignored if present. They were valid in versions prior to Novell Storage Manager 3.0, but they are no longer applicable.

Table D-2 *Ignored Command Line Switches*

`--root`
or
`-r`
	Deprecated. All mappings are map-rooted.

`--force`
or
`-f`
	Deprecated. The drive letter or path will always be unmapped (if it is currently mapped) before being mapped.

`--quiet`
or
`-q`
	Deprecated. Redirect the output by using >NUL: 2>NUL: to suppress all console output.

`--log=<`*`log-file`*`>`
or
`-l=<`*`log-file`*`>`
	Deprecated. Redirect the output using >*filename* or 2>*filename*.

E Glossary

Associated policy: A policy specifically assigned to a container, group, or user through the Associations settings in the Policy Editor.

Auxiliary policy: A policy associated with a User Home Folder policy that creates auxiliary storage for a user (along with the user home folder that is created from a user home folder policy) when a new user is created in Active Directory.

Auxiliary storage: Home folders associated to a user in addition to the regular network home folder. Depending on the storage policy, auxiliary storage can be made accessible or unaccessible to the associated user.

Backfill operation: Previous terminology for what is now known as a "Management Action."

Blocking policy: A policy designed to block other Novell Storage Manager policies from affecting members of organizational units, members of groups, or even individual users.

Consistency check: This Management Action notifies you of inconsistencies or potential problems pertaining to user and group storage being managed through Novell Storage Manager. These potential problems might be missing storage quotas, inconsistent directory attributes, missing home directories, inconsistent file paths, and more.

Container: A synonym for organizational unit in the Novell Storage Manager documentation.

Collaborative storage: A shared storage area where a group of people in an organization can collaborate by sharing files. Novell Storage Manager lets you easily create collaborative storage areas through collaborative storage policies that you can assign to Group objects or to an organizational unit.

Cross-Empire Data Migration: A susbsystem introduced in Novell Storage Manager 3.0.1 that allows for the movement of file system data between storage infrastructures on different platforms governed by different identity and security frameworks. Novell Storage Manager currently migrates data only from a Novell network to a Microsoft network.

Deferred delete event: The scheduled deletion of a user home folder or a collaborative storage folder, but has not yet taken place because the number of days in the Cleanup Storage parameter of the policy has not been met.

Dynamic Template Processing: Within Novell Storage Manager, the process that creates personal folders in a collaborative storage folder.

Effective policy: A policy that is applied by default to a group, user, or subcontainer when no associated policy is specifically assigned.

Enumeration operation: The process of locating and displaying all User objects.

Identity map: Within the Cross-Empire Data Migration subsystem, the file that lets you make security and ownership associations between the source Novell platform and the target Microsoft platform.

Management Action: A manual action that allows you to enact a setting from a policy on existing users.

NSMAdmin: The management interface for Novell Storage Manager.

Personal folder: A user-specific folder in a collaborative storage area.

Policy: Rules and settings within Novell Storage Manager that indicate what storage-specific actions to enact when an event in Active Directory takes place. These actions include creating user storage when a new user is added to Active Directory, moving storage when a user is moved from one organizational unit to another, and archiving or deleting storage when a user is removed.

Policy weight: When a user is a member of multiple groups and each group has a separate policy, Novell Storage Manager uses this setting to determine which policies to apply. Novell Storage Manager applies the policy with the largest numerical weight.

Primary policy: Previous terminology specific to user-based storage. Because there are so many different types of user-based policies in Novell Storage Manager for Active Directory, this term is now rarely used.

Quota Manager: A Web browser-based management interface for designated users such as help desk administrators or support personnel that enables them to adjust user home folder or collaborative storage areas without needing rights to the file system. Quota Manager can also provide select storage information such as total number of files and file types in a home folder.

Target Path: The path to the network share where user home folders are hosted.

Template: If you want to have subfolders and documents provisioned in a home folder, auxiliary storage folder, or collaborative storage folder when they is created, you can use an existing file path in the file system as a template.

F Documentation Updates

This section contains information about documentation content changes that were made in this *Novell Storage Manager 3.1.1 for Active Directory Administration Guide* after the initial release of Novell Storage Manager 3.0 for Active Directory. The changes are listed according to the date they were published.

The documentation for this product is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the changes listed in this section.

If you need to know whether a copy of the PDF documentation that you are using is the most recent, the PDF document includes a publication date on the title page.

The documentation was updated on the following dates:

F.1 October 17, 2013

Updates were made to the following sections:

Location	Update Description
"Apply Home Drive" on page 212.	New section.
"Apply Ownership" on page 213.	New section.

F.2 September 26, 2013

Updates were made to the following sections:

Location	Update Description
"Importing Identity Associations through Delimited Text" on page 120.	New section.
"Creating Object Associations" on page 124.	New section.
Section 11.5.5, "Saving the Identity Map," on page 132.	New section.
Section 11.5.6, "Exporting an Identity Map," on page 132.	New section.
Section 11.5.7, "Importing an Identity Map," on page 132.	New section.

F.3 June 12, 2013

Updates were made to the following sections:

Location	Update Description
Section 5.5.1, “Setting Policy Options,” on page 43.	Updated the description of Bypassable Events.
Section 5.5.4, “Setting Target Paths,” on page 46.	Updated the description of the Leveling Algorithm.
Section 12.1.6, “Pending Events,” on page 219.	Updated the description of the *Defer* field.
“Replacing an Unexpired License File” on page 233.	New section.
“Replacing an Expired License File” on page 234.	New section.
“Deleting an Event Monitor” on page 234.	New section.
“Deleting an Agent” on page 235.	New section.

F.4 February 13, 2013

Updates were made to the following sections:

Location	Update Description
“Using the NovScan NLM to Run the Job File” on page 181.	Added parameters for using the NovScan NLM.
“Using the NovScan NLM to Run the Job File” on page 188.	Added parameters for using the NovScan NLM.

F.5 January 18, 2013

Updates were made to the following sections:

Location	Update Description
Multiple locations throughout the manual.	Changed references of 3.0.*x* to 3.1.
Chapter 9, “Mobile Management,” on page 103.	New chapter.
Chapter 10, “The Network Operations Center Dashboard,” on page 105.	New chapter.
“Folder to Folder” on page 114.	Discussion of new Cross-Empire Data Migration utilities.
Section 11.12, “Performing a Folder to Folder Migration,” on page 166.	Presented a two-phased approach for folder to folder migration, including the use of the new utilities.
Appendix E, “Glossary,” on page 263.	Added new glossary entries.

F.6 October 15, 2012

Updates were made to the following sections:

Location	Update Description
"Folder to Folder" on page 114.	New paragraph about the *Skip Open Files* option.
Section 11.12, "Performing a Folder to Folder Migration," on page 166.	IMPORTANT information added about the *Skip Open Files* option.
Section 11.12.1, "Migrating to an Existing Target Folder," on page 167.	Inserted a new Step 2 on page 167. Expanded Step 16 on page 172 to include the *Advanced Namespace Handling* and *Open File Options*.
Section 11.12.2, "Creating a Target Folder in the Data Migration Wizard," on page 196.	Inserted a new Step 2 on page 196. Expanded Step 17 on page 201 to include *Advanced Namespace Handling* and *Open File Options*.

F.7 May 18, 2012

Updates were made in the following section:

Location	Update Description
Appendix B, "Distributed File System (DFS)," on page 245.	New appendix.

F.8 February 2, 2012

Updates were made to the following sections:

Location	Update Description
Throughout the manual.	Changed 3.0.2 to 3.0.*x*.
Section 5.5.5, "Setting Quota Options," on page 47	Added a note about managing quota on NAS devices.

F.9 July 5, 2011

Updates were made to the following sections:

Location	Update Description
Section 8.3, "Understanding Quota Manager Status Indicators," on page 100	Added this section.

F.10 May 16, 2011

Updates were made to the following sections:

Location	Update Description
"What's New" on page 11	Description of identity mapping in the Cross-Empire Data Migration subsystem.
Chapter 6, "Managing Existing Collaborative Storage," on page 67	Added this chapter.
Section 11.2, "Security and Ownership," on page 114	Updated this section with new information on identity mapping.
Section 11.5, "Creating and Modifying an Identity Map," on page 119	Added this section.
Appendix E, "Glossary," on page 263	Added new glossary terms.

F.11 March 16, 2011

Updates were made to the following sections:

Location	Update Description
Section 11.3.1, "Prerequisite Tasks," on page 116	Added this section.
Section 11.10, "Performing a Group to Group Data Migration," on page 153	Prefaced the procedures with an Important notice stating that the group folders to be migrated must be managed through group-based collaborative storage policies in eDirectory.

F.12 March 1, 2011

Updates were made to the following sections:

Location	Update Description
Section 11.4, "Creating the Migration Proxy Account," on page 117	Inserted information on the need for the Universal Password policy to support 32-character passwords, and provided a link to documentation on how to reconfigure the policy.

F.13 February 14, 2011

Updates were made to the following sections:

Location	Update Description
Chapter 1, "What's New," on page 11	Descriptions of features new to Novell Storage Manager 3.0.1.
Section 5.10, "Copying Policy Data," on page 59	Procedures for importing a policy.

Location	Update Description
Chapter 11, “Performing a Cross-Empire Data Migration,” on page 111	Procedures for using Data Migration.
Section 12.1.12, “Data Migration,” on page 224	Summary of Data Migration.