

NetStorage for Linux^{*} Administration Guide

Novell[®] Open Enterprise Server

2.0 SP1

December, 2008

www.novell.com



Legal Notices

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

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

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

Copyright © 2007–2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

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

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

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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	7
1 NetStorage Overview	9
1.1 How NetStorage Works	9
1.2 What Users See When They Access NetStorage	10
1.3 What's Next	11
2 What's New	13
3 Installing NetStorage	15
3.1 Requirements	15
3.2 Installing NetStorage After the OES Installation	16
3.3 Changing the NetStorage Default Configuration	16
3.4 Creating Storage Location Objects and Lists	17
3.4.1 SSH Storage Location Objects	17
3.4.2 Creating a Storage Location Object	17
3.4.3 Creating a Storage Location List	19
3.5 What's Next	19
4 Configuring NetStorage with Novell Cluster Services	21
4.1 NetStorage Installation and Configuration	21
4.2 Novell Cluster Services Configuration and Setup	22
4.2.1 Prerequisites	22
4.2.2 Creating a NetStorage Cluster Resource	22
4.2.3 Editing NetStorage Load and Unload Scripts	23
4.2.4 Setting the NetStorage Resource Start, Failover, and Failback Modes	24
4.2.5 View or Edit NetStorage Resource Server Assignments	25
4.2.6 Accessing NetStorage After Cluster Configuration	26
5 Running NetStorage in a Virtualized Environment	27
6 Using NetStorage	29
6.1 Accessing NetStorage	29
6.2 Viewing or Modifying Directory and File Attributes and Rights	30
6.3 Accessing Archived Files	31
6.3.1 What Files Are Versioned	31
6.3.2 Accessing File Versions	32
6.4 Setting Directory Quotas on NSS Volumes and Directories	32
6.5 Purging and Salvaging Deleted NSS Files	33
7 Administering NetStorage	35
7.1 Using iManager to Administer NetStorage	35
7.2 Understanding the NetStorage Configuration Settings	36

7.2.1	Authentication Domains	36
7.2.2	Current Sessions	38
7.2.3	Files	38
7.2.4	iFolder Storage Provider	38
7.2.5	NetWare Storage Provider	38
7.2.6	NetStorage Options	40
7.2.7	NetStorage Statistics	41
7.2.8	Resource Usage	41
7.2.9	WebDAV Provider	41
7.2.10	Storage Location	41
7.3	What's Next	44
8	Troubleshooting NetStorage	45
8.1	Unexpected Results from Login Scripts	45
8.2	Slow Login	45
8.3	Configuring LDAP Contextless Login for Use with NetStorage	46
8.4	Configuring NetStorage to Use the Proper Code Page or Character Set	47
8.5	Configuring NetStorage with iChain	47
8.5.1	Enabling Cookieless Authentication	47
8.5.2	Editing the Logout.html.utf8 file	48
8.6	Accessing CIFS or SSH Storage Locations	48
8.7	LUM Must Have SSHD Access Enabled	48
8.8	Restricted SSH Access for Samba Users	48
8.9	Phantom Folders	49
8.10	The Assign Storage Location Page Navigates to the Home Page.	49
A	Security Considerations	51
A.1	Security Features	51
A.2	Security Configuration	52
A.2.1	NetStorage Configuration Settings	52
A.2.2	Security Information for Other Products	52
A.3	Security Recommendations	53
A.3.1	Registry Access Control	53
A.3.2	Use NMAS	54
A.3.3	Use SSL with Your Web Server.	54
A.3.4	Persistent and Session Cookies	54
A.3.5	Use Web Server Logs	54
A.3.6	Use XTLog	54
A.3.7	Denial of Service Attacks	54
A.3.8	Trusted Roots in CAPI	55
A.3.9	Certificate Validation Registry Setting	55
A.4	Other Security Considerations	55

About This Guide

This guide includes information on Novell® NetStorage, which provides secure Internet-based access to files and folders on a Linux* server in your network through either a browser or Microsoft* Web Folders.

- ♦ Chapter 1, “NetStorage Overview,” on page 9
- ♦ Chapter 2, “What's New,” on page 13
- ♦ Chapter 3, “Installing NetStorage,” on page 15
- ♦ Chapter 4, “Configuring NetStorage with Novell Cluster Services,” on page 21
- ♦ Chapter 5, “Running NetStorage in a Virtualized Environment,” on page 27
- ♦ Chapter 6, “Using NetStorage,” on page 29
- ♦ Chapter 7, “Administering NetStorage,” on page 35
- ♦ Chapter 8, “Troubleshooting NetStorage,” on page 45
- ♦ Appendix A, “Security Considerations,” on page 51

Audience

The audience for this document is network administrators. This documentation is not intended for users of the network.

Feedback

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

Documentation Updates

For the most recent version of this guide, see the *NetStorage Administration Guide for Linux* (http://www.novell.com/documentation/oes2/file_netstor_lx/index.html?page=/documentation/oes2/file_netstor_lx/data/h9izvdye.html#h9izvdye).

Additional Documentation

For information about Novell iManager, see the *Novell iManager 2.7 Administration Guide* (http://www.novell.com/documentation/imanager27/index.html?page=/documentation/imanager27/imanager_admin_27/data/bsxrjzp.html#bsxrjzp).

Documentation Conventions

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

In this documentation, a trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

NetStorage Overview

1

NetStorage provides secure Internet-based access to files and folders on Linux and NetWare[®] servers on your network, using either a browser or Microsoft Web Folders (Microsoft's implementation of WebDAV). NetStorage authentication relies on the power of Novell[®] eDirectory[™] to provide secure access, so Internet-based access is as secure as accessing files from within the network.

Novell NetStorage includes the following benefits:

- ♦ Lets users securely copy, move, rename, delete, read, and write files between any Internet-enabled machine and Linux or NetWare servers on your network.
- ♦ Lets users access archived copies of their files.
For more information, see the *OES 2 SPI: Novell Archive and Version Services 2.1 User Guide*.
- ♦ Eliminates the need to use a virtual private network (VPN) client to access files.
- ♦ Eliminates the need to e-mail or copy data from one machine to another.
- ♦ Supports Internet standards such as HTTP, HTTPS, HTML, XML, and WebDAV.
- ♦ Supports the use of drive mappings that users are accustomed to when they log in through the Novell Client[™] (see [Section 1.2, “What Users See When They Access NetStorage,” on page 10](#)).
- ♦ Provides access to network files and folders via Novell Virtual Office and Novell exteNd Director[™] 4.1 Standard Edition.
- ♦ Supports Storage Location objects used to display a specified name for a network directory in the NetStorage directory access list displayed through Microsoft Web Folders or a Web browser (see [“Storage Location” on page 41](#)).

With NetStorage installed on one OES Linux server, users can potentially have access to any Linux or NetWare 5 or later server anywhere on your geographically dispersed network.

- ♦ [Section 1.1, “How NetStorage Works,” on page 9](#)
- ♦ [Section 1.2, “What Users See When They Access NetStorage,” on page 10](#)
- ♦ [Section 1.3, “What's Next,” on page 11](#)

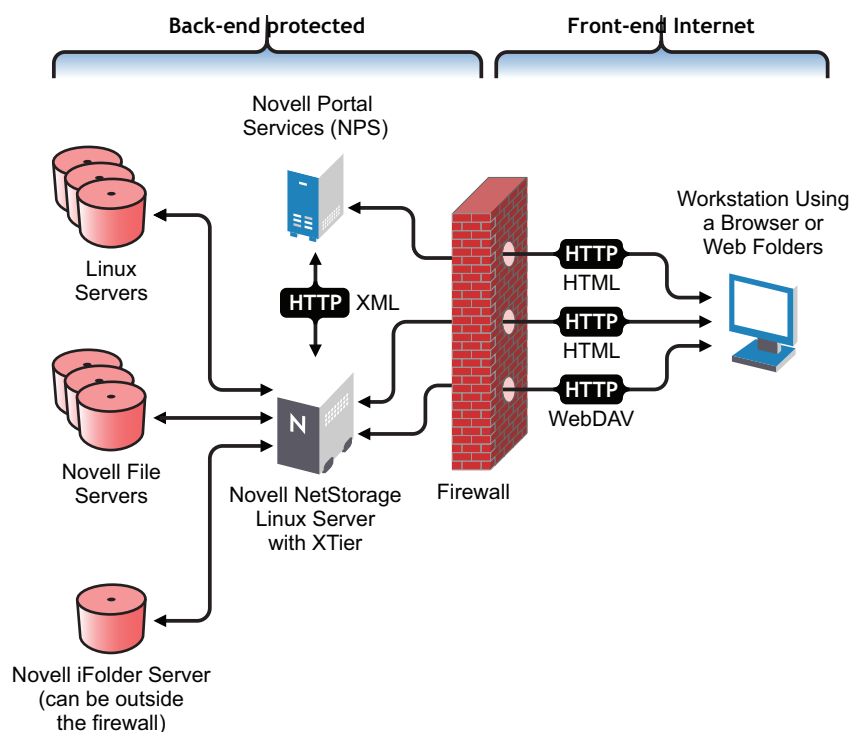
1.1 How NetStorage Works

NetStorage is installed on one Linux server that acts as a Middle Tier (also known as XTier) server. Middle Tier server configuration information is stored in an XML file on the Linux server. Novell iManager provides an easy method for changing Middle Tier configuration. XTier is the Novell Web services framework and is used by various Novell products.

NOTE: Previous versions of NetStorage were administered with the NSAdmin utility. Configuration should now be done through Novell iManager.

After the Middle Tier server is set up, it appears as an Internet Web server to users and can be accessed either with a Web browser or with Microsoft Web Folders. NetStorage also includes a gadget that provides access through Novell exteNd Director 4.1 Standard Edition.

Figure 1-1 Middle Tier Server



The Middle Tier server communicates with the NetWare or Linux servers in the network and provides secure authentication using eDirectory and the users' usernames and passwords.

All transactions can also be encrypted by using SSL to increase the security.

NOTE: Although SSL can be used to encrypt transactions, no server authentication is performed.

For specific information on how login scripts are processed by NetStorage, see “[Setting Up Login Scripts](#)” in the *Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide*. See also the [Login Script Processing by NetStorage TID10068983](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10068983.htm) (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10068983.htm>).

1.2 What Users See When They Access NetStorage

The NetStorage Web page displays the network files and folders currently accessible for each user. For NetWare servers, NetStorage reads the user's login script to determine drive mappings, reads eDirectory User object properties to determine the path to the user's home directory, and then displays a list of files and folders based on this information. Storage Location objects are required for accessing files and directories on Linux servers and can also be used on NetWare servers. If Storage Location objects have been created and the user has rights to view these objects, the directories associated with these objects are also displayed.

NetStorage reads the container, profile, and user login scripts only from the primary eDirectory server specified during the installation. For NetWare servers, it displays the user's drive mappings based only on those login scripts. However, because login scripts were designed to be processed by the Novell Client on the user's workstation, NetStorage processes only a subset of the login script functions.

TIP: If you specified alternate IP addresses or DNS names of servers in other eDirectory trees during the NetStorage installation, NetStorage reads the User object properties in the other eDirectory trees and also displays those home directories. This is useful if a user normally logs in to more than one eDirectory tree and you want that user to have access to additional home directories in different eDirectory trees through NetStorage. The User object name must be the same for each eDirectory tree.

NetStorage processes login scripts in order to find MAP statements. Each MAP statement defines a NetWare file system storage resource that the user can access through NetStorage. IF, ELSE, END, INCLUDE, and EXIT commands are also recognized by NetStorage. All other login script statements are treated as comments and ignored. Finally, login script variables are also recognized. Variables are preceded by a percent sign (%). Because mapped drives do not exist in Linux, you must create and use Storage Location objects to access storage on Linux servers.

Users might have specific eDirectory rights to certain files and folders on your network, but cannot access those files and folders through NetStorage unless login script drive mappings exist to those folders or the files and folders are in the user's home directory, or Storage Location objects have been created. If you want to provide users with NetStorage access to a specific folder, you might need to add a drive mapping command to that folder in a login script (container, profile, or user) or create a Storage Location object.

1.3 What's Next

For more information on installing NetStorage, see [Chapter 3, “Installing NetStorage,” on page 15](#).

If you need to provide users with information on how to use NetStorage, see [Chapter 6, “Using NetStorage,” on page 29](#).

After you have installed NetStorage, you can administer settings. See [Chapter 7, “Administering NetStorage,” on page 35](#).

If you need to troubleshoot issues with NetStorage, see [Chapter 8, “Troubleshooting NetStorage,” on page 45](#).

What's New

2

There are no feature changes in this release of NetStorage.

Installing NetStorage

3

NetStorage is automatically installed and preconfigured to default settings during the Open Enterprise Server (OES) portion of the SUSE® Linux Enterprise Server (SLES) 10 installation. OES can be installed with the SLES 10 installation.

For more information, see the *OES2 SP1: Linux Installation Guide*. You can change the NetStorage configuration default settings during the OES portion of the installation. See [Changing the NetStorage Default Configuration](#) below for more information. For most networks, you need NetStorage installed on only one server; however, this might vary depending on the size of your network and your organization's needs. For example, if your company is geographically dispersed, you might want to install NetStorage on one server in each geographic region.

You can use Novell® iManager to change the NetStorage configuration after the OES installation. For more information on iManager, see [Chapter 7, “Administering NetStorage,” on page 35](#).

IMPORTANT: Unsupported Service Combinations: Do not install any of the following service combinations on the same server. Although not all of the combinations will cause pattern conflict warnings, Novell does not support any of the following combinations:

- ♦ Novell NetStorage
 - ♦ Novell Domain Services for Windows
 - ♦ Xen Virtual Machine Host Server
-
- ♦ [Section 3.1, “Requirements,” on page 15](#)
 - ♦ [Section 3.2, “Installing NetStorage After the OES Installation,” on page 16](#)
 - ♦ [Section 3.3, “Changing the NetStorage Default Configuration,” on page 16](#)
 - ♦ [Section 3.4, “Creating Storage Location Objects and Lists,” on page 17](#)
 - ♦ [Section 3.5, “What's Next,” on page 19](#)

3.1 Requirements

In addition to meeting the requirements for OES, NetStorage requires the following:

- ❑ **Server Requirements:** At least one Linux server with OES or one NetWare® 6.5 server in the Novell eDirectory™ tree where NetStorage will be installed.

An eDirectory replica is not required to be on the same server where NetStorage is installed.

IMPORTANT: In order to avoid time issues, this server must have time set correctly according to your network specifications. If time is not set, workstations might not be able to access files.

- ❑ **Workstation Requirements:** Netscape* Navigator* 4.7 or later, Internet Explorer* 5.5 or later, Mozilla*, other Linux browsers, or Microsoft Web Folders.

3.2 Installing NetStorage After the OES Installation

If you did not install NetStorage during the OES installation, you can install it later. To do this, enter `yast2 netstorage` at the Linux server console and then continue with [Step 4 on page 16](#).

3.3 Changing the NetStorage Default Configuration

You can change the NetStorage default configuration during the OES installation.

- 1 Start the SUSE Linux Enterprise Server 10 (SLES 10) installation and continue through the add-on products (OES) part of the install until you get to the Installation Settings screen, then click *Software*.

OES is an add-on product for SLES 10, and can be installed during the SLES 10 installation.

The SLES 10/OES installation includes several steps not described here because they do not directly relate to Novell NetStorage. For more detailed instructions on installing OES with SLES 10, see the [OES2 SP1: Linux Installation Guide](#).

- 2 On the Software Selection screen, click *Detailed Selection*.
- 3 In the Selection window, click *NetStorage* and any other OES components that you want to install, then click *Accept*.
- 4 Select the IP address for the NetStorage Authentication Domain Host, or accept the default.

This is the IP address of a server in your eDirectory tree that has the master replica or a read/write replica of eDirectory.

The eDirectory server IP address is required for NetStorage to function properly. This does not need to be the IP address of the server where NetStorage is to be installed.

When a user attempts to log in, NetStorage searches the eDirectory database on the server you specify for the User object. If the User object is found, NetStorage attempts to authenticate the user to eDirectory.

- 5 Specify the Proxy User Name, including the context, or accept the default.

This is required to perform LDAP searches for logging in.

IMPORTANT: It is not possible to access iFolder 2.x or 3.x by using NetStorage on Linux.

- 6 Specify the Proxy User Password, or accept the default.

- 7 Specify the Users Context, or accept the default.

This is the eDirectory context for the users that will use NetStorage. NetStorage searches the eDirectory tree down from the specified context for User objects. If you want NetStorage to search the entire eDirectory tree, specify the root context.

- 8 (Conditional) If you are running in a clustered environment, install NetStorage on two nodes in the cluster, using the identical configuration used on the first server.

The default configuration for Apache2 on NetWare 6.5 is to listen on all IP addresses. This is done with a Listen directive in `/etc/apache2/listen.conf` that only specifies a port and doesn't have a specific IP address. If you have modified the default configuration to listen on a

specific IP address, and you want the server to be a part of a cluster, you should either remove the specific IP address or add another Listen directive that does not specify an IP address so that Apache2 listens on all IP addresses.

For more information about running NetStorage in a clustered environment, see “[Configuring NetStorage with Novell Cluster Services](#)” in the *Novell Cluster Services Resource Configuration Guide*.

3.4 Creating Storage Location Objects and Lists

After installing NetStorage, you might be able to see only a local shared directory on the Linux server that is using NetStorage. Storage Location objects are required for accessing files and directories on Linux servers unless you have the NCP™ Server component of OES installed. They can also be used on NetWare servers. Without NCP Server, users might have specific eDirectory rights to certain files and folders on your network but cannot access those files and folders through NetStorage unless storage location objects have been created.

- [Section 3.4.1, “SSH Storage Location Objects,” on page 17](#)
- [Section 3.4.2, “Creating a Storage Location Object,” on page 17](#)
- [Section 3.4.3, “Creating a Storage Location List,” on page 19](#)

3.4.1 SSH Storage Location Objects

The SSH file access method is included with NetStorage and allows access to files on Linux systems that don't support either NCP or CIFS protocols. This method uses the Secure Shell (SSH) protocol to access files on Linux systems. SSH is accessed by creating an eDirectory Storage Location object with a URL prefix of `ssh://`. For example:

```
ssh://yourserver.yourcompany.com/home/youruser
```

The username and password that you use to access files on your Linux system must be the same as those used to log in to NetStorage. You can use the SSH file access method with NetStorage to access files locally on your Linux system if NetStorage is running on that system. To do this, create a Storage Location object that uses the IP address of the local Linux machine with the `ssh://` prefix.

IMPORTANT: NetStorage storage location objects defined using the SSH protocol do not function unless SSHD has been enabled for LUM users.

If you want to access local files or files on another server in the same eDirectory tree by using the SSH file access method, you must select the SSHD check box during the OES installation or enable SSHD afterwards by using YaST. The check box is in the Linux User Management configuration section in the OES installation.

3.4.2 Creating a Storage Location Object

- 1 Start your browser (Internet Explorer 5 or later, Mozilla, etc.) and specify the URL for iManager.

The URL is `http://server_ip_address/nps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running NetStorage or the IP address for Apache-based services.

- 2 Enter your username and password.

- 3 In the left column, click *File Access* and then click *New Storage Location*.
- 4 Specify the object name, display name, directory location, context, and a comment.

The object name is the name of the object in the eDirectory tree.

The display name is the name to be displayed in the NetStorage directory access list. This is the shortcut name and is seen by users. If you use the same display name for two different Storage objects, a digit is added to the names to make each name unique.

The directory location is the location of the directory on the file system. The location is a URL that includes the file system type, server name, volume, and directory path.

If the storage being accessed is on a NetWare server, the URL must be in the following format:

```
ncp://server_name/volume/path_to_directory
```

For example:

```
ncp://server1.digitalair.com/mktg/reports
```

or

```
ncp://111.222.3.4/mktg/reports
```

If the storage being accessed is on a Linux server, the URL must be in one of the following formats:

- ♦ `ncp://server_name/volume/path_to_directory`

This method requires that the NCP Server component of OES be installed on your Linux server.

A storage location using this format can only access files on an NCP or NSS volume.

- ♦ `cifs://server_name/cifs_share_name`

This method can be used if you have configured a CIFS or Samba share (cifs can be interchanged with smb in the format).

- ♦ `ssh://yourserver.yourcompany.com/home/youruser`

This method allows access to files on Linux systems that don't support either NCP or CIFS (SMB) protocols.

If the file system is omitted, it is assumed that it is NCP.

The context is the directory context that the Storage Location object resides in. Click the object selector to select the context.

The comment is entered by the administrator and is not displayed to users.

- 5 Click *Create*, then click *OK*.

IMPORTANT: If the IP address of the server that is represented in the eDirectory storage location object is changed, you must update the storage location object with the new IP address. You need not change any configuration files. To modify a storage object, refer to “**Modifying a Storage Location Object**” on page 43.

3.4.3 Creating a Storage Location List

After you create a Storage Location object, you must create a list of Storage Location objects that can be used with a specified User, Group, Profile, or Container object. Users see the directory associated with the object the next time they log in. After this list is created, you can modify it in the same window by assigning additional Storage Location objects to the list or by deleting Storage Location objects from the list.

- 1 Start your browser (Internet Explorer 5 or later, Mozilla, etc.) and specify the URL for iManager.
The URL is `http://server_ip_address/nps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running NetStorage or the IP address for Apache-based services.
- 2 Enter your username and password.
- 3 In the left column, click *File Access*, then click *Assign Storage Location* to Object.
- 4 Click the *Object Selector* button; select the User, Group, Profile, or Container object that the list is to be created for; then click *OK*.
- 5 Click the *Object Selector* button, select the Storage Location objects you want included in this list, then click *OK*.
You can select multiple Storage Location objects in the Object Selector window. When you select multiple Storage Location objects, they appear in the *Selected Objects* list. If the list already contains Storage Location objects and you want to add more, ensure that the original objects are still in the list before clicking *OK*.
- 6 (Optional) Remove existing storage locations by deleting their names from the list.
- 7 When you are finished creating or modifying the list, click *OK*.

3.5 What's Next

After you have installed NetStorage, inform users that they can access their files from the Web. Instructions for accessing files through NetStorage are available in [Chapter 6, “Using NetStorage,” on page 29](#).

If you need to change the NetStorage configuration, use iManager. See [Chapter 7, “Administering NetStorage,” on page 35](#).

Configuring NetStorage with Novell Cluster Services

4

NetStorage provides secure Internet-based access to files and folders on a Novell® Open Enterprise Server (OES) 2 Linux server on your network, using either a browser or Microsoft Web Folders (Microsoft's implementation of WebDAV). If the OES 2 Linux server running NetStorage goes down, Internet-based access to files and folders is not possible. Configuring NetStorage with Novell Cluster Services™ helps ensure that Internet-based access to files and folders can continue even if a server running NetStorage goes down.

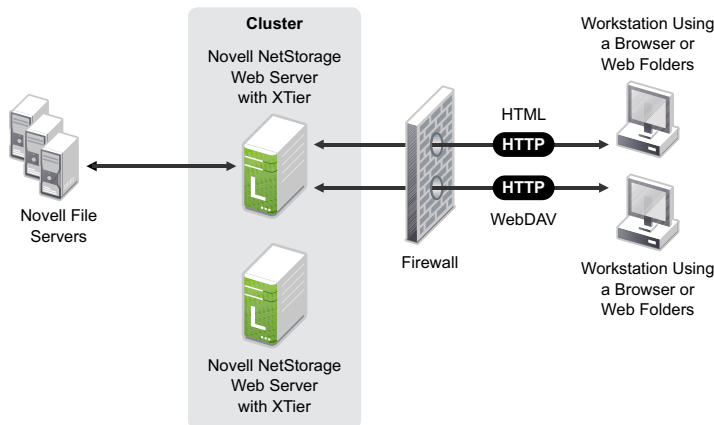
- ♦ [Section 4.1, “NetStorage Installation and Configuration,” on page 21](#)
- ♦ [Section 4.2, “Novell Cluster Services Configuration and Setup,” on page 22](#)

4.1 NetStorage Installation and Configuration

Novell NetStorage software is included with OES 2 Linux and can be installed during the OES 2 Linux add-on installation. You must select the Novell NetStorage component check box to install NetStorage. Because NetStorage requires iManager and Apache*, you must also select the Apache Web server and iManager check boxes. See [Chapter 3, “Installing NetStorage,” on page 15](#) for more information on installing and configuring NetStorage.

Because most networks require NetStorage to be installed on only one server, it is generally only necessary to install NetStorage on two servers in the cluster. Users gain access to files and folders by connecting to one NetStorage server. The other NetStorage server acts as a backup in case the first NetStorage server fails. The following figure shows how a typical NetStorage cluster configuration might look.

Figure 4-1 Cluster Configuration for NetStorage on Linux



When you install NetStorage with OES 2 Linux, you are asked to specify the DNS name or IP address of the Primary eDirectory Server. This is the IP address or registered DNS name of a server in your eDirectory tree that has the master replica or a read/write replica of eDirectory. For NetStorage to function properly in a cluster, you must specify same DNS name or IP address of the primary eDirectory Server on all servers in the cluster that have NetStorage installed.

Any NetStorage-specific configuration changes made to one NetStorage server must be made on all other NetStorage servers in the cluster. In order for NetStorage to function properly with Novell Cluster Services, all NetStorage servers in the cluster must be identically configured.

4.2 Novell Cluster Services Configuration and Setup

- [Section 4.2.1, “Prerequisites,” on page 22](#)
- [Section 4.2.2, “Creating a NetStorage Cluster Resource,” on page 22](#)
- [Section 4.2.3, “Editing NetStorage Load and Unload Scripts,” on page 23](#)
- [Section 4.2.4, “Setting the NetStorage Resource Start, Failover, and Failback Modes,” on page 24](#)
- [Section 4.2.5, “View or Edit NetStorage Resource Server Assignments,” on page 25](#)
- [Section 4.2.6, “Accessing NetStorage After Cluster Configuration,” on page 26](#)

4.2.1 Prerequisites

Novell Cluster Services must be installed and running on the servers that have NetStorage installed before performing the remainder of the NetStorage and Novell Cluster Services configuration. For information, see “[Installing Novell Cluster Services on OES 2 Linux](#)” in the *OES 2 SP1: Novell Cluster Services 1.8.5 for Linux Administration Guide*.

IMPORTANT: Because NetStorage is installed and configured identically on the cluster servers where it will run and because that configuration information is stored on each server, no shared storage is required to run NetStorage with Novell Cluster Services.

4.2.2 Creating a NetStorage Cluster Resource

A cluster resource containing a secondary IP address is necessary to ensure that users continue to have access to NetStorage if a server running NetStorage goes down.

Novell Cluster Services includes a Generic IP Service resource template, which simplifies the process for creating a NetStorage cluster resource.

- 1 Start your Internet browser and enter the URL for iManager.
The URL is `http://server_ip_address/nps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of a server in the cluster or with the IP address for Apache-based services.
- 2 Enter your username and password.
- 3 In the left column, click *Clusters*, then click the *Cluster Options* link.
iManager displays four links under *Clusters* that you can use to configure and manage your cluster.
- 4 Browse to locate and select the Cluster object of the cluster you want to manage, then click the *New* link.
- 5 Specify Resource as the resource type you want to create by clicking the *Resource* radio button, then click *Next*.

- 6 Specify a name for the NetStorage cluster resource that you want to create.
Do not use periods in cluster resource names. Novell clients interpret periods as delimiters. If you use a space in a cluster resource name, that space is converted to an underscore.
- 7 In the *Inherit From Template* field, select the *Generic_IP_Service* template.
- 8 Select the *Define Additional Properties* check box, then click *Next*.
- 9 Select the *Define Additional Properties* check box, click *Create*, and then continue with [Section 4.2.3, “Editing NetStorage Load and Unload Scripts,” on page 23](#).
The Generic IP Service template helps configure the NetStorage cluster resource by automatically creating load and unload scripts, setting failover and failback modes, and assigning the resource to all nodes in the cluster.
You should only assign the resource to those nodes in the cluster that have NetStorage installed and running.

4.2.3 Editing NetStorage Load and Unload Scripts

The Generic IP Service resource template automatically creates load and unload scripts to start and stop the NetStorage resource on servers in your cluster. The load script contains commands that you must customize for your specific NetStorage configuration.

If you are creating a new cluster resource, the load script page should already be displayed. You can start with [Step 5](#).

- 1 In iManager, click *Clusters*, then click *Cluster Options*.
- 2 Browse to locate and select the Cluster object of the cluster you want to manage.
- 3 Select the check box next to the resource whose load script you want to edit, then click the *Details* link.
- 4 Click the *Scripts* tab, then click the *Load Script* link.
The load script includes instructions and commands, all of which should currently be commented out with the # symbol.
- 5 Edit the NetStorage load script.
 - 5a Uncomment the following line by removing the # symbol:

```
#add secondary ipaddress A.B.C.D
```
 - 5b Replace A.B.C.D with the IP address you want to assign to the NetStorage resource.
For example, if the IP address for the NetStorage cluster resource is 192.168.1.10, the line in the load script would now appear as follows:

```
add secondary ipaddress 192.168.1.10
```


Clients can now use the NetStorage cluster resource IP address as part of the URL to access NetStorage instead of the NetStorage server's IP address or DNS name.
 - 5c Specify the *Load Script Timeout* value, then click *Apply* to save the script or, if you are creating a new cluster resource, click *Next*.
The timeout value determines how much time the script is given to complete. If the script does not complete within the specified time, the resource becomes comatose.
- 6 Edit the NetStorage unload script.
 - 6a Click *Unload Script* on the *Scripts* tab on the property page to edit the unload script.

If you are creating a new cluster resource, the unload script page should already be displayed. The unload script includes instructions and commands, all of which should currently be commented out with the # symbol.

6b Uncomment the following line by removing the # symbol:

```
#del secondary ipaddress A.B.C.D
```

6c Replace A.B.C.D with the IP address you want to assigned to the NetStorage resource in [Step 5b](#).

For example, if the IP address for the NetStorage cluster resource is 192.168.1.10, the line in the unload script would now appear as follows:

```
del secondary ipaddress 192.168.1.10
```

7 Continue with [Section 4.2.4, “Setting the NetStorage Resource Start, Failover, and Failback Modes,”](#) on page 24.

4.2.4 Setting the NetStorage Resource Start, Failover, and Failback Modes

A cluster resource cannot be edited while it is loaded or running on a server. Make sure to offline the resource before attempting to modify its resource properties, policies, or scripts.

The Generic IP Service resource template sets the NetStorage resource Start Mode and Failover Mode to AUTO, and the Failback Mode to DISABLE.

If the NetStorage resource Start Mode is set to AUTO, the resource automatically starts on a designated server when the cluster is first brought up (the secondary IP address specified in the resource is automatically added to the server). If the NetStorage resource Start Mode is set to MANUAL, you can manually start the resource on a specific server when you want, instead of having it automatically start when servers in the cluster are brought up.

If the NetStorage resource Failover Mode is set to AUTO, the NetStorage resource automatically moves to the next server in the Assigned Nodes list in the event of a hardware or software failure. If the NetStorage resource Failover Mode is set to MANUAL, you can intervene after a failure occurs and before the resource is started on another node.

If the NetStorage resource Failback Mode is set to DISABLE, the resource continues running on the node it has failed to. If the NetStorage resource Failback Mode is set to AUTO, the resource automatically moves back to its preferred node when the preferred node is brought back online. Set the NetStorage resource Failback Mode to MANUAL to prevent the resource from moving back to its preferred node when that node is brought back online, until you are ready to allow it to happen.

The preferred node is the first server in the Assigned Nodes list for the resource.

IMPORTANT: Resources fail back only to the first node in their Assigned Nodes list. For example, if a resource has failed over to three servers since it originally ran on its preferred node, and the second server the resource was running on comes back up, the resource does not fail back to that second server.

Resources do not automatically move from node to node just because a node higher in the Assigned Nodes list rejoins the cluster, unless the Failback mode is set to AUTO and the first node in the Assigned Nodes list rejoins the cluster.

If you are creating a new cluster resource, the Resource Policies page should already be displayed. You can start with [Step 5](#).

- 1 In iManager, click *Clusters*, then click *Cluster Options*.
- 2 Browse to locate and select the Cluster object of the cluster you want to manage.
- 3 Select the box next to the resource whose *Start*, *Failover*, or *Failback* modes you want to view or edit, then click the *Details* link.
- 4 Click the *Policies* tab.
- 5 (Conditional) Select the *Resource Follows Master* check box if you want to ensure that the resource runs only on the master node in the cluster.
If the master node in the cluster fails, the resource fails over to whichever node becomes the master.
- 6 (Conditional) Select the *Ignore Quorum* check box if you don't want the cluster-wide timeout period and node number limit enforced.
The quorum default values were set when you installed Novell Cluster Services. You can change the quorum default values by accessing the properties page for the Cluster object.
Selecting this box ensures that the resource is launched immediately on any server in the Assigned Nodes list as soon as any server in the list is brought online.
- 7 Specify the *Start*, *Failover*, and *Failback* modes for this resource.
The default for both *Start* and *Failover* modes is AUTO, and the default for *Failback* mode is DISABLE.
- 8 Continue with [“View or Edit NetStorage Resource Server Assignments” on page 25](#), or if you are creating a new cluster resource, click *Next*, then continue with [“Configuring NetStorage with Novell Cluster Services” on page 21](#).

4.2.5 View or Edit NetStorage Resource Server Assignments

A cluster resource cannot be edited while it is loaded or running on a server. Make sure to offline the resource before attempting to modify its resource properties, policies, or scripts.

The Generic IP Service resource template automatically assigns the NetStorage resource to all nodes in the cluster. The order of assignment is the order the nodes appear in the resource list. You should assign the NetStorage resource only to those servers in the cluster that have NetStorage installed.

If you are creating a new cluster resource, the Preferred Nodes page should already be displayed. If you are assigning nodes for an existing resource, the Preferred Nodes page is displayed as part of the Resource Policies page. You can start with [Step 5](#).

- 1 In iManager, click *Clusters*, then click *Cluster Options*.
- 2 Browse to locate and select the Cluster object of the cluster you want to manage.
- 3 Select the box next to the resource whose preferred node list you want to view or edit, then click the *Details* link.
- 4 Click the *Preferred Nodes* tab.
- 5 View the current NetStorage resource server assignments and, if necessary, click the right-arrow or left-arrow button to assign or unassign servers to the resource.
The *Assigned Nodes* list should contain only servers where you have installed and configured NetStorage.

- 6 View the order of the NetStorage resource server assignments and, if necessary, click the up-arrow and down-arrow buttons to change the preferred failover order of the servers assigned to the resource or volume.
- 7 Click *Apply* to save node assignment changes.

4.2.6 Accessing NetStorage After Cluster Configuration

To access NetStorage after configuring it with Novell Cluster Services, use the NetStorage cluster resource IP address as part of the URL to access NetStorage instead of the NetStorage server's IP address or DNS name. For more information on accessing NetStorage, see [Chapter 6, "Using NetStorage," on page 29](#).

Running NetStorage in a Virtualized Environment

5

NetStorage runs in a virtualized environment just as it does on a physical NetWare[®] server, or on a physical server running Open Enterprise Server (OES) 2 Linux, and requires no special configuration or other changes.

To get started with virtualization, see *SUSE Linux Enterprise Server 10 SP2: Virtualization with Xen* (http://www.novell.com/documentation/sles10/xen_admin/data/bookinfo.html)

For information on setting up OES 2 Linux on a Xen*-based virtual guest server, see “**Installing, Upgrading, or Updating OES 2 SP1 Linux on a Xen-based Virtual Machine**” in the *OES2 SP1: Linux Installation Guide*.

Using NetStorage

6

NetStorage provides secure Internet-based access to files and folders on Linux and NetWare[®] servers on your network, using either a browser or Microsoft Web Folders (Microsoft's implementation of WebDAV). NetStorage authentication relies on the power of Novell[®] eDirectory[™] to provide secure access, so Internet-based access is as secure as accessing files from within the network.

Based on how NetStorage has been configured, the NetStorage Web page displays the network files and folders you have access to. Initially, you might be able to see only a local shared directory and NSS volumes on the Linux server. Storage Location objects are required for accessing files and directories on Linux servers unless the NCP Server component of OES is installed. They can also be used on NetWare servers. For Linux servers with NCP Server installed, NetStorage reads your login script to determine drive mappings, reads eDirectory User object properties to determine your home directory, and then displays a list of files and folders based on mapped drives and home directories. If you usually log in to more than one eDirectory tree, you might have access to additional home directories in different eDirectory trees.

NetStorage reads the container, profile, and user login scripts only from the primary eDirectory server specified during the installation, and displays the user's drive mappings based on those login scripts.

Users might have specific eDirectory rights to certain files and folders on your network, but cannot access those files and folders through NetStorage unless Storage Location objects have been created, login script drive mappings exist to those folders, or the files and folders are in the user's home directory. If you want to provide users with NetStorage access to a specific folder, you might need to add a drive mapping command to that folder in a login script (container, profile, or user).

- ♦ [Section 6.1, “Accessing NetStorage,” on page 29](#)
- ♦ [Section 6.2, “Viewing or Modifying Directory and File Attributes and Rights,” on page 30](#)
- ♦ [Section 6.3, “Accessing Archived Files,” on page 31](#)
- ♦ [Section 6.4, “Setting Directory Quotas on NSS Volumes and Directories,” on page 32](#)
- ♦ [Section 6.5, “Purging and Salvaging Deleted NSS Files,” on page 33](#)

6.1 Accessing NetStorage

To access NetStorage from a workstation:

- 1 Start your browser or Microsoft Web Folders, then specify the URL for NetStorage.

The URL is `http://server_ip_address/oneNet/NetStorage/`. Replace *server_ip_address* with the IP address or DNS name of the server running NetStorage or the IP address for Apache-based services. If Apache-based services use a port other than 80, you must also specify that port number with the URL.

For example, if the IP address for NetStorage is 127.1.1.1, then you would specify `127.1.1.1/oneNet/NetStorage/`.

In the above example, if you had changed the port number to 51080, then you would specify `127.1.1.1:51080/oneNet/NetStorage/`.

Although the oneNet portion of the URL is required if you are using WebDAV (Web Folders), it is not required if you are using a browser. In a browser, you can use 127.1.1.1/NetStorage/.

If you have the Persistent Cookies feature enabled (See [Section 7.2.6, “NetStorage Options,” on page 40](#)), the date and time on the workstation being used to access NetStorage should be within 24 hours of the date and time on the server running NetStorage in order to avoid conflicts.

2 Enter your username and password.

NetStorage uses your Novell eDirectory username and password, so you don't need to remember or use a separate username or password.

You can use many of the same conventions for expanding and contracting folders and opening files that are available in Windows* Explorer. To create new folders or to copy, paste, delete, rename, move, upload, or download existing files with a browser, click the *File* menu. If you are using Internet Explorer, you can copy and move files and folders by dragging and dropping them. This functionality is not available with browsers other than Internet Explorer.

Clicking the *Folder View* button in the browser window displays folders in another column and lets you expand and contract folders. The Text View displays only the files and folders in the current directory and does not let you expand or contract folders. Clicking the *Name*, *Size*, or *Modified* headings lets you sort directory and file listings in ascending or descending order by name, size, or date.

Local files and folders in a shared directory on the Linux server where NetStorage is installed can be accessed through NetStorage. This is useful for uploading files to the local Linux server. The path to the shared folder is `/var/opt/novell/NetStorage/shared`.

You cannot map drives or change login scripts from NetStorage.

NetStorage lets you upload and download multiple files and folders simultaneously.

6.2 Viewing or Modifying Directory and File Attributes and Rights

NetStorage provides the ability to view or change NSS and NCP™ directory and file attributes and rights. If you have created a Storage Location object by using NCP, the ability to change file and directory attributes is limited unless you are logged in as user Admin or equivalent. This limitation does not apply if you have created a Storage Location object by using SSH. See [“Creating a Storage Location Object” on page 42](#) for more information.

To view or modify directory or file rights by using NetStorage:

1 Start your browser and specify the URL for NetStorage.

The URL is `http://server_ip_address/oneNet/NetStorage/`. Replace *server_ip_address* with the IP address or DNS name of the server running NetStorage or the IP address for Apache-based services. If Apache-based services use a port other than 80, you must also specify that port number with the URL.

For example, if the IP address for NetStorage is 127.1.1.1, then you would specify `127.1.1.1/oneNet/NetStorage/`.

In the above example, if you had changed the port number to 51080, then you would specify `127.1.1.1:51080/oneNet/NetStorage/`.

Although the oneNet portion of the URL is required if you are using WebDAV (Web Folders), it is not required if you are using a browser. In a browser, you can use 127.1.1.1/NetStorage/.

The date and time on the workstation being used to access NetStorage should be (within a few hours) of the date and time on the server running NetStorage to avoid conflicts.

- 2 Enter your username and password.

NetStorage uses your Novell eDirectory username and password, so you don't need to remember or use a separate username or password.

- 3 Right-click the directory or file you want to view or modify attributes or rights for and select *Properties*.

- 4 Click the *NetWare Info* tab to view or modify directory or file attributes. Click the *NetWare Rights* tab to view or modify file system trustee rights.

Although the option label refers to NetWare, use the option for your Linux NSS and non-NSS volumes, and your NetWare NSS volumes. For information about file system trustees, trustee rights, and attributes for directories and files on NSS volumes, see the *OES 2 SP1: NSS File System Administration Guide*.

For additional information on directory and file attributes and rights, see the *Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide*.

NOTE: Viewing or changing directory and file attributes and rights through NetStorage is only possible with a browser. This functionality is not available through Microsoft Web Folders.

6.3 Accessing Archived Files

Novell Archive and Version Services provides a convenient and cost-effective way for you to instantly restore previous versions of your modified, deleted, or lost files.

IMPORTANT: You can use NetStorage to access previous versions of archived files, but NetStorage cannot be used to restore archived deleted directories. You must use the NSS File Version Utility to restore archived directories that have been deleted. You can access file versions from anywhere, at any time, using a Web browser and an active network without the help of your administrator.

For information on accessing and restoring archived file versions, see the *OES 2 SP1: Novell Archive and Version Services 2.1 User Guide*.

6.3.1 What Files Are Versioned

Your administrator sets criteria to determine which files are eligible for versioning. Files can be included or excluded according to the path, file extension, or filename patterns. If your files meet the inclusion criteria, they are eligible for versioning.

Versioning occurs for eligible files at scheduled intervals, called epochs. It does not matter how many changes users make to a file during an epoch; only those files that exist at the end of the epoch are saved. If a user creates and deletes a file within the epoch, it cannot be versioned. This means that a file's lifetime must span to the end of an epoch to be versioned.

Versioned files might have a limited life in the archive, depending on the delete policies your administrator sets. The administrator sets the maximum keep time and the maximum number of versions to retain. The delete policy for some volumes can allow indefinite retention of versioned files.

For information about the versioning policies for your files, contact your Archive and Version Services administrator.

6.3.2 Accessing File Versions

You can access previous versions of your files whenever you need to by using the NetStorage interface.

- 1 Log in to NetStorage.
- 2 Select a file or directory that you want to see previous versions of.
- 3 Right-click to open the pop-up menu.
- 4 Click *Archive*.

To restore a previous version of the file:

- 1 Navigate through the Archive dialog boxes to find the file you want to see previous versions of.
- 2 Review the time stamps of the file versions, then select the version of the file that you want to restore.
- 3 In the *Restore To* field, type the path and filename where you want to restore the version, or browse to that location, type a filename, then click *OK*.
- 4 Click *Restore*.

WARNING: The restored version overwrites any file by that name in the Restore To location.

6.4 Setting Directory Quotas on NSS Volumes and Directories

You can use NetStorage to create or change directory quotas on NSS volumes and directories for both NetWare and Linux. See “[Managing Space Quotas for Volumes, Directories, and Users](#)” in the *OES 2 SP1: NSS File System Administration Guide*. You must be a user with rights equivalent to the Admin user to create or change directory quotas.

- 1 Start your browser and specify the URL for NetStorage.

The URL is `http://server_ip_address/oneNet/NetStorage/`. Replace *server_ip_address* with the IP address or DNS name of the server running NetStorage or the IP address for Apache-based services. If Apache-based services use a port other than 80, you must also specify that port number with the URL.

For example, if the IP address for NetStorage is 127.1.1.1, then you would specify `127.1.1.1/oneNet/NetStorage/`.

In the above example, if you had changed the port number to 51080, then you would specify `127.1.1.1:51080/oneNet/NetStorage/`.

Although the oneNet portion of the URL is required if you are using WebDAV (Web Folders), it is not required if using a browser. In a browser, you can just use `127.1.1.1/NetStorage/`.

The date and time on the workstation being used to access NetStorage should be within a few hours of the date and time on the server running NetStorage to avoid conflicts.

- 2 Enter your username and password.

NetStorage uses your Novell eDirectory username and password, so you don't need to remember or use a separate username or password.

- 3 Right-click the directory or file you want to create or change a directory quota for and select *Properties*.
- 4 Click the *NetWare Info* tab, then click the *Restrict size* check box.
- 5 Specify the directory size limit and click *Apply* to save your changes.

6.5 Purging and Salvaging Deleted NSS Files

Using NetStorage, you can purge and possibly undelete NSS files that were previously deleted if either of the following is true:

- ♦ You are user Admin and have the NCP Server component of OES installed on the Linux server.
- ♦ You have a Storage Location object set up to the directory where the deleted files or folders were.

IMPORTANT: Users must be LUM-enabled in order to undelete and purge deleted files from Linux NSS volumes.

- 1 Access NetStorage and, in the left column, select the directory where the deleted files were.
- 2 Click *View* and then *Show Deleted Files*.
- 3 Select the boxes next to the files you want to undelete or purge.
- 4 Click *File*, then click either *Purge* or *Undelete*.

Administering NetStorage

7

You can use Novell® iManager to change your NetStorage configuration after NetStorage has been installed on a Linux server (known as the Middle Tier or XTier server). NetStorage configuration information is stored in an XML file on the Linux server and iManager provides an easy method for changing NetStorage configuration. iManager requires Internet Explorer 5 or later.

If you are running in a clustered environment, any registry changes made to one node in the cluster must be made to the registry of each node in the cluster. After you have made a change to one node, run iManager on each node in the cluster and make the same changes. For more information about running NetStorage in a clustered environment, see “[Configuring NetStorage with Novell Cluster Services](#)” in the *Novell Cluster Services Resource Configuration Guide*.

After changing any settings in the iManager console, run `rcnovell-xsrvc restart` at the command prompt to implement the changes to NetStorage. We recommend you to also restart the apache and tomcat services by executing the following commands:

```
/etc/init.d/novell-tomcat5 stop
/etc/init.d/apache2 stop
/etc/init.d/novell-tomcat5 start
/etc/init.d/apache2 start
```

7.1 Using iManager to Administer NetStorage

- 1 Open an Internet browser and enter the URL for iManager.

The URL is `https://server_ip_address/nps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running NetStorage or the IP address for Apache-based services.

The date and time on the workstation being used to access NetStorage should be within a few hours of the date and time on the server running NetStorage to avoid conflicts.

- 2 Enter your username and password.
- 3 In the left column, locate the *File Access (NetStorage)* configuration options you want to change.

iManager displays a list of links in the left column that are used to access the various pages for editing and viewing NetStorage configuration information in the XML file. For more information on each setting, click *Help* or see [Section 7.2, “Understanding the NetStorage Configuration Settings,”](#) on page 36.

- 4 Make the necessary configuration changes.
- 5 (Conditional) If you are running in a clustered environment, run iManager on each node in the cluster and make the same changes.

For more information about running NetStorage in a clustered environment, see “[Configuring NetStorage with Novell Cluster Services](#)” in the *Novell Cluster Services Resource Configuration Guide*.

7.2 Understanding the NetStorage Configuration Settings

This section includes information on all configuration settings that can be set. The settings are organized according to the link in the left column where they appear. This information is also available if you click *Help*.

Most configuration settings have a *Set Defaults* button. If you click the *Set Defaults* button, the value is set to whatever value appears in the *Default Value* column. If there is no value in the *Default Value* column, the value is set to blank (no value).

- ♦ [Authentication Domains \(page 36\)](#)
- ♦ [“Current Sessions” on page 38](#)
- ♦ [“Files” on page 38](#)
- ♦ [“iFolder Storage Provider” on page 38](#)
- ♦ [“NetWare Storage Provider” on page 38](#)
- ♦ [“NetStorage Options” on page 40](#)
- ♦ [“NetStorage Statistics” on page 41](#)
- ♦ [“Resource Usage” on page 41](#)
- ♦ [“WebDAV Provider” on page 41](#)
- ♦ [“Storage Location” on page 41](#)

7.2.1 Authentication Domains

Lets you change or add the Novell eDirectory™ server URLs and contexts that are required by NetStorage. It also lets you add support for dotted usernames, e-mail address names, and universal passwords, as well as giving you the option to change the eDirectory server that is designated as the Primary.

Table 7-1 *Authentication Domain Setting and Description*

Setting	Description
Dotted Names	<p>Allows the use of a dot in a username. Some usernames contain dots (for example: john.doe). Enabling this option allows usernames containing dots to authenticate through NetStorage.</p> <p>If this option is disabled, usernames containing dots can still authenticate through NetStorage by adding a forward slash (/) in front of the dot in the username (for example: john/.doe).</p>
eMail Address Names	<p>Allows the use of the At symbol (@) in a username. Some usernames are e-mail address names and contain the At symbol. Enabling this option allows usernames containing this character to authenticate through NetStorage. If this option is disabled, NetStorage reads the username up to the At symbol and then tries to authenticate with that much of the name.</p>

Setting	Description
Universal Password	<p>Allows universal passwords to be used for NetStorage Authentication.</p> <p>Universal password functionality is disabled by default. If you have enabled universal passwords, enable this option to let users with universal passwords authenticate through NetStorage.</p> <p>If universal passwords have not been configured and enabled, selecting this option has no effect. NetStorage uses whatever password type is configured.</p> <p>See Deploying Universal Passwords (http://www.novell.com/documentation/nmas23/index.html?page=/documentation/nmas23/admin/data/allq21t.html) for information on configuring universal passwords.</p>
Add Domain	Adds another eDirectory server IP address or DNS name. Users are authenticated to this eDirectory server.
Make Primary	Makes the eDirectory server URL listed above the button the Primary.
Remove Domain	Removes the eDirectory server URL from the list of URLs used by NetStorage.
Add Context	<p>Adds a context that NetStorage searches when authenticating users. Use periods to separate the context. For example, ou=users.o=digitalair.</p> <p>If the user is not located in the first context, any additional contexts added here are searched. If the user is not found in any context listed, an LDAP search of all subdirectories is performed.</p> <p>If clear-text passwords are not enabled on the server, this search fails.</p>
Remove Context	Removes the context (if there is one) from the eDirectory server URL.
Add Host	<p>Lets you list additional hosts for an Authentication Domain. Clicking the <i>Add Hosts</i> button lets you create a list of alternative hosts for the domain.</p> <p>If the Middle Tier server cannot reach the host specified in the domain, it searches the <i>Other Hosts</i> list specified in the <i>Value</i> field to find another server to use for authentication. Specify DNS names or IP addresses of alternate servers, separated by a comma delimiter, in the <i>Value</i> field.</p> <p>For example, you could enter a string similar to either of the following:</p> <p>Middletier.boston.digitalair.com,Middletier1.boston.digitalair.com</p> <p>or</p> <p>111.22.33.4,111.22.33.41</p>
Context Priority	<p>Lets you specify a priority for the context assigned to the eDirectory server URL. Adding a context priority lets you specify the order you want the different contexts searched.</p> <p>If no context priority is specified, the default priority is used, which is 0. The priority range is from 0 (lowest) to 9999999.</p>

7.2.2 Current Sessions

Displays a report with information on the current NetStorage sessions.

7.2.3 Files

Displays the NetStorage Web page. This provides a way to access NetStorage from iManager, without entering the NetStorage URL. See [Chapter 6, “Using NetStorage,” on page 29](#) for more information on the NetStorage Web page.

7.2.4 iFolder Storage Provider

This option is not functional on OES Linux. However, it does function on OES NetWare®.

7.2.5 NetWare Storage Provider

NOTE: The name fields should not contain any special characters that are misinterpreted as separators in any type of path or URL string. The characters includes /, :, and \.

Table 7-2 *NetWare Storage Provider Settings and Description*

Settings	Description
Home Name	<p>This text is displayed on the NetStorage Web page and is followed by the tree name and path to the user's home directory. The user might have home directories in multiple trees, in which case multiple paths are displayed.</p> <p>The default is Home@. You might want to change this if you want to reference home directories with a different word or in a language other than English. See the Alternate Tree Name listing below for more information on configuring NetStorage to display multiple home directories.</p>
Drive Name	<p>This text is displayed on the NetStorage Web page and includes the drive letter being referenced, followed by the path to the mapped drive. The user's login script on the Primary tree is parsed by NetStorage to gather information on mapped drives.</p> <p>You might want to change this if you want to use a different word or words to reference mapped drives on the NetStorage Web page. This applies to NetStorage on NetWare servers only.</p>

Settings	Description
Public Directory Name	<p>This registry key provides a way for any NetStorage user to make documents or files available to other NetStorage users.</p> <p>A public directory can be automatically created in each user's home directory by NetStorage. If public directories are created by NetStorage, all users in the same eDirectory context have Read and File Scan rights to the other users' public directories.</p> <p>If you don't want public directories created in users' home directories, leave this field blank (the default).</p> <p>If you want public directories created in users' home directories, specify the name for the public directories. For example, if you specify My Public Files as the name for the public directories, a folder named My Public Files is created at the root of each user's home directory the first time the user logs in through NetStorage.</p> <p>To access a public directory, users need to add <code>~username</code> at the end of the URL used to access NetStorage. For example if you want to access the public directory for a user named jsmith, you might specify a URL similar to <code>http://file.i-login.net/oneNet/NetStorage/~jsmith</code>.</p>
Alternate Tree Name	<p>When a user's home directory is displayed by NetStorage, the name of the eDirectory tree is also displayed. With this configuration field, you can change the tree name that users see in NetStorage to something that might be more intuitive. For example, if the tree name is SERVICES 2 and you want users to see i-Login, you would type <code>SERVICES2/i-Login</code> in this configuration field. The eDirectory tree name and the substitute name are separated with a slash (/).</p> <p>NetStorage can access user home directories in multiple eDirectory trees. If you want to substitute eDirectory tree names in more than one tree, separate those tree name substitutions with a comma. An example of this is <code>SERVICES2/i-Login,SERVEME2/Staging</code>.</p>
Container Search Height	<p>Specifies the number of container levels (from where the User object is located) that NetStorage searches up the eDirectory tree for the container login script. The default is 1, which is the same level used by Novell Client™ software.</p> <p>If you specify a number greater than the number of container levels in the eDirectory tree, NetStorage searches up to and including the root container in the tree. If you specify 0, NetStorage only searches the container where the User object is located.</p>
Home Dirs	<p>Specifies if home directories are to be processed. The default is 1, meaning that they are processed. If you specify 0, no home directories are processed or displayed to the user.</p>
Check MAP Drives	<p>Specifies if mapped drives (from login script MAP statements) are checked when the user logs in. The default is 0, meaning that mapped drives are not checked and all mapped drives are displayed to the user. If the user attempts to access a mapped drive pointing to a directory that does not exist or that the user does not have access rights to, an error occurs.</p> <p>If you specify 1, each mapped drive is checked at login and map drives that do not exist or that the user does not have access to are not displayed.</p>
LoginScripts	<p>Specifies if login scripts are to be processed. The default is 1, meaning that they are processed. If you specify 0, no login scripts are processed, so no user object details associated with them are displayed.</p>

Settings	Description
Storage Locations	Specifies if storage locations are to be processed. The default is 1, meaning that they are processed. If you specify 0, no storage locations are processed, or displayed to the user.
Shared Directory	Specifies if shared directories are to be processed. The default is 1, meaning that they are processed. If you specify 0, no shared directories are processed or displayed to the user.

7.2.6 NetStorage Options

Table 7-3 *NetStorage Settings and Description Options*

Settings	Description
Proxy Username and Proxy Password	<p>The Admin username and password that you entered when you installed NNLS. If you want the Middle Tier Server to use a different username and password for administrator access, specify them in the fields provided.</p> <p>If you click the <i>Set Defaults</i> button, the value is set to whatever value appears in the <i>Default Value</i> column. If there is no value in the <i>Default Value</i> column, the value is set to blank (no value).</p>
Location	<p>The registered location you want users to enter as part of the NetStorage URL to access NetStorage. The default is oneNet.</p> <p>If you change this registry setting, you must also edit the <code>etc/opt/novell/xtier/xsrv.conf</code> file and change the <code>/oneNet</code> setting in the <code>Location</code> section (first section) to the same setting you specified in iManager.</p>
Session Timeout	The amount of time (in seconds) that the session remains idle before it is terminated. If there is no NetStorage activity for this amount of time, the user is required to log in again to NetStorage before being allowed file access.
Janitorial Interval	This setting should not be changed except under direction from Novell.
Persistent Cookies	<p>This setting can be turned on or off. Persistent Cookies is turned off (the default) if there is no value or if the value is set to 0. You can turn Persistent Cookies on by changing the value to 1.</p> <p>With Persistent Cookies turned off, the NetStorage session ends when the user closes the current browser or Web folder. Also, if the user has a current instance of NetStorage running in a browser window or Web folder and starts up a new browser instance or Web folder, the user is required to reauthenticate.</p> <p>Turning off Persistent Cookies can be beneficial if you have workstations that are shared, because as long as the browser instance is closed, the next user of the workstation cannot accidentally or intentionally obtain access to your network through NetStorage.</p> <p>Leaving Persistent Cookies turned on can be beneficial if your workstations are not shared, because users are not required to unnecessarily reauthenticate.</p> <p>If the user selects the <i>Logout</i> option in NetStorage, the session ends regardless of whether Persistent Cookies is turned on or off.</p>

Settings	Description
LDAP Port	<p>Lets you change the LDAP port number if there is a conflict between Active Directory* and eDirectory for LDAP requests.</p> <p>This conflict exists because the back end is acting as a domain controller, which has Active Directory installed on it. The conflict is created by both eDirectory and Active Directory attempting to use the same default port (number 389). Active Directory normally wins the conflict. The Proxy User object type exists in eDirectory but not in Active Directory. Because of this, when the Middle Tier server tries to bind as a Proxy User, the bind attempt fails. This is also the reason LDAP lookups fail.</p>
Cookieless	<p>The Cookieless option can be turned either on or off. With the value set to 0, Cookieless authentication is turned off (the default). Cookieless authentication can be turned on by setting the value to 1.</p> <p>Cookieless authentication is needed for some clients that use versions of WebDav that don't support cookies. For example, Apple* clients use a WebDav version that does not support cookies.</p> <p>If Cookieless authentication is turned on, you must close all browser instances to log out.</p>

7.2.7 NetStorage Statistics

Displays a report with information about server up time, login failures, number of NetStorage sessions, etc.

7.2.8 Resource Usage

Displays a detailed report of resource utilization for NetStorage.

7.2.9 WebDAV Provider

Table 7-4 *WebDAV Provider Settings and Description*

Settings	Description
Moniker	The location of the NetStorage WebDAV provider (<code>xdav.nlm</code>). It is the location you want users to specify as part of the NetStorage URL to access NetStorage. The default is NetStorage.
Template Directory	The directory for the HTML interface. This setting should not be changed except under direction from Novell.

7.2.10 Storage Location

You can create a Storage Location object to display a specified name for a network directory in the NetStorage directory access list displayed through Microsoft Web Folders or a Web browser. Creating a Storage Location object is useful if users expect the directory to have a certain name. Unlike directories that are displayed from a login script, or Home directories that have a name that cannot be altered, you can specify the Storage Location object name.

After you have created a Storage Location object, you must associate this object with a User, Group, Location, or Container object. Users see the directory associated with the object the next time they log in.

- ♦ “Creating a Storage Location Object” on page 42
- ♦ “Creating or Modifying a Storage Location List” on page 43
- ♦ “Modifying a Storage Location Object” on page 43
- ♦ “Deleting a Storage Location Object” on page 44

Creating a Storage Location Object

- 1 Start your browser (Internet Explorer 5 or later, Mozilla, etc.) and specify the URL for iManager.

The URL is `http://server_ip_address/nps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running NetStorage or the IP address for Apache-based services.

- 2 Type your username and password.

- 3 In the left column, click *File Access*, then click *New Storage Location*.

- 4 Specify the object name, display name, directory location, context, and a comment.

The object name is the name of the object in the eDirectory tree.

The display name is the name to be displayed in the NetStorage directory access list. This is the shortcut name and is seen by users. If you use the same display name for two different Storage objects, a digit is added to the names to make each name unique.

The directory location is the location of the directory on the file system. The location is a URL that includes the file system type, server name, volume, and directory path.

If the storage being accessed is on a NetWare server, the URL must be in the following format:

`ncp://server_name/volume/path_to_directory`

For example:

`ncp://server1.digitalair.com/mktg/reports`

or

`ncp://111.222.3.4/mktg/reports`

If the storage being accessed is on a Linux server, the URL must be in one of the following formats:

- ♦ `ncp://server_name/volume/path_to_directory`

This method requires that the NCP Server component of OES be installed on your Linux server.

- ♦ `cifs://server_name/cifs_share_name`

This method can be used if you have configured a CIFS or Samba share (cifs can be interchanged with smb).

- ♦ `ssh://yourserver.yourcompany.com/home/youruser`

This method allows access to files on Linux systems that don't support either NCP or CIFS (SMB) protocols.

IMPORTANT: NetStorage storage location objects defined with the SSH protocol do not function unless SSHD has been enabled for LUM users.

If you want to access local files or files on another server in the same eDirectory tree by using the SSH file access method, you must select the SSHD check box during the OES installation or enable SSHD afterwards by using YaST. The check box is in the Linux User Management configuration section on the OES installation.

If the file system is omitted, it is assumed that it is NCP.

The context is the directory context that the Storage Location object resides in. Click the object selector to select the context.

The comment is entered by the administrator and is not displayed to users.

- 5 Click *Create*, then click *OK*.

Creating or Modifying a Storage Location List

After you create a Storage Location object, you must create a list of Storage Location objects that can be used with a specified User, Group, Profile, or Container object. Users see the directory associated with the object the next time they log in. After this list is created, you can modify it from the same window by assigning additional Storage Location objects to the list or by deleting Storage Location objects from the list.

- 1 Start your browser (Internet Explorer 5 or later, Mozilla, etc.) and specify the URL for iManager.

The URL is `https://server_ip_address/nps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running NetStorage or the IP address for Apache-based services.

- 2 Type your username and password.
- 3 In the left column, click *File Access*, then click *Assign Storage Location to Object*.
- 4 Click the *Object Selector* button; select the User, Group, Profile, or Container object that the list is to be created for; then click *OK*.

IMPORTANT: If you enter an invalid object name in the *Object* field and click *OK*, you are directed back to the Home page instead of going to the next page.

- 5 Click the *Object Selector* button, select the Storage Location objects you want included in this list, then click *OK*.

You can select multiple Storage Location objects in the Object Selector window. When you select multiple Storage Location objects, they appear in the *Selected Objects* list. If the list already contains Storage Location objects and you want to add more, ensure that the original objects are still in the list before clicking *OK*.

- 6 (Optional) Remove existing storage locations by deleting their names from the list before clicking *OK*.
- 7 When you are finished creating or modifying the list, click *OK*.

Modifying a Storage Location Object

- 1 Start your browser (Internet Explorer 5 or later, Mozilla, etc.) and specify the URL for iManager.

The URL is `https://server_ip_address/nps/manager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running NetStorage or the IP address for Apache-based services.

- 2** Type your username and password.
- 3** In the left column, click *File Access*, then click *Edit Storage Location*.
- 4** Click the *Object Selector*, then select the Storage Location object that you want to modify.
- 5** Modify the display name, display location, or comment, then click *OK*.
If you need to modify the object name or eDirectory context, you must delete this object and create a new Storage Location object.
- 6** Click *OK*.

Deleting a Storage Location Object

- 1** Start your browser (Internet Explorer 5 or later, Mozilla, etc.) and specify the URL for iManager.
The URL is `https://server_ip_address/nps/manager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running NetStorage or the IP address for Apache-based services.
- 2** Type your username and password.
- 3** In the left column, click *File Access*, then click *Delete Storage Location*.
- 4** Click the *Object Selector* button, then select the Storage Location object that you want to delete.
- 5** Click *OK*.

7.3 What's Next

After you have configured NetStorage, inform users that they can access their files from the Web. Instructions for accessing files through NetStorage are available in [Chapter 6, “Using NetStorage,” on page 29](#).

Troubleshooting NetStorage

8

This section contains information on common troubleshooting issues. In addition to the information in this section, additional information is located in Technical Information Documents (TIDs) available in the Knowledge base on the [Novell Support Web site \(http://support.novell.com\)](http://support.novell.com).

- ♦ [Section 8.1, “Unexpected Results from Login Scripts,” on page 45](#)
- ♦ [Section 8.2, “Slow Login,” on page 45](#)
- ♦ [Section 8.3, “Configuring LDAP Contextless Login for Use with NetStorage,” on page 46](#)
- ♦ [Section 8.4, “Configuring NetStorage to Use the Proper Code Page or Character Set,” on page 47](#)
- ♦ [Section 8.5, “Configuring NetStorage with iChain,” on page 47](#)
- ♦ [Section 8.6, “Accessing CIFS or SSH Storage Locations,” on page 48](#)
- ♦ [Section 8.7, “LUM Must Have SSHD Access Enabled,” on page 48](#)
- ♦ [Section 8.8, “Restricted SSH Access for Samba Users,” on page 48](#)
- ♦ [Section 8.9, “Phantom Folders,” on page 49](#)
- ♦ [Section 8.10, “The Assign Storage Location Page Navigates to the Home Page,” on page 49](#)

8.1 Unexpected Results from Login Scripts

When a user authenticates to NetStorage, if NCP Server is installed, the login scripts associated with the Novell eDirectory™ User object in the primary authentication domain are processed. These login scripts are the same scripts processed by the Novell Client™.

However, because login scripts were designed to be processed by the Novell Client on the user's workstation, some of the defined statement types and script variables cannot be processed by NetStorage.

Specific information about how login scripts interact with NetStorage is available in [Login Script Processing by NetStorage \(TID10068983\) \(http://support.novell.com/cgi-bin/search/searchtid.cgi?/10068983.htm\)](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10068983.htm).

The maximum size of a login script is 16 KB. If the 16 KB limit is exceeded, login script drive mappings fail.

8.2 Slow Login

The most common cause of a slow login to NetStorage is large or poorly configured login scripts. When a user authenticates to the Primary Authentication domain, all applicable login scripts for that User object are processed. The more commands executed, the longer the login process.

Invalid authentication domains can also slow the login process. After the user has been authenticated to the Primary Authentication domain, the same username and password are used to authenticate to any Secondary Authentication domains. Authentication failure on any of these domains slows logins. Users can successfully authenticate to the Primary Authentication domain but fail at each of the secondary domains.

It is helpful to determine if slow logins are global (all users) or specific to a given user object. If all users are affected, it is more likely to be a problem with the XTier authentication domain configuration. If a single user or groups of users are affected, check all login scripts that apply to that user or group. A problem with a context's login script can affect a large number of users. Finding out which scripts apply to which users can help narrow the problem.

For more information, see [Login Script Processing by NetStorage \(TID10068983\)](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10068983.htm) (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10068983.htm>).

8.3 Configuring LDAP Contextless Login for Use with NetStorage

When configuring LDAP contextless login, consider the following issues:

Primary Authentication Domain: The user must be authenticated to the Primary Authentication domain (an eDirectory server with a replica). You can provide more than one context in the Primary Authentication domain, resulting in each context being searched for the presence of the user. The search is performed through an LDAP search of the configured contexts.

Secondary Authentication Domain: After the user is authenticated to the Primary Authentication domain, the same username and password is used to authenticate to any Secondary Authentication domains. The search is performed through an LDAP search of the configured contexts for that domain. If authentication to any Secondary domains is unsuccessful, the user is still authenticated to the Primary Authentication domain. Authentication failure on a Secondary domain can cause a delay in the login process and is one of the most common causes of slow logins to NetStorage.

Enable TLS for Simple Binds with Passwords: Passwords are encrypted in eDirectory, so you must enable TLS for simple binds with passwords in LDAP. For more information, see “[Requiring TLS for Simple Binds with Passwords](#)” in the *Novell eDirectory 8.7.3 Administration Guide*.

LDAP needs Read and Browse rights to the entire tree. By default, when a user performs an anonymous bind (doesn't specify a password), a special object in the directory calculates access control for that user. This object is termed [Public]. By default, this object can browse the entire tree hierarchy and read a limited number of attributes on entries.

If you want to have an anonymous bind use a different object in the tree, you can specify the object in the *Proxy Username* field. By doing this, you can restrict the types of objects and attributes that anonymous users can access by setting the appropriate access controls on the proxy User object. The proxy username must be a distinguished name. To easily select an object, click the directory browser button to the right of the text field on the LDAP Group Object. A dialog box appears that allows you to choose an object in the tree. Any eDirectory User object can be used and the anonymous access assumes the rights of that user.

IMPORTANT: A proxy user must have a blank password in order to work correctly. This is very different from having no password. If a user has no password, then he or she does not have a public/private key pair to compare against when attempting login. A blank password generates a public/private key pair, although the actual string for the password is empty.

8.4 Configuring NetStorage to Use the Proper Code Page or Character Set

NetStorage can be configured to use different languages and characters by changing the character set or code page on your Linux server. Character set or character map is the Linux equivalent of the code page in NetWare®. The default character set for NetStorage is the same as the character set that `root` is configured to use. This character set is determined during the Virtual Office installation.

You can determine the character set that `root` is configured to use by entering `locale charmap` at the Linux server console. Character sets for different users are configured by setting the `LC_*` environment variables.

If the character set that `root` is configured to use is not the same as the one that NetStorage is configured to use, you must configure NetStorage to use a different character set. To do this, edit the `/etc/opt/novell/xtier/xsrvd/envvars` file and modify the `XTIER_CODE_PAGE` environment variable.

As a general rule, NetStorage should use the same code page as the servers hosting storage that NetStorage accesses. For example, if NetStorage is being used to access storage on NetWare servers that are configured to use the 437 code page, then you should set the `XTIER_CODE_PAGE` environment variable to 437.

You can determine which character sets are installed and available on your Linux server by entering `iconv --list` at the server console.

Character set names might not be exactly the same between NetWare and Linux servers. For example, the 1254 NetWare code page maps to the WINDOWS-1254 Linux character set.

8.5 Configuring NetStorage with iChain

If you are configuring NetStorage to run behind a Novell iChain server (fronting NetStorage with iChain), there are some configuration changes required in order for NetStorage to function properly. These configuration changes include enabling cookieless authentication and editing the `logout.html.utf8` file.

- ♦ [Section 8.5.1, “Enabling Cookieless Authentication,” on page 47](#)
- ♦ [Section 8.5.2, “Editing the Logout.html.utf8 file,” on page 48](#)

8.5.1 Enabling Cookieless Authentication

- 1 Start your browser (Internet Explorer 5 or later, Mozilla, etc.) and specify the URL for iManager.

The URL is `http://server_ip_address/nps/imanager.html`. Replace *server_ip_address* with the IP address or DNS name of the Linux server running NetStorage or the IP address for Apache-based services.

- 2 Enter your username and password.
- 3 In the left column, click *File Access*, then click *NetStorage Options*.
- 4 Set the value for the *Cookieless* option to 1.

The *Cookieless* option can be turned either on or off. With the value set to 0, cookieless authentication is turned off (the default). Cookieless authentication can be turned on by setting the value to 1.

If cookieless authentication is turned on, you must close all browser instances to log out.

8.5.2 Editing the Logout.html.utf8 file

The `logout.html.utf8` file is located in the `/opt/novell/netstorage/webapp` directory on the Linux server where NetStorage is installed. Edit the file and replace `<iChainDNS>` with the DNS name of the iChain server. To enable iChain logout, some lines must be uncommented and others must be removed. There are instructions in the file on which lines to remove and uncomment.

8.6 Accessing CIFS or SSH Storage Locations

If you experience problems accessing CIFS (SMB) or SSH storage locations, the problem might be related to CIFS or SSH, and not NetStorage. Try logging in through a different client to determine if a CIFS or SSH problem exists.

8.7 LUM Must Have SSHD Access Enabled

If you want to access local files or files on another server in the same eDirectory tree by using the SSH file access method, you must select the SSHD check box checked during the OES installation. The check box is in the Linux User Management configuration section of the OES installation.

The check box is not selected by default. If you leave the SSHD check box deselected during the OES installation, users cannot login through SSH and will not be able to access files using that method unless you use YaST to enable SSHD after the installation.

If you encounter an error similar to the following example, the problem might be caused by not having SSHD enabled.

```
NetStorage encountered an error while trying to access this location.
```

```
Severity: Error
```

```
Facility: SSH WebDAV Handler
```

```
Message: Access Denied: Caller does not have required access rights for operation
```

```
Code: 0xC7A10006
```

8.8 Restricted SSH Access for Samba Users

Users that have been enabled for Samba do not by default have access to files and folders by using SSH Storage Location objects.

When a user is enabled for Samba, that user is automatically added to a Samba group. The Samba group by default does not allow SSH access. This means that any user in the Samba group is not allowed SSH access even if that user belongs to another group that allows SSH access.

To allow a Samba-enabled user to have SSH access (and use SSH storage locations), you can either remove the user from the Samba group or enable SSH access for the Samba group, which also enables SSH access for all users in the Samba group.

For more information, see the *OES 2:Planning and Implementation Guide* (http://www.novell.com/documentation/oes2/oes_implement_lx_nw/data/manage-ssh.html).

8.9 Phantom Folders

A phantom folder might appear with some uses of Microsoft WebDAV. The phantom folder has a different icon than normal folders and should be ignored.

A phantom folder usually appears when using My Network Places on a Windows client. My Network Places uses Microsoft's WebDAV client, which assumes that the directory name returned means that there is also a subdirectory with the same name.

8.10 The Assign Storage Location Page Navigates to the Home Page

In the Assign Storage Location page, when you enter an object name in the *Object* field and click *OK*, you might be directed to the Home page instead of the Create / Modify Storage Location List page. Check the following:

- ♦ Ensure that you have entered a valid object name.
- ♦ Ensure that the Storage Location object was correctly created. For more information, see [“Creating a Storage Location Object” on page 42](#).

Security Considerations

A

This section contains specific instructions on how to configure Novell® NetStorage in the most secure way possible. It contains the following subsections:

- ♦ [Section A.1, “Security Features,” on page 51](#)
- ♦ [Section A.2, “Security Configuration,” on page 52](#)
- ♦ [Section A.3, “Security Recommendations,” on page 53](#)
- ♦ [Section A.4, “Other Security Considerations,” on page 55](#)

A.1 Security Features

The following table contains a summary of the security features of NetStorage:

Table A-1 *NetStorage Security Features*

Feature	Yes/No	Details
Users are authenticated	Yes	Administrative users are authenticated via eDirectory™.
Users are authorized	Yes	Users are authorized via eDirectory trustees.
Access to configuration information is controlled	Yes	Access to the administrative interface is restricted to valid users that have write rights to the configuration files.
Roles are used to control access	Yes	Configurable through iManager.
Logging and/or security auditing is done	Yes	Syslog on Linux. On NetWare®, messages go on the logger screen. XTier has its own login mechanism on all platforms. XTlog is also used.
Data on the wire is encrypted by default	Yes	Data is encrypted on the wire if SSL is used. If SSL is not used, NetIdentity can be used to provide secure authentication.
Stored data is encrypted	No	
Passwords, keys, and any other authentication materials are stored encrypted	Yes	Username and passwords are encrypted. NetStorage configuration is encrypted in eDirectory.
Security is on by default	Yes	This is a Web server setting, and can be turned on or off at the Web server.

A.2 Security Configuration

The following subsections provide a summary of security-related configuration settings for NetStorage:

- [Section A.2.1, “NetStorage Configuration Settings,” on page 52](#)
- [Section A.2.2, “Security Information for Other Products,” on page 52](#)

A.2.1 NetStorage Configuration Settings

The following table lists the NetStorage configuration settings that are security related or that impact the security of NetStorage:

Table A-2 *NetStorage Security Configuration Settings*

Configuration Setting	Possible Values	Default Value	Recommended Value for Best Security
Session timeout	Time in seconds		
Persistent Cookies	0, 1	0	0 (Disabled)
Cookieless Authentication	0, 1	0	0 (Disabled)
Secure Port		443	443

A.2.2 Security Information for Other Products

The following table provides links to security-related information for other products that impact the security of NetStorage:

Table A-3 *Security Information for Other Products*

Product Name	Links to Security Information
NSS	“Securing Access to NSS Volumes, Directories, and Files” (http://www.novell.com/documentation/oes/nss_enu/data/bv8n39l.html#bv8n39l). and “Security Considerations” (http://www.novell.com/documentation/oes/nss_enu/data/bx8gp06.html).
eDirectory	Security for eDirectory is provided by NCI. See the NICI 2.7x Administration Guide (http://www.novell.com/documentation/nici27x/nici_admin_guide/data/a20gkue.html)

Product Name	Links to Security Information
Novell Client™	<p>“Security Considerations” (http://www.novell.com/documentation/linux_client/linuxclient12/data/bu0ossa.html#bu0ossa) in the <i>Novell Client for Linux Administration Guide</i>.</p> <p>and</p> <p>“Managing File Security and Passwords” (http://www.novell.com/documentation/noclienu/noclienu/data/h9nmmvwn.html#h9nmmvwn) in the <i>Novell Client for Windows Installation and Administration Guide</i>.</p>
Samba	See “Security Implications” (http://www.novell.com/documentation/oes/samba_admin/data/bxqfo6c.html) in the <i>Samba Administration Guide for OES Linux</i> .
Novell Password Management	<i>Novell Password Management Administration Guide</i> (http://www.novell.com/documentation/password_management31/treetitl.html)

A.3 Security Recommendations

The following subsections provide a summary of security-related recommendations for NetStorage:

- ♦ Section A.3.1, “Registry Access Control,” on page 53
- ♦ Section A.3.2, “Use NMAS,” on page 54
- ♦ Section A.3.3, “Use SSL with Your Web Server,” on page 54
- ♦ Section A.3.4, “Persistent and Session Cookies,” on page 54
- ♦ Section A.3.5, “Use Web Server Logs,” on page 54
- ♦ Section A.3.6, “Use XTLog,” on page 54
- ♦ Section A.3.7, “Denial of Service Attacks,” on page 54
- ♦ Section A.3.8, “Trusted Roots in CAPI,” on page 55
- ♦ Section A.3.9, “Certificate Validation Registry Setting,” on page 55

A.3.1 Registry Access Control

Access control to the registry is enforced by the operating system.

On Windows (any version), each branch of the registry can have its own ACL (access control list). Windows checks to see if the calling thread has permissions to read/write/modify the registry entry being accessed, and returns status appropriately.

On NetWare, local access to the registry is a trusted operation, and any NLM™ running on the server is allowed access.

On Linux, XTier has implemented its own registry based on XFLAIM, and access to this database is via UNIX domain sockets. Only XTier's registry user (novlxregd) and group (novlxtier) have access to these domain sockets, and access control is enforced via file system permissions. For any process to access the registry, the user associated with the process must be a member of the novlxtier group. Adding a user to a group is a privileged operation, and can be done only by an administrator.

WARNING: Do not store security-sensitive information in the registry. Sensitive information such as passwords should not be stored in the registry unless it is protected by strong encryption.

A.3.2 Use NMAS

NMAS™ login is designed to be more secure than NDS4. You should enable NMAS login for eDirectory users and enable the corresponding setting in NetStorage.

A.3.3 Use SSL with Your Web Server

Without SSL, all traffic to the Web server from the client, browser, or WebDAV client is in the clear. This allows anyone to snoop the traffic and look at all the data, including the data for authentication. This applies when the Basic authentication scheme is used. Using SSL provides privacy for all data traffic between the workstation/client and the Web server.

A.3.4 Persistent and Session Cookies

Session cookies are valid only for the duration of the browser/client session. After the windows of the browser are closed, these cookies are discarded by the browser, and a new instance of the browser has no knowledge of previously set session cookies.

Persistent cookies have an expiration date/time, and are valid until then. Persistent cookies are stored in persistent storage (usually the file system), so that newer instances of the browser can pick them up.

For more information about cookies, see “Persistent Client State HTTP Cookies” (http://wp.netscape.com/newsref/std/cookie_spec.html).

A.3.5 Use Web Server Logs

You should check Web server logs frequently for security-related information.

A.3.6 Use XTLog

See “Enable Debug Logging in ZDM 6.5 and 7” (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3112868&sliceId=SAL_Public&dialogID=36914517&stateId=1%200%202640049) for information on how and when to use XTLog.

Although the information refers to the ZENworks® Middle Tier Server, it also applies to other XTier applications such as NetStorage.

A.3.7 Denial of Service Attacks

Application developers should be aware of the possibility of denial of service attacks. This is true for any Web-based application. For example, if a DoS attack can be mounted on Apache or IIS, any XTier-web application is affected, because XTier-web runs as a module (or extension) of Apache and IIS.

A.3.8 Trusted Roots in CAPI

For instructions on setting up trusted roots in CAPI, see “Trusted Root Certification Authority Policy” (http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_pkpusecertroot.msp?mfr=true).

A.3.9 Certificate Validation Registry Setting

If you are using NetIdentity, do not use the registry setting that allows a connection without certificate validation. The NetIdentity client places a registry setting on the client workstation. For more information, see “Setting Up NetIdentity Authentication” (<http://www.novell.com/documentation/zenworks7/dm7install/index.html?page=/documentation/zenworks7/dm7install/data/ahi6dan.html>) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

A.4 Other Security Considerations

- ♦ Servers should be kept in a physically secure location with access by authorized personnel only.
- ♦ The corporate network should be physically secured against eavesdropping or packet sniffing. Any packets associated with the administration of NetStorage should have the highest security.
- ♦ Access to NetStorage configuration settings and logs should be restricted. This includes file system access rights, FTP access, access via Web utilities, SSH, and any other type of access to these files.
- ♦ When NetStorage is administered by users outside of the corporate firewall, the HTTPS protocol should be used. A VPN should also be employed.
- ♦ If a server is accessible from outside the corporate network, a local server firewall should be employed to prevent direct access by a would-be intruder.
- ♦ Log files should be kept and analyzed periodically.

