Dynamic Storage Technology 1.0 Administration Guide

Open Enterprise Server 2 SP3

June 2013

Novell.

Legal Notices

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

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

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

Copyright © 2007–2013 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.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This guide describes how to install, configure, and manage the Dynamic Storage Technology for Novell Open Enterprise Server (OES) 2 Linux (or later). It is divided into the following sections:

Audience

This guide is intended for storage services administrators. Security administrators can find a summary of security information for Dynamic Storage Technology in Chapter 15, "Security Considerations," on page 179.

It is assumed that the reader has some understanding of the OES 2 Services components that are used with Dynamic Storage Technology, including the OES 2 Linux operating system, the NSS file system, the file access services (NCP (NetWare Core Protocol), Novell CIFS (Common Information File System), and SMB/CIFS), and Novell Cluster Services.

Feedback

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

Documentation Updates

For the most recent version of the *Dynamic Storage Technology Administration Guide*, see the Novell Open Enterprise Server 2 documentation Web site (http://www.novell.com/documentation/oes2/).

Additional Documentation

For documentation on Novell Storage Services (NSS) volumes, see the *OES 2 SP3: NSS File System Administration Guide for Linux*.

For documentation on NCP Server and NCP file access, see the *OES 2 SP3: NCP Server for Linux Administration Guide*.

For documentation on other OES 2 products, see the Novell Open Enterprise Server 2 documentation Web site (http://www.novell.com/documentation/oes2/).

1 Overview of Dynamic Storage Technology

Dynamic Storage Technology (DST) for Novell Open Enterprise Server (OES) 2 Linux is an information life-cycle management technology that uses a policy-based approach for relocating data between two Novell Storage Services (NSS) volumes located on different devices. It transparently provides a merged view of the file tree to users. An administrator can specify policies that classify data to be moved by its frequency of use, file extension, and file size. Policy enforcement is automated with scheduled and on-demand runs of the policies.

Dynamic Storage Technology allows you to seamlessly tier storage between high-performance and lower-performance devices. For example, you can establish policies that keep frequently used, mission-critical data on high-performance devices, and move rarely accessed, less-essential data to lower-performance devices. Backup can be performed separately on the two volumes, which allows for different backup schedules.

Dynamic Storage Technology enables you to manage data more efficiently for the enterprise. In doing so, the enterprise can potentially realize significant cost savings in storage management.

This section provides an overview of Dynamic Storage Technology and its components.

1.1 Understanding Dynamic Storage Technology

Dynamic Storage Technology (DST) for OES 2 Linux is a feature of NCP Server that allows you to specify a shadow relationship between two volumes that form a *shadow volume pair*. The secondary directory tree structure, or *secondary file tree*, shadows the primary file tree.

IMPORTANT: Only NSS volumes are supported to be used for DST shadow volume pairs.

1.1.1 Merged View of the File Tree

Dynamic Storage Technology presents the directory trees on each volume in a merged view, as illustrated in Figure 1-1. The primary file tree and shadow file tree have the same directory structure, so that each directory appears in both locations as data is moved between the two volumes. The primary tree and the secondary tree are overlaid to create one virtual volume tree that is transparently presented to the users. When accessing files through the merged view, users are not aware of the actual physical location of the files. If the shadow relationship is removed, the secondary volume can once again function independently and normally.

Figure 1-1 *User View of the File System Directory*
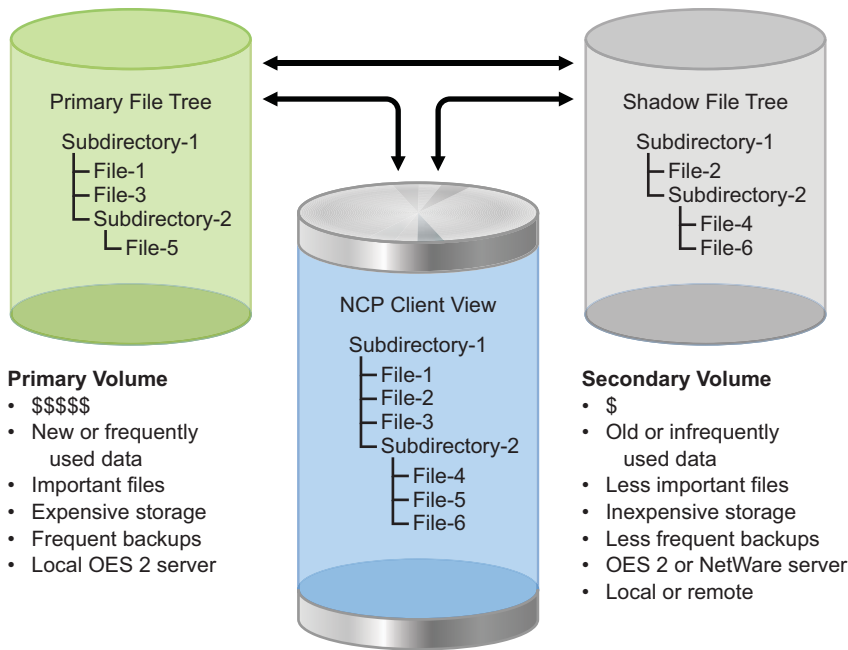
An example of the merged view of the shadow volume is shown in Figure 1-1. When an NCP client lists files for `Subdirectory-1`, the user sees `File-1`, `File-2`, and `File-3`. `File-1` and `File-3` are stored in the primary file tree. `File-2` is stored in the shadow file tree.

When a client creates new files, the files are automatically stored in the primary file tree. When files in the shadow file tree are modified, a configurable option allows the files to be moved to the primary file tree (default), or left in the shadow file tree.

For example, if your policy is to place newer files in the primary file tree and to place older files in the shadow file tree, you want an older file in the secondary file tree to move to primary file tree if the file's content is modified. On the other hand, if you are placing files of one type (such as `.doc` and `.ppt`) in the primary area and files of a different type (such as `.mp3` and `.jpg`) in the secondary area, you want files to stay where they are whenever they are modified.

When a new directory is created, it is created in the primary file tree. A configurable option allows the necessary branches of the tree to be created in the shadow file tree in one of two ways:

- The new directory path is created as needed when policies are enforced to move files to the directory in the secondary location (the default)

- The new directory path is created immediately in the secondary location, and files are moved to the directory as policies are enforced.

Performance is better when the directory branches are created only as needed.

When a directory is deleted, it is deleted in both areas. When a directory is renamed, it is renamed in both areas. The coordination of the file and directory management happens automatically so that the areas remain synchronized and have the same directory structure.

1.1.2 Merged View for User File Access

Dynamic Storage Technology supports a merged view via NCP for user file access. You can also install and configure one of the following OES Services on the DST host server to provide a merged view for CIFS user access:

- Novell CIFS (in OES 2 SP3 Linux or later)

  Use Novell CIFS with the primary NSS volume in the DST shadow volume pair, just as you would with a regular NSS volume.

- Novell Samba

  This SMB/CIFS solution requires FUSE and ShadowFS as described in Chapter 12, "Using ShadowFS to Provide a Merged View for Novell Samba Users," on page 129. Configure SMB/CIFS shares on the primary NSS volume.

Users access files by connecting to the primary volume. All file operations (such as read, write, rename, delete, and so on) can be performed whether a file resides on the primary or secondary location. Dynamic Storage Technology executes the transaction transparently for the user.

In general, transactions are executed wherever the file resides. Any file that requires a normal user-level action (copy, delete, and so on) is moved back to the primary for the action to take place, which simplifies the auditing requirements. Some transactions, such as a directory rename, occur in both file trees in order to keep the paths synchronized.

In OES 2 SP2 Linux and earlier, only NCP and the Novell Samba solution are supported for a merged view of user file access.

1.1.3 Local File Access

After you create the shadow relationship, the secondary volume is hidden to everyone but those users or applications that are authorized to view the local Linux file system, such as the root user. The only operations that are intended to take place directly on the secondary volume are backup, or "remove and archive."

For example, backup administrators and system administrators with root user privileges on the server can see the primary file tree and the shadow file tree as separate and independent directories. Thus, backup tools can apply one backup policy to the primary volume location and apply a different backup policy to the secondary volume location.

1.1.4 File Systems

The primary area and the secondary area can each be located anywhere in the logical Linux directory tree that is available to the server. For example, the default location for NSS volumes is in the /media/nss/ directory, but DST can handle any mount point that you specify for your NSS volumes.

The primary volume and secondary volume must use the same file system. Only the NSS file system is supported at this time.

The primary and secondary volumes can be located on a local SCSI devices, Fibre Channel SAN devices, and iSCSI SAN devices. The device types and performance can differ between the primary and secondary devices, with the secondary volume typically being on the device with lower performance.

Clustering is supported with Novell Cluster Services.

1.2 Benefits of Dynamic Storage Technology

Shadow volumes have many benefits:

- Section 1.2.1, "Transparent File Access to End Users," on page 18
- Section 1.2.2, "Policy-Based Migration between Primary and Secondary Storage Areas," on page 18
- Section 1.2.3, "Faster and Smaller Backups of Important Data," on page 18
- Section 1.2.4, "Faster Disaster Recovery," on page 19
- Section 1.2.5, "More Efficient Use of Expensive Storage," on page 19
- Section 1.2.6, "Fast Storage for Active Data and Slower, Less Expensive Storage for Old Data," on page 19
- Section 1.2.7, "Moving Files from an Existing Secondary Volume," on page 19
- Section 1.2.8, "Access to the Secondary Storage Area without the Performance Penalties of HSM Solutions," on page 20

1.2.1 Transparent File Access to End Users

Because shadow volumes present a merged view of the file trees, the end user's files appear to be in the same logical place regardless of their physical location. This allows the administrator to manage the data without disrupting the end user's view of the files.

1.2.2 Policy-Based Migration between Primary and Secondary Storage Areas

DST provides policy-based control of the files to move and the direction that you want to move data between devices. You can set up policies that migrate data by file extension, file size, and the date last accessed or modified. You can also specify a list of files to move in either direction for a one-time move. Policies can be scheduled to run and run on demand. You can set policies so that data stored on the secondary storage volume can be accessed without de-migrating it.

1.2.3 Faster and Smaller Backups of Important Data

Backup policies can differ for the primary storage volume and the secondary storage volume. For example, the DST administrator can allocate the data between the two volumes in a way that supports separate backup schedules:

- Important or active data that needs to be maintained on quality storage and backed up frequently
- Less important or stale data that can be stored on less expensive storage and backed up less frequently

Analyzing the inventory of a volume's data shows that a large portion of its data is seldom used. Having a shadow volume allows the administrator to spend more on the most important data and spend less on the less important data. The important data, which is stored on the primary area, can be backed up nightly. The less important data, which is stored in the secondary area, can be backed up weekly or even monthly. Getting the less important data out of the way enables the backups of your important data to run more quickly and efficiently. Allocating data in this way can significantly lower the cost of backups by reducing both labor and tape requirements.

For information about backing up data on DST volumes, see:

- Section 5.11, "Using Backup Utilities with DST Shadow Volumes," on page 55
- Section 9.11, "Backing Up DST Shadow Volumes," on page 92

1.2.4 Faster Disaster Recovery

Start by locating your most important files on the primary area. Then, during a disaster recovery, the server administrator can restore the primary area first. This restores the critical files first, and leaves the recovery of the less important secondary area until later. The users can continue working while files they probably do not need immediately are being restored. Also, other fault-tolerant replication solutions like snapshots can be used for the primary area without wasting money on files that do not require the same level of fault tolerance.

1.2.5 More Efficient Use of Expensive Storage

Policies can be used to partition files based on file age, owner, type, size, and so on. You can move the less important files to from a higher quality storage array to a lower quality storage, thus reserving the higher-cost storage for your most important files. For example, you can configure the primary area on block-based SCSI storage devices in a Fibre Channel SAN-based hardware RAID array or storage array, and configure the secondary area on a lower quality storage array using slower devices like SATA. This allows you to get more use out of your Fibre Channel storage solution, and keep it from filling up with unimportant files. You can store more data on your server with a lower overall cost per gigabyte.

1.2.6 Fast Storage for Active Data and Slower, Less Expensive Storage for Old Data

Storage media can differ for the primary storage volume and the secondary storage volume. Storage costs can be reduced by allowing data that is used infrequently to be stored on lower-cost storage. Locate the primary area on storage drives that are faster and higher quality. Then locate the secondary area on less expensive storage drives. Files that the users are currently working on can be located on the high-performance drives. The files that have not been modified for a long time can be moved to the lower-performance drives to free up space on the high-performance drives. In this way, you can locate a large amount of your data on less expensive, lower-performance storage drives, while your users still get high-quality performance because their active files are located on the high-performance storage drives.

1.2.7 Moving Files from an Existing Secondary Volume

You can start with an empty primary NSS volume, and have the shadow area be an existing volume. The combined view initially presented by the NCP Engine is equivalent to the secondary volume. You can define a policy to move files to the primary as they are modified or accessed. As users access

their data through the new primary volume, the files they use are automatically migrated to the new server. This migration-on-demand approach migrates the data gradually, freeing the IT department from spending off-hours time migrating the data with the server offline.

1.2.8 Access to the Secondary Storage Area without the Performance Penalties of HSM Solutions

With HSM (hierarchical storage management) solutions, files are migrated from the primary storage to a secondary storage device, and a copy of the file's metadata (stub file) is left behind in the volume's directory tree. If the file is ever accessed again, it needs to be migrated back to the primary storage before it is available.

In contrast, DST shadow volumes can access files directly regardless of which area (primary or secondary) they are in, and without de-migrating them. If a user searches through all the files on a shadow volume, the files are searched without needing to move them to the primary area. Also, shadow volume backups are faster because there are no HSM metadata stub files for the backup software to scan. The backup software does not need to be HSM aware.

1.3 Shadowing Scenarios

The flow of data between the primary storage area and the secondary storage area can take place two ways:

- Section 1.3.1, "Existing Volume as Primary with an Empty Volume as Secondary," on page 20
- Section 1.3.2, "Empty Volume as Primary with an Existing Volume as Secondary," on page 21

1.3.1 Existing Volume as Primary with an Empty Volume as Secondary

In this scenario, all data currently exists on an NSS volume that you want to make the primary volume. You create a new volume to use as the secondary storage, then define a shadow volume for the two NSS volumes.

The volume contains information that is seldom used and rarely changes, and you want to move the seldom-used data to a location where it can be accessed but backed up less frequently. This decreases the time it takes to back up or restore the data you use the most.

Then, you can configure a policy that governs what data moves to the secondary storage area. Data is returned to the primary area based on a policy of usage or file type. For example, if the user simply views the data in a file, then the data does not move. If the user modifies the file, then the file is moved back to the primary volume. Users are not aware of where the data are physically stored because they see a merged view of both volumes.

1.3.2 Empty Volume as Primary with an Existing Volume as Secondary

You have an existing volume on older storage and want to move the data to new storage arrays. You create a new volume on a storage device in a Fibre Channel SAN solution. You define a shadow volume that uses the empty device as the primary area, and the existing volume as the secondary area.

You can configure a policy so that the data moves to the primary volume based upon usage. Data gradually flows to the primary volume as it is used. In this way, there is a natural background migration of data from the existing volume to the new volume. The new volume gradually grows, and the relationship between the primary and shadow volume is as if the primary had been populated first.

For example, suppose you have an existing pool that spans multiple LUNs, and contains multiple volumes. The current best practice is to use a separate LUN for each pool, and a single volume per pool. You create a new pool on a new larger LUN (or fewer larger LUNs), then create a single NSS volume in the pool. You might need to rename the old and new NSS volumes if users need to access the data via known paths, because after the shadow volume is created, users access data via the new volume. Repeat this process so that you have one new empty volume for each of the old volumes on the pool. As the new and old volumes are ready, you create a DST shadow volume with the new volume as the primary storage area and an existing volume from the old pool as the secondary storage area.

To begin de-migrating the data, configure the global policies to shift data from the secondary storage area to the primary storage area whenever they are accessed or modified. You can also configure individual shadow volume policies or use inventory reports to shift data on schedule or on-demand based on age, file names, file types, or file size. De-migration occurs with the storage online and accessible to end users; they are not aware of where the data is actually stored.When you have moved all the data from the old NSS volume to the new one, you can remove the shadow volume, then delete the empty old NSS volume from the old pool. When the old pool has had all its volumes deleted, you can delete the old pool, which frees that storage for use in other volumes. Users are not aware that the volumes are on a new pool. They see only the volume by its name.

1.4 DST Policy Scenarios

DST policies control how data flows between the primary storage area and the secondary storage.

- Section 1.4.1, "Move Files Based on the Last Time Accessed or Modified," on page 21
- Section 1.4.2, "Move Files Based on File Size," on page 22
- Section 1.4.3, "Move Files Based on File Extensions," on page 22
- Section 1.4.4, "Move Selected Files," on page 22

1.4.1 Move Files Based on the Last Time Accessed or Modified

You can create a DST policy that moves files to the secondary volume that have not been modified or accessed for a period of time, such as 6 months or 1 year.

1.4.2 Move Files Based on File Size

You can create a DST policy that moves files to the secondary volume that have are greater than or less than a specified file size.

By default, files in the secondary area are moved back to the primary area if they are modified. You should disable the SHIFT_MODIFIED_SHADOW_FILES parameter to turn off this auto-move feature. The SHIFT_ACCESSED_SHADOW_FILES parameter is disabled by default so that files are not moved when accessed. These settings are global settings that apply to all shadow volumes on a given server. In this way, the desired file types stay in the secondary area after they are moved there.

1.4.3 Move Files Based on File Extensions

You can create a DST policy that moves non-essential types of files based on file extensions, such as `*.jpg`, `*.mp3`, `*.wma`, `*.mpeg`, `*.iso`, `*.zip`, `*.cab`, and so on.

By default, files in the secondary area are moved back to the primary area if they are modified. You should disable the SHIFT_MODIFIED_SHADOW_FILES parameter to turn off this auto-move feature. The SHIFT_ACCESSED_SHADOW_FILES parameter is disabled by default so that files are not moved when accessed. These settings are global settings that apply to all shadow volumes on a given server. In this way, the desired file types stay in the secondary area after they are moved there.

1.4.4 Move Selected Files

You can use the Shadow Volume Inventory page in Novell Remote Manager for Linux to view statistics on files and usage for the DST shadow volume. At the bottom of the page, use the form to move selected files between the two volumes. This one-time move is not policy based.

1.5 DST Components

There are four main components for Dynamic Storage Technology.

1.5.1 NCP Engine

The NCP Engine provides support for NCP clients and the main file copy engine for Dynamic Storage Technology. It provides the merged view for NCP users and Novell CIFS users. It supports the ShadowFS access for SMB/CIFS users.

1.5.2 Shadow Volume

Shadow Volume allows NCP users and Novell CIFS users to see a merged file-tree view of the primary file tree and shadow file tree.

1.5.3 ShadowFS

The Shadow File System (ShadowFS) works with Novell Samba and FUSE (File Systems in Userspace) to provide a merged view for SMB/CIFS users. It also allows Linux applications (such as Samba Server, PureFTP, and SSH) to see the merged view of the shadow volume.

> **IMPORTANT:** Beginning in OES 2 SP3, Novell CIFS can be used instead Novell Samba. Novell CIFS does not require ShadowFS and FUSE. For information, see "Novell CIFS" on page 45.

ShadowFS uses FUSE to create a local mount point for each DST shadow volume in `/media/shadowfs/shadow_volume_name`. FUSE is an open source software package included in OES 2 Linux that is installed automatically when you install DST.

1.5.4 Policy Engine

The DST policy engine allows you to create, manage, and enforce policies for a shadow. There are two types of policies:

- **Global:** The policy applies to every mounted shadow volume on the server. If global policies are set for a server where volumes are in a clustered pool, these policies must be set on every node in the cluster. For information about setting global policies, see Chapter 3, "Installing Dynamic Storage Technology," on page 31.
- **Volume:** The policy applies only to a specified volume. Volume policies can be used for local or shared volumes. They should be used when volumes are in a clustered pool so that the policy easily follows the volume when the cluster resource fails over. For information, see Chapter 10, "Creating and Managing Policies for Shadow Volumes," on page 101.

1.6 Management Tools

Dynamic Storage Technology shadow volumes, global policies, and shadow volume policies can be managed in Novell Remote Manager for Linux. For information about using Novell Remote Manager, see Chapter 6, "Management Tools for DST," on page 57.

DST shadow volumes can be created and removed with commands by using the NCP Console (NCPCON, `ncpcon(8)`) utility. For information, see Appendix A, "Commands and Utilities for DST," on page 183.

1.7 What's Next

For information about installing NCP Server, Dynamic Storage Technology, and NSS, see Chapter 3, "Installing Dynamic Storage Technology," on page 31.

For information about planning your DST solution, see Chapter 5, "Planning for DST Shadow Volumes and Policies," on page 41.

2 What's New or Changed for Dynamic Storage Technology

This section describes enhancements and additions to the Dynamic Storage Technology for Novell Open Enterprise Server (OES) 2 Linux.

2.1 What's New (May 2013 Patches)

In addition to bug fixes, the following enhancements are available:

- **ShadowFS:** The *Load ShadowFS (enable only if using Samba)* label has been modified to Load *ShadowFS (enable only if using Samba or Linux file access protocols)*. The change was made for clarity; there is no change in functionality.

2.2 What's New (April 2013 Patches)

Upgrade to eDirectory 8.8.7

An upgrade to Novell eDirectory 8.8 SP7 is available in the April 2013 Scheduled Maintenance for OES 2 SP3. For information about the eDirectory upgrade, see TID 7011599 (http://www.novell.com/support/kb/doc.php?id=7011599) in the Novell Knowledgebase.

There will be no further eDirectory 8.8 SP6 patches for the OES platform. Previous patches for Novell eDirectory 8.8 SP6 are available on Novell Patch Finder (http://download.novell.com/patch/finder/#familyId=112&productId=29503).

2.3 What's New (January 2013 Patches)

Upgrade to Novell iManager 2.7.6

The January 2013 Scheduled Maintenance for OES 2 SP3 includes a channel upgrade from Novell iManager 2.7.5 to Novell iManager 2.7.6.

Novell iManager 2.7.6 provides the following enhancements:

- Microsoft Internet Explorer 10 certification in the desktop user interface view on Windows 8 (excluding Windows 8 RT) and Windows Server 2012.
- Apple Safari 6.0 certification on Mac OSX Mountain Lion (version 10.8).
- iManager Workstation certification on Windows 8 Enterprise Edition (32-bit and 64-bit).
- Manager 2.7.6 support for Tomcat 7.0.32. and Java 1.7.0_04 versions.

iManager documentation links in this guide have been updated to reflect this change.

iManager 2.7.6 documentation is available on the Web (https://www.netiq.com/documentation/imanager/). For earlier iManager versions, see "Previous Releases" (https://www.netiq.com/documentation/imanager27/#prev).

Novell Client Support for Windows 8 and Server 2012

The January 2013 Scheduled Maintenance for OES 2 SP3 announces the availability of Novell Client 2 SP3 for Windows with support for:

- Windows 8 (32-bit and 64-bit) excluding Windows 8 RT
- Windows Server 2012 (64-bit)

Novell Client 2 documentation links in this guide have been updated to reflect the release of SP3.

Novell Client 2 SP3 for Windows documentation is available on the Web (http://www.novell.com/documentation/windows_client/). Documentation for earlier versions is available under Previous Releases (http://www.novell.com/documentation/windows_client/#previous).

New Novell Cluster Services Plug-in for iManager 2.7.5 and Later

The Clusters plug-in for Novell iManager 2.7.5 or later was released in OES 11 SP1. It supports the management of OES and NetWare clusters and resources. The availability of different cluster management features depends on the version of Novell Cluster Services and the server platform that are installed on the cluster being managed. A comparison of the old and new interface is available in "What's New (January 2013 Patches)" (http://www.novell.com/documentation/oes2/clus_admin_lx/data/ncs_new_jan2013.html) in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux* (http://www.novell.com/documentation/oes2/clus_admin_lx/data/h4hgu4hs.html).

2.4 What's New (July 2012 Patches)

In addition to bug fixes, the following enhancements or behavior changes are available in the July 2012 Scheduled Maintenance for OES 2 SP3:

- **Subdirectory Restrictions:** The Subdirectory Restrictions filter has been modified as follows:
    - Precede subdirectory paths with a forward slash (/), such as

```
/subdir1/subdir2
```

- In addition to subdirectory paths, the Exclude Subdirectory option allows you to specify a directory name that might exist in multiple places on a volume. You indicate this intended action by specifying only a directory name with no forward slashes, and the directory name must contain at least one wildcard (such as ? or *). All instances of directories that match the specified directory name are excluded from the policy run.

  For example, to exclude all GroupWise archive subdirectories, specify the following directory name with wildcards:

  ```
  of???arc
  ```

For information, see Section 10.1.10, "Subdirectory Restrictions," on page 105.

2.5   What's New (May 2012 Patches)

In addition to bug fixes, the following enhancements are available:

- **Search Pattern:** You can specify file names with spaces in them.
- **ShadowFS:** The *Load ShadowFS now and at boot time* option has been renamed as *Load ShadowFS (enable only if using Samba)*.

2.6   What's New for OES 2 SP3

In addition to bug fixes, the following capabilities for Dynamic Storage Technology in OES 2 SP3 have been added since the OES 2 SP2 release.

- Section 2.6.1, "Confirming a Policy Deletion," on page 27
- Section 2.6.2, "Stopping a Running Policy," on page 27
- Section 2.6.3, "Using Encrypted NSS Volumes," on page 27
- Section 2.6.4, "Using Novell CIFS," on page 28
- Section 2.6.5, "Using a Remote Secondary NSS Volume in a DST Shadow Volume," on page 28

2.6.1   Confirming a Policy Deletion

When you delete a policy, you are now prompted to confirm the deletion.

2.6.2   Stopping a Running Policy

A option was added to the Dynamic Storage Technology Options page that allows you to stop policies that are currently in progress. For information, see Section 10.7, "Stopping a Running Policy," on page 113.

2.6.3   Using Encrypted NSS Volumes

You can use Encrypted NSS volumes to form a DST shadow volume pair. For information, see "Encryption" in Section 5.4.2, "DST Support for NSS Features and Actions," on page 50.

2.6.4 Using Novell CIFS

Novell CIFS provides a merged view of DST shadow volumes that are built with Novell Storage Services (NSS) volumes. It works with local or remote secondary volumes. For information, see "Novell CIFS" on page 45.

2.6.5 Using a Remote Secondary NSS Volume in a DST Shadow Volume

A technology preview is available for Dynamic Storage Technology that allows you to use a remote NSS volume as the secondary volume. The merged view is supported for both NCP users and Novell CIFS users. The Novell Client 2.0 (or later) for Linux is used to mount the remote NSS volume to the OES 2 SP3 Linux server where DST is running.

IMPORTANT: The remote secondary capability for DST shadow volumes is presented as a technology preview. It is not recommended for a production environment.

For information, see Section C.2, "Requirements for Using a Remote Secondary NSS Volume," on page 201.

2.7 What's New for OES 2 SP2

In addition to bug fixes, the following capabilities for Dynamic Storage Technology in OES 2 SP2 have been added since the OES 2 SP1 release.

- Section 2.7.1, "Specifying Multiple Extensions in a Policy," on page 28
- Section 2.7.2, "Specifying Multiple Paths to Either Include or Exclude in a Policy," on page 28

2.7.1 Specifying Multiple Extensions in a Policy

Beginning in OES 2 SP2 Linux, you can specify multiple extensions as Search Pattern options for a given policy. Previously, only one file extension was allowed, requiring multiple policies for each desired extension.

For information, see "Search Pattern" on page 106.

2.7.2 Specifying Multiple Paths to Either Include or Exclude in a Policy

Beginning in OES 2 SP2 Linux, the *Subdirectory Restrictions* filter allows multiple paths to be specified for being included or excluded in a policy when it runs. You can either specify included paths or excluded paths in a given policy, but not both. Previously, only one path was allowed to be included or excluded in a given policy.

For information, see Section 10.1.10, "Subdirectory Restrictions," on page 105.

2.8　What's New for OES 2 SP1

In addition to bug fixes, the following capability for Dynamic Storage Technology in OES 2 SP1 has been added since the initial release of OES 2:

2.8.1　iSCSI Block Storage Devices

DST supports using iSCSI block storage devices running on OES servers for the primary and secondary storage areas for NSS volumes. They can also be used for clustered DST shadow volume pairs. For guidelines, see Section 5.1.2, "iSCSI Block Storage Devices," on page 42.

2.9　What's New for OES 2

This is an initial release of Dynamic Storage Technology 1.0.

3 Installing Dynamic Storage Technology

This section describes installation requirements and how to install Dynamic Storage Technology on a Novell Open Enterprise Server (OES) 2 Linux server.

3.1 Installation Requirements for Dynamic Storage Technology

Make sure your system satisfies the required software and configuration settings that are specified in this section.

3.1.1 Novell Open Enterprise Server 2 Linux

Dynamic Storage Technology runs on OES 2 Linux (or later) servers. DST supports 32-bit and 64-bit processors. For information about installing and configuring OES 2 Linux, see the *OES 2 SP3: Installation Guide*.

3.1.2 NCP Server and Dynamic Storage Technology

Dynamic Storage Technology is a component of the NetWare Core Protocol (NCP) Server. NCP Server for Linux provides the NCP services for the shadow volume. NCP Server must be installed and running in order for DST to work. NCP Server also provides a merged view of the data for NCP users and applications.

DST is automatically enabled when NCP Server is running and enabled, even if there are no shadow volume pairs currently defined. There is no way to separately turn DST on or off in Novell Remote Manager for Linux or in the YaST Runlevel Editor.

For information about managing NCP Server for Linux, see the *OES 2 SP3: NCP Server for Linux Administration Guide*.

3.1.3 Novell Storage Services

Dynamic Storage Technology supports only Novell Storage Services (NSS) volumes in shadow volumes. You must install Novell Storage Services and any other OES 2 services that it requires. For information, see "Installing and Configuring Novell Storage Services" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

IMPORTANT: Some restrictions apply when using NSS volumes in a DST shadow volume. For information, see Section 5.4, "Using NSS Volumes in DST Shadow Volumes," on page 48.

3.1.4 Novell eDirectory 8.8.2 or Later

Dynamic Storage Technology requires that access to data be restricted to users with User objects defined in Novell eDirectory 8.8.2 or later. For information about configuring eDirectory and users, see the *Novell eDirectory 8.8 SP7 Administration Guide*.

IMPORTANT: All users of data on the shadow volume pair must be eDirectory users. In OES 2 Linux, the server's `root` user is the only local user who can access data without authenticating in eDirectory.

3.1.5 Novell CIFS

In OES 2 SP3 Linux (or later), Novell CIFS is supported to give CIFS users access to the data on DST volumes that are built with NSS volumes. CIFS users see a merged view of the data by accessing a CIFS share on the primary volume. For information about configuring and managing Novell CIFS, see the *OES 2 SP3: Novell CIFS for Linux Administration Guide*. For planning information, see "Novell CIFS" on page 45.

Novell CIFS is supported as an alternative to the Novell Samba solution. Novell CIFS does not require ShadowFS, FUSE, or LUM.

3.1.6 Novell Samba with ShadowFS, FUSE, and LUM

Novell Samba is supported as an alternative to Novell CIFS to give SMB/CIFS users access to the data on DST volumes.

The SMB/CIFS users and the Linux Samba service must be enabled with Linux User Management (LUM).

The merged view for SMB/CIFS is provided by the Shadow File System (ShadowFS) and FUSE (File System in Userspace). These components are installed automatically when you install NCP Server and Dynamic Storage Technology. For information, see Chapter 12, "Using ShadowFS to Provide a Merged View for Novell Samba Users," on page 129.

3.1.7 Linux User Management

Linux User Management is selected and installed automatically when you install NCP Server and Dynamic Storage Technology. LUM is required if you use Novell Samba with DST volumes. For information about how to configure users and services for LUM, see the *OES 2 SP3: Novell Linux User Management Administration Guide*.

3.1.8 Novell Cluster Services for Linux

NCP Server and Dynamic Storage Technology support the sharing of shadow volumes in clusters with Novell Cluster Services for OES 2 Linux or later.

NCP Server and DST are not cluster-aware. They must be installed and configured on each OES 2 Linux node in the cluster where you plan to fail over DST shadow volumes.

For information about installing Novell Cluster Services, see "Planning for Novell Cluster Services" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

For information about managing cluster resources, see "Configuring and Managing Cluster Resources" the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

For information about configuring shadow volumes in cluster resources, see Chapter 13, "Configuring DST Shadow Volume Pairs with Novell Cluster Services," on page 139.

3.1.9 Novell Remote Manager for Linux

Novell Remote Manager for Linux is required for managing NCP Server services and Dynamic Storage Technology. It is selected and installed by default when you install NCP Server and Dynamic Storage Technology.

For information about managing Novell Remote Manager and using its other features, see the *OES 2 SP3: Novell Remote Manager for Linux Administration Guide*. For information about management options for DST, see Section 6.1, "Dynamic Storage Technology Plug-In for Novell Remote Manager for Linux," on page 57.

3.1.10 Novell iManager 2.7.4 for Linux

Novell iManager 2.7.4 for Linux is required for managing eDirectory users, Samba services, Novell CIFS services, Linux User Management, Novell Storage Services, and Novell Cluster Services for Linux. It is not necessary to install iManager on every server, but it must be installed somewhere in the same eDirectory tree. For information about installing and using Novell iManager, see the *Novell iManager 2.7.6 Administration Guide*.

You use the Storage plug-in to share devices and to create and manage NSS pools and volumes. For information, see "Storage Plug-In Quick Reference" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

You use the Clusters plug-in for Novell iManager to manage the DST shadow volume cluster resource, load script, and unload script. For information, see "Configuring and Managing Cluster Resources" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

3.1.11 OpenWBEM and CIMOM

OpenWBEM is a PAM-enabled Linux utility that must be enabled and running on the OES 2 Linux server when you are managing services with Novell Remote Manager for Linux and Novell iManager. During the install, ensure that you enable OpenWBEM (the default) when you configure Linux services. For information, see "Services in OES 2 That Require LUM-Enabled Access" in the *OES 2 SP3: Planning and Implementation Guide*.

Port 5989 is the default setting for secure HTTP (HTTPS) communications. If you are using a firewall, the port must be opened for CIMOM communications.

IMPORTANT: If you receive file protocol errors, it might be because WBEM is not running.

The following table contains some useful commands for resolving CIMOM issues:

To perform this task	At a terminal console prompt, enter as the `root` user
To check openWBEM status	`rcowcimomd status`
To restart openWBEM	`rcowcimomd restart`

3.1.12 Other OES 2 Linux Services

Ensure that you install and configure additional OES 2 Linux services that might be required by each of the other services mentioned in this section. Refer to the individual guides for those services for information about how to install and manage them.

3.2 Installing NCP Server and Dynamic Storage Technology

NCP Server for Linux and Dynamic Storage Technology can be installed during the OES 2 Linux installation, or on an existing server. Before you set up DST volumes on the server, ensure that you configure the DST global policies.

- Section 3.2.1, "Installing on a New OES 2 Linux Server," on page 34
- Section 3.2.2, "Installing on an Existing OES 2 Linux Server," on page 36

3.2.1 Installing on a New OES 2 Linux Server

NCP Server for Linux and Dynamic Storage Technology can be installed during the OES 2 Linux installation. For general installation instructions, see the *OES 2 SP3: Installation Guide*.

1 During the YaST install, on the *Install Settings* page, click *Software* to view details.

2 Select *Novell NCP Server / Dynamic Storage Technology* from the *OES Services* options.

When you select *Novell NCP Server / Dynamic Storage Technology*, the following additional *OES Services* options are automatically selected:

- *Novell Backup / Storage Management Services*
- *Novell eDirectory*
- *Novell Linux User Management*
- *Novell Remote Manager (NRM) for Linux*
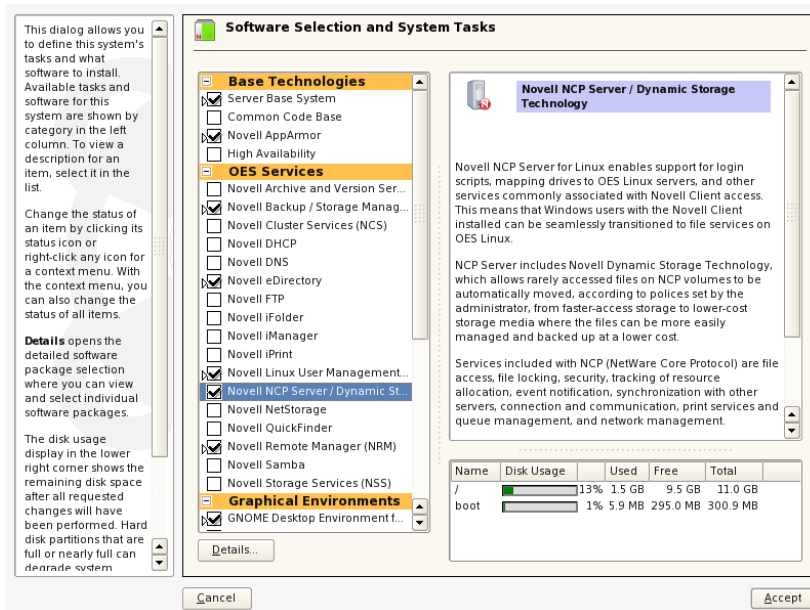
3 Select *Novell Storage Services* from the *OES Services* options.

IMPORTANT: DST shadow volumes are supported only for Novell Storage Services volumes.

4 (Optional) Select *Novell iManager* from the *OES Services* options.

You must install Novell iManager somewhere in your network, but it is not necessary to install it on every server.

5 (Optional) If you plan to configure shared DST shadow volumes in a cluster, select *Novell Cluster Services (NCS)* from the *OES Services* options.

For detailed information about configuring cluster settings after the install for Novell Cluster Services for Linux, see "Configuring Novell Cluster Services" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

6 (Optional) If you plan to provide access to DST shadow volumes for CIFS users, select one of the following from the *OES Services* options:

* *Novell CIFS* (supported for OES 2 SP3 Linux and later)
* *Novell Samba*

7 Click *Accept* to continue with the installation.

This dialog allows you to define this system's tasks and what software to install. Available tasks and software for this system are shown by category in the left column. To view a description for an item, select it in the list.

Change the status of an item by clicking its status icon or right-click any icon for a context menu. With the context menu, you can also change the status of all items.

Details opens the detailed software package selection where you can view and select individual software packages.

The disk usage display in the lower right corner shows the remaining disk space after all requested changes will have been performed. Hard disk partitions that are full or nearly full can degrade system

Software Selection and System Tasks

Base Technologies
- ☑ Server Base System
- ☐ Common Code Base
- ☑ Novell AppArmor
- ☐ High Availability

OES Services
- ☐ Novell Archive and Version Ser...
- ☑ Novell Backup / Storage Manag...
- ☐ Novell Cluster Services (NCS)
- ☐ Novell DHCP
- ☐ Novell DNS
- ☑ Novell eDirectory
- ☐ Novell FTP
- ☐ Novell iFolder
- ☑ Novell iManager
- ☐ Novell iPrint
- ☑ Novell Linux User Management...
- ☑ Novell NCP Server / Dynamic St...
- ☐ Novell NetStorage
- ☐ Novell QuickFinder
- ☑ Novell Remote Manager (NRM)
- ☐ Novell Samba
- ☑ Novell Storage Services (NSS)

Graphical Environments
- ☑ GNOME Desktop Environment f...

Details...

Novell NCP Server / Dynamic Storage Technology

Novell NCP Server for Linux enables support for login scripts, mapping drives to OES Linux servers, and other services commonly associated with Novell Client access. This means that Windows users with the Novell Client installed can be seamlessly transitioned to file services on OES Linux.

NCP Server includes Novell Dynamic Storage Technology, which allows rarely accessed files on NCP volumes to be automatically moved, according to polices set by the administrator, from faster-access storage to lower-cost storage media where the files can be more easily managed and backed up at a lower cost.

Services included with NCP (NetWare Core Protocol) are file access, file locking, security, tracking of resource allocation, event notification, synchronization with other servers, connection and communication, print services and queue management, and network management.

Name	Disk Usage	Used	Free	Total
/	8%	1.6 GB	17.1 GB	18.7 GB

Cancel   Accept

8 After you have installed and configured the server, continue with .

3.2.2   Installing on an Existing OES 2 Linux Server

You can install NCP Server and Dynamic Storage Technology at any time after the initial OES 2 Linux install by using *YaST > Open Enterprise Server > OES Install and Configuration*. For general instructions for installing and configuring OES 2 components on an existing OES 2 Linux server, see "Installing or Configuring OES 2 SP3 on an Existing Server" in the *OES 2 SP3: Installation Guide*.

1 Log in to the server as the root user, then launch YaST.

2 In YaST, select *Open Enterprise Server > OES Install and Configuration*.

3 On the Software Selection page under *OES Services*, select *Novell NCP Server / Dynamic Storage Technology* and any other compatible OES components that you want to install.

IMPORTANT: Services that are already installed are indicated by a blue check mark in the status check box next to the service. If a service is already installed, do not select it again.

When you select *Novell NCP Server / Dynamic Storage Technology*, the following additional *OES Services* options are automatically selected:

- ◆ *Novell Backup / Storage Management Services*
- ◆ *Novell eDirectory*
- ◆ *Novell Linux User Management*
- ◆ *Novell Remote Manager (NRM) for Linux*

4 If it is not already installed, select *Novell Storage Services* from the *OES Services* options.

5 (Optional) If it is not already installed, select *Novell iManager* from the *OES Services* options.

You must install Novell iManager somewhere in your network, but it is not necessary to install it on every server.

6 (Optional) If it is not already installed, and if you plan to configure shared DST shadow volumes on a cluster node, select *Novell Cluster Services (NCS)* from the *OES Services* options.

For detailed information about configuring cluster settings after the install for Novell Cluster Services for Linux, see "Configuring Novell Cluster Services" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

7 (Optional) If you plan to provide access to DST shadow volumes for CIFS users, select one (not both) of the following protocol solutions from the *OES Services* options if it is not already installed:

   ◆ *Novell CIFS* (supported for OES 2 SP3 Linux and later)

   ◆ *Novell Samba*

8 Click *Accept* to continue with the installation.

9 After you have installed and configured the server, continue with Section 3.3, "Configuring Global Policies for DST," on page 37.

3.3 Configuring Global Policies for DST

After DST has been installed on the server, configure the global policies for DST. Global policies apply to all DST shadow volumes on the server.

In a cluster, the global policies should be configured with the same settings on all nodes where you plan to run a DST shadow volume cluster resource. Whenever you modify global policies on a given node in the cluster, you must make those same changes on the other nodes.

For information about setting DST global policies, see the following:

   ◆ Section 8.1, "Replicating Branches of the Primary File Tree in the Secondary File Tree," on page 65

   ◆ Section 8.2, "Shifting Files from the Secondary File Tree to the Primary File Tree," on page 66

   ◆ Section 8.3, "Resolving Instances of Duplicate Files," on page 70

   ◆ Section 8.4, "Loading ShadowFS," on page 75

3.4 Installing DST on Nodes in a Novell Cluster Services for Linux Cluster

NCP Server and Dynamic Storage Technology software are not cluster aware. They must be installed on every OES 2 Linux node in the cluster where you plan to migrate or fail over the cluster resource that contains shadow volumes. You do not cluster NCP Server or DST services.

1 For each node in the OES 2 Linux cluster, install NCP Server and Dynamic Storage Technology along with Novell Cluster Services for Linux.

For information, see Section 3.2, "Installing NCP Server and Dynamic Storage Technology," on page 34.

2 On each node in the OES 2 Linux cluster, configure the DST global policies with the same settings. Global policies apply to all DST shadow volumes on the server.

For information, see Chapter 8, "Configuring DST Global Policies," on page 65.

IMPORTANT: Whenever you modify global policies on a given node in the cluster, you must make those same changes on the other nodes.

3 Set up the shadow volume cluster resource on the first node in the cluster by using a method described in Chapter 13, "Configuring DST Shadow Volume Pairs with Novell Cluster Services," on page 139.

4 Set up shadow volume policies for the shadow volume as described in Chapter 10, "Creating and Managing Policies for Shadow Volumes," on page 101.

If you set up policies by using the *All Volumes* option, you must copy the policy information to all nodes. For information, see "All-Shadow-Volumes Policies" on page 146.

4 Using Dynamic Storage Technology in a Virtual Environment

Dynamic Storage Technology (DST) for Novell Open Enterprise Server (OES) 2 Linux works similarly on a native hardware environment and on a virtual machine, with the following caveats:

- DST supports up to 16 shadow volumes and up to 16 ShadowFS volumes in a virtualized guest server environment.
- DST is not supported for use in the virtualization host server environment.

Xen limits for the number of devices assigned to a virtual machine:

- **Para-virtualized:** 16 devices
- **Fully virtualized:** 4 devices

To get started with virtualization, see "Introduction to Xen Virtualization" (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/sec_xen_basics.html) in the *Virtualization with Xen* (http://www.novell.com/documentation/sles10/book_virtualization_xen/data/book_virtualization_xen.html) guide.

For information on setting up virtualized OES 2 Linux, see "Installing, Upgrading, or Updating OES on a Xen-based VM" in the *OES 2 SP3: Installation Guide* guide.

5 Planning for DST Shadow Volumes and Policies

This section describes guidelines for using Dynamic Storage Technology (DST) on Novell Open Enterprise Server (OES) 2 for Linux servers.

For installation requirements, see Section 3.1, "Installation Requirements for Dynamic Storage Technology," on page 31.

5.1 Planning to Create DST Shadow Volumes

5.1.1 Storage Devices

Volumes in a shadow volume pair can reside on any device that is seen as local to the DST server, such as direct-attached storage and Fibre Channel SAN devices. For information about using iSCSI SAN devices, see Section 5.1.2, "iSCSI Block Storage Devices," on page 42.

Block storage devices used for the primary and secondary storage can have different performance characteristics. Typically, the secondary storage area is slower and less expensive.

In the OES 2 SP3 technology preview, DST supports using a remote NSS volume as the secondary volume in the shadow volume pair. For information, see "Requirements for Using a Remote Secondary NSS Volume" on page 201.

5.1.2 iSCSI Block Storage Devices

Dynamic Storage Technology supports using target iSCSI block storage devices to store the primary and secondary volumes in a shadow volume pair. Any iSCSI block storage device should work in a shadow volume pair, if it is compatible with the Linux iSCSI initiator software running on the OES 2 Linux server where you create and manage the shadow volume pair. However, only iSCSI targets running on the following OES servers (or later versions) have been tested and are supported:

- OES 2 Linux or later
- NetWare 6.5 SP7 or later
- OES 1 SP2 Linux

IMPORTANT: Third-party iSCSI solutions have not been tested, so they are not supported.

For example, Figure 5-1 illustrates a NetWare 6.5 SP7 (or later) server as the iSCSI target server that connects to the OES 2 Linux server via the Linux iSCSI initiator software.

Figure 5-1   *NetWare 6.5 to OES 2 Linux*
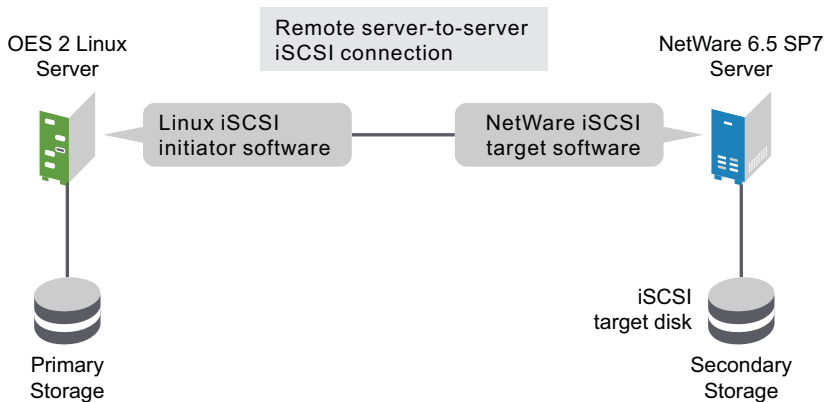
For information about setting up iSCSI target devices on OES 2 Linux servers, see the following:

- "Setting Up an iSCSI Target" (http://www.novell.com/documentation/sles10/book_sle_reference/data/sec_inst_system_iscsi_target.html) in the *SLES 10 Installation and Administration Guide* (http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html)
- "Configuring iSCSI Targets" in the *NW 6.5 SP8: iSCSI 1.1.3 Administration Guide*

The iSCSI targets must be connected to the Linux iSCSI initiator software running on the OES 2 Linux server where you are creating DST shadow volumes. For information, see the following resources:

- "Configuring iSCSI Initiator" (http://www.novell.com/documentation/sles10/book_sle_reference/data/sec_inst_system_iscsi_initiator.html) in the *SLES 10 Installation and Administration Guide* (http://www.novell.com/documentation/sles10/book_sle_reference/data/book_sle_reference.html)
- "Accessing iSCSI Targets on NetWare Servers from Linux Initiators" in the *NW 6.5 SP8: iSCSI 1.1.3 Administration Guide*

IMPORTANT: OES 2 Linux does not support running iSCSI target software and initiator software on the same server.

5.1.3 Remote Secondary Volumes (Technology Preview)

In the OES 2 SP3 technology preview, you can use a remote NSS volume as the secondary volume in a shadow volume pair. The merged view is supported for NCP users and Novell CIFS users. Novell Samba (with ShadowFS and FUSE) has not been tested in this configuration.

For information about using remote secondary NSS volumes, see:

- Appendix C, "Technology Preview: Creating and Managing DST Shadow Volumes with Remote Secondary NSS Volumes," on page 199
- Appendix D, "Technology Preview: Using DST Shadow Volumes with Remote Secondary NSS Volumes and Novell Cluster Services," on page 211

IMPORTANT: Remote secondary NSS volumes are not supported for other server-to-server connections such as for the NFS and Linux Samba.

5.1.4 File Systems

Dynamic Storage Technology supports using two Novell Storage Services (NSS) volumes in a shadow volume pair. For more information, see Section 5.4, "Using NSS Volumes in DST Shadow Volumes," on page 48.

IMPORTANT: Mixing file systems for the primary and secondary areas in a given DST shadow volume pair is not supported.

5.2 Providing a Merged View for Users

Consider the guidelines in this section when planning how to provide access to the merged view of data in the DST shadow volume.

- Section 5.2.1, "User Access and Authentication," on page 43
- Section 5.2.2, "File Access Protocols," on page 44
- Section 5.2.3, "ShadowFS and FUSE," on page 46

5.2.1 User Access and Authentication

Users access the merged view of the data in the DST shadow volume by connecting to the primary volume. Users should not be allowed to connect directly to the secondary volume.

All file access is controlled with the Novell Trustee Model, which requires users to authenticate via Novell eDirectory 8.8.2 or later. You can use the Novell Client or similar NCP client tools to set trustees and file system rights in the merged file view by connecting to the primary volume.

All users (except the `root` user) of the shadow volume must have User objects defined in eDirectory. For information about configuring eDirectory users, see the *Novell eDirectory 8.8 SP7 Administration Guide*. The `root` user of the OES 2 Linux server is the only local user who has direct access to the volumes.

5.2.2 File Access Protocols

A merged user view of the file system is available for both NCP and CIFS users. The CIFS access can be set up by using either Novell CIFS or Novell Samba; OES does not support using both CIFS user access solutions on the same server. NCP Server is required to be installed and running even if all users access data via Novell CIFS or Novell Samba.

This section describes the requirements and guidelines for file access protocols:

- "Performance for File Access Protocols" on page 44
- "Cross-Protocol File Locking" on page 44
- "NCP" on page 44
- "Novell CIFS" on page 45
- "Novell Samba with ShadowFS and FUSE" on page 46
- "Novell AFP (Not Supported)" on page 46
- "Other Linux Protocols (Not Supported)" on page 46

Performance for File Access Protocols

Using DST affects the file access performance, depending on the file access protocol being used, as shown in Table 5-1.

Table 5-1 *Performance for File Access Protocols Used with DST Volumes*

User Access	Aggregate Performance
Novell Client users	Performance is reduced by less than 10%.
Novell CIFS users	Performance is reduced by about 25%.
SMB/CIFS users (requires Novell Samba, FUSE, ShadowFS, and Linux-enabling of users with Linux User Management)	Performance is reduced by up to 48%.

Cross-Protocol File Locking

When users access the files via multiple protocols, you should enable the NCP Server Cross-Protocol File Locks option to protect against data corruption. For information, see "Configuring Cross-Protocol File Locks for NCP Server" in the *OES 2 SP3: NCP Server for Linux Administration Guide*

NCP

The DST Shadow Volumes engine supports file access for NCP users. Users access data via an NCP share on the primary storage location, by using the Novell Client or other NCP clients. For information about configuring NCP Server for the OES 2 Linux server, see the *OES 2 SP3: NCP Server for Linux Administration Guide*.

Novell Client: See the following resources for the latest release of the Novell Client, which provides NCP access for users on Linux and Windows clients:

- Novell Client 2.0 SP3 for Linux (http://www.novell.com/documentation/linux_client/index.html)

- Novell Client 1.0 SP1 for Windows Vista, Windows 7, and Windows Server 2008 (http://www.novell.com/documentation/vista_client/index.html)
- Novell Client 4.91 SP5 for Windows XP/2003 (http://www.novell.com/documentation/noclienu/index.html)

Only NCP client versions that are configured to receive broadcast messages are eligible to receive the duplicate file conflict messages. For information, see Section 8.3.3, "Enabling or Disabling Broadcast Messages for Duplicate Files Conflicts," on page 74.

NetStorage: NetStorage for Linux has limited use for accessing files on shadow volumes. NetStorage presents a merged view of the data, and the user can see, read, and write files. However, certain management functions (such as getting file properties, setting trustees, and salvaging files) work only if the files are on the primary volume. The user will find that the commands work for some files but not others because they are not aware of where the file is physically stored. For information about using NetStorage, see *OES 2 SP3: NetStorage Administration Guide*.

Novell CIFS

Beginning in OES 2 SP3, Novell CIFS supports using NSS volumes in a DST shadow volume configuration. It supports the following DST features:

- **Merged View:** Novell CIFS works with NCP Server to provide a merged view of the two NSS volumes. CIFS users can access data on both volumes via a Novell CIFS share on the primary NSS volume.
- **Duplicate Files:** CIFS can handle duplicate files, but it does not support the broadcast message notification via NCP. It shows the instance of the file on the primary volume to users. The administrator or user can rename the file so that the secondary instance of the file is again visible. The user can then determine which instance to delete.

  If the global policy is set to hide duplicate files, CIFS moves the files on the secondary volume to the /._DUPLICATE_FILES folder where the administrator can access them for recovery, if necessary.
- **Global DST Policies:** When users access or modify files, CIFS honors the global DST policies for moving files from the secondary volume to the primary volume.

Setting up Novell CIFS for use with a DST shadow volume is similar to setting up CIFS for an NSS volume. You create the CIFS share on the primary volume, but not on the secondary volume. Enable the cross-protocol file locking parameter for NCP Server on the DST server.

Novell CIFS features should work as expected, including cross-protocol file locking. The key difference is that users access the merged view of data in both volumes via the CIFS share on the primary NSS volume. The users do not know that the data is stored on two different volumes.

For information, see the following:

- *OES 2 SP3: Novell CIFS for Linux Administration Guide*
- "Configuring Cross-Protocol File Locks for NCP Server" in the *OES 2 SP3: NCP Server for Linux Administration Guide*

Consider the following requirements when configuring Novell CIFS for use with DST volumes:

- Novell CIFS supports only NSS volumes on Linux. Thus, Novell CIFS can be used only with DST volumes built on NSS volumes.
- CIFS users access a merged view of the DST shadow volume by using a Novell CIFS share on the primary volume. Create a CIFS share on the Primary volume only; delete the share on the secondary (or do not give users rights to access the secondary share).

- ◆ Novell CIFS users don't see broadcast messages if the Broadcast Messages for Duplicate Files Conflicts feature is enabled for Duplicate Files errors. This DST option works only for Novell Client users as described in Section 8.3.3, "Enabling or Disabling Broadcast Messages for Duplicate Files Conflicts," on page 74. If you have only Novell CIFS users and no NCP users, you might as well disable the broadcasting option.

- ◆ If you use Novell CIFS with a DST volume in a cluster, you need to add the Novell CIFS lines in the load/unload scripts for the DST cluster resource. The differences are described in Chapter 13, "Configuring DST Shadow Volume Pairs with Novell Cluster Services," on page 139.

- ◆ You cannot configure Novell CIFS and the SMB/CIFS setup on the same server. This limitation is derived from the requirement that Novell Samba and Novell CIFS cannot be installed on the same server, and is unrelated to DST.

Novell Samba with ShadowFS and FUSE

Novell Samba is supported for providing SMB/CIFS user access to shadow volumes. This Samba version is the standard Linux Samba that has been integrated with eDirectory. For information, see the *OES2 SP3: Samba Administration Guide*.

To provide a merged view for SMB/CIFS users, you must also set up ShadowFS (Shadow File System) and FUSE (Filesystem in Userspace). See Chapter 12, "Using ShadowFS to Provide a Merged View for Novell Samba Users," on page 129 for installation and configuration requirements.

SMB/CIFS users must be Linux-enabled users of the OES 2 Linux server. The Linux Samba service must also be LUM enabled. For information, see the *OES 2 SP3: Novell Linux User Management Administration Guide*.

Enable the cross-protocol file locking parameter for NCP Server. For information, see "Configuring Cross-Protocol File Locks for NCP Server" in the *OES 2 SP3: NCP Server for Linux Administration Guide*.

Novell AFP (Not Supported)

Novell AFP (Apple Filing Protocol) does not support DST shadow volumes. AFP users are able to see only the data that is on the primary volume. Do not create AFP shares on the primary or secondary volumes that are used in a DST shadow volume.

Other Linux Protocols (Not Supported)

User access to shadow volumes via other native Linux protocols (such as HTTP, FTP, NFS, and others) is not supported.

5.2.3 ShadowFS and FUSE

The Shadow File System (ShadowFS) is used to provide a merged view of the shadow volume tree when you use Novell Samba for user file access. ShadowFS must be running in order for the SMB/CIFS users to access the data.

When ShadowFS is running, it automatically creates a shadow file system directory for each of the shadow volumes, not just the ones where you plan to allow SMB/CIFS access. SMB/CIFS users see only those volumes where they have file system trustee rights.

ShadowFS requires FUSE (File System in Userspace) to be installed and running. For information, see Chapter 12, "Using ShadowFS to Provide a Merged View for Novell Samba Users," on page 129.

5.3 Using DST Shadow Volumes

Consider the guidelines in this section when working with DST shadow volumes.

5.3.1 Number of Shadow Volumes per Server

DST supports the following number of DST shadow volume pairs per DST server:

- **Physical server:** 32
- **Virtual server:** 16

IMPORTANT: This constraint is imposed because of a known defect in FUSE (File System in Userspace).

5.3.2 Data Volumes

DST shadow volumes are intended for use with data volumes that contain unstructured data. Consider the following guidelines for choosing which volumes to use with DST:

- Do not put system files and application files on DST shadow volumes.
- Do not create a DST shadow volume for the _ADMIN volume.
- If the volume contains database files. rebuild situations might occur because of the additional latency related to the DST handling, or if the secondary storage area becomes unavailable for any reason.

  Policies should exclude directories that contain databases such as those for Novell GroupWise and MySQL. You can alternatively create policies in such a way that they do not affect database files.

5.3.3 Files and Folders

- New files are automatically created on the primary volume.
- While a file is moved from one area to the other, the file is locked so that clients cannot access it during relocation.
- A policy cannot move a file between the areas if the file is open.

  When DST enforces policies or moves files, the relocation request fails if a user has the file open; only files that are not in use can be moved.

- If you rename a folder through the merged view, the name is changed on the instance of the folder in the primary location and the secondary location.

- Always use the merged view when renaming or modifying files. Do not rename or modify files or directories by directly accessing them on the secondary location.

  If you rename a folder by directly accessing the folder on the secondary location, the instance of the folder on the primary location is not renamed or deleted. Instead, an instance is created on the primary location for the newly renamed folder. The renamed folder contains the files that were stored in it when it was renamed. The files appear to have disappeared from the original instance of the folder.

5.3.4 File System Trustees and Rights

When the NCP protocol is used in conjunction with the NSS file system, all native NCP functionality (security, rights, trustees, salvage, directory quotas, and so on) is preserved in a DST environment. No functionality is lost, and no management patterns are changed.

When you use Novell CIFS or Novell Samba, all native CIFS functionality for security, rights, and so on is preserved in a DST environment. The conversion of CIFS ACLs (access control lists) to NSS ACLs based on the POSIX definitions is based on code resident in Samba and is not supported for modification by Novell.

IMPORTANT: The CIFS support of ACLs is offered as-is, and is not modified to take advantage of the expanded management features of NSS file systems.

5.3.5 File System Management Utilities

You can continue using existing file management utilities that currently execute successfully against the designated file systems. DST is transparent to this operation. All file management operations currently available to NSS users through Novell iManager 2.7, NSSMU, and Novell Remote Manager for Linux function transparently for shadow volumes. File operations and the location of the file are transparent to the NCP and CIFS clients.

5.4 Using NSS Volumes in DST Shadow Volumes

Dynamic Storage Technology supports shadow volumes created with Novell Storage Services volumes. Consider the guidelines and caveats in this section when planning your shadow volume solution.

5.4.1 DST Support for NSS Volume Attributes

Make sure you enable the same NSS volume attributes on both volumes in the shadow relationship to ensure a consistent user experience. For example, if Salvage is enabled for the primary volume but not for the secondary volume, files that are deleted when they reside on the secondary volume are purged immediately, and are not available for salvage.

Table 5-2 describes which NSS volume attributes are supported for use with Dynamic Storage Technology, and any caveats to consider when using them. For information about the volume attributes, see "Volume Attributes" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

Table 5-2 *DST Support for NSS Volume Attributes*

NSS Volume Attribute	Supported	Caveats
Allow mount point to be renamed	No	DST does not track the renaming of NSS volumes or their mount points. Before you rename or modify the mount point for an NSS volume, you must remove the shadow volume definition. Afterwards, you can re-create the shadow volume.
Backup	Yes	The Linux file system sees both volumes, so you back up each volume separately.
Compression	Yes	You can set compression on one or both volumes. Compressed files are uncompressed when they are moved from the primary volume to secondary volume, and vice versa. In order for the move to occur, there must be sufficient space on the source volume to allow both the uncompressed and compressed copies of the file to coexist until the move is completed. There must also be sufficient space on the destination volume for the uncompressed file to be stored. The file is re-compressed according to the compression schedule and settings in the destination volume.
Data Shredding	Yes	For security compliance reasons, you should set this attribute on both volumes if you use it.
Directory Quotas	Yes	Set a directory quota for a directory only on the primary volume. For more information, see Section 5.7, "Using NSS Quotas on DST Shadow Volumes," on page 52.
File-level Snapshot	Yes	No known issues.
Flush Files Immediately	Yes	No known issues.
Lookup Namespace	Yes	In OES 2 SP1 and later, the default Lookup Namespace for NSS on Linux is Long, which treats file names as case insensitive. In prior versions, the default name space is UNIX. Using the Long name space helps improve performance because NetWare and Windows treat file names as case insensitive. This is especially important when files are accessed through the SMB/CIFS protocol.
Migration (to near-line HSM storage)	No	DST should not be used in combination with HSM storage solutions.

NSS Volume Attribute	Supported	Caveats
Modified File List (Use Event File List APIs instead.)	No	By default, modified files are moved back to the primary location. If you disable the Shift Modified Files parameter, modified files might also be located on the secondary location. Modified File List is rarely used. It has been replaced by the Event File List APIs that provide more information than the Modified File List. For information, see "Using the Event File List to Refine the Backup" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.
Salvage	Yes	Deleted files on a NSS volume that are salvageable remain salvageable after that volume is used in a shadow volume pair. Duplicate deleted folders might be presented when using Salvage (undelete) and Purge options for folders. You must restore the folders in order to see which one contains the deleted files (on the primary volume), and which is empty (on the secondary volume). NetStorage does not see the deleted files that are available for salvage on the secondary volume.
User Space Quotas	Yes	Set up the user space quotas separately on each of the volumes. For more information, see Section 5.7, "Using NSS Quotas on DST Shadow Volumes," on page 52.
User-level Transaction Model	No	NSS does not support the NetWare Transaction Tracking System for NSS volumes on Linux.

5.4.2 DST Support for NSS Features and Actions

Table 5-3 describes caveats for using the NSS volume features and actions when working with DST shadow volumes.

Table 5-3   *Caveats for NSS Features and Actions*

NSS Feature	Supported	Caveats
Novell Archive and Version Services	Yes	File versions can be archived only for files located on the primary volume of the DST shadow volume. You cannot set up archive jobs for the secondary volume.
Novell Distributed File Services	Yes	Some limitations apply. For information, see Section 5.9, "Using Novell Distributed File Services with DST Shadow Volumes," on page 53.
Encryption	Yes	Beginning in OES 2 SP3, using encrypted NSS volumes is supported for DST shadow volume pairs. For information, see Section 5.6, "Using NSS Encrypted Volumes in a DST Shadow Volume," on page 52.
Hard links	No	DST does not support hard links on NSS volumes used in a shadow volume. if a file is a hard link, and the hard-linked file is moved between the primary and the secondary area, the move is really a copy and has the effect of breaking the hard link and creating an additional version of the file that is not linked to the other ones.

NSS Feature	Supported	Caveats
Media format for enhanced hard links	Yes	The media format that supports enhanced hard links is supported, but the hard links themselves are not.
Multiple Server Activation Prevention	Yes	Each pool enforces this separately.
Pool low-space warnings and watermarks	Yes	You must set the pool-level watermarks for low-space warnings separately for the primary pool and the secondary pool. **IMPORTANT:** NSS does not have a volume-level low-space-warning feature. However, you can take advantage of the NCP Server global parameters for managing low-space warnings for NCP volumes on NSS, Ext3, and Reiser file systems. For information, see "NCP Volumes Low-Space Warning" in the *OES 2 SP3: NCP Server for Linux Administration Guide*.
Pool snapshots	Yes	Take pool snapshots separately for the primary and secondary pools. **IMPORTANT:** For NSS on Linux, pool snapshots are not supported for clustered pools. If the primary volume is configured to contain the most frequently used data, pool snapshots of the primary pool have a higher percentage of changed data than does the secondary pool.
Renaming a volume's mount point	No	Renaming a volume's mount point breaks the shadow volume. If you need to rename a volume's mount point, remove the shadow, rename the volume's mount point, then create the shadow volume again.
Renaming a volume	No	Renaming a volume breaks the shadow volume. If you need to rename a volume, remove the shadow, rename the volume, then create the shadow volume again.
Resizing (growing) a pool	Yes	No known issues.
Sharing a pool and its volumes in a cluster	Yes	When using NSS volumes in shared pools, you must manage both pools' resources in the primary pool resource load and unload scripts. For information, see Section 5.8, "Using DST Shadow Volumes with Novell Cluster Services," on page 53.
Volume quotas	Yes	Set the volume quotas separately for each volume. For more information, see Section 5.7, "Using NSS Quotas on DST Shadow Volumes," on page 52.

5.5 Using NSS File System Trustees, Rights, and Attributes on DST Shadow Volumes

Authentication and file access is controlled by the file system trustees and rights that you set from the merged view. Users do not have direct access to the secondary volume.

Explicit trustee settings for files and folders are stored in both volumes.

Inherited trustee rights are calculated and enforced based on the trustee settings for the folders on the primary volume. The primary folder tree contains instances of the folders on the secondary volume in order to support this function.

File system attributes are enforced by the NSS file system. For NSS on Linux, the Read Only, Read/Write, Execute, and Hidden attributes are available.

5.6 Using NSS Encrypted Volumes in a DST Shadow Volume

If encrypted NSS volumes are used, both the primary and secondary volumes should be encrypted in order to provide the same level of security on both volumes.

The first time the volumes are mounted after a server reboot, the encrypted volumes must mounted manually by using NSSMU in order to provide the encryption passwords. Mount the secondary volume first so that it is available to DST when you mount the primary volume.

5.7 Using NSS Quotas on DST Shadow Volumes

DST supports using volume, directory, and user quotas features of NSS volumes. However, DST does not have a unified quota system for the two volumes that manages quotas for the combined primary and secondary volumes in a shadow volume pair.

5.7.1 NSS Volume Quotas

Volume quotas specify how big a volume can grow within a NSS pool. You can set a volume quota on the primary volume, secondary volume, or both volumes in the shadow volume pair. Each quota is enforced independently of the other.

Users of the shadow volume pair can map drives only to the primary volume. They are not aware of the existence of the secondary volume. Users see only the volume quota status for the primary volume. The volume quota information is not presented with a total space usage across both volumes. Users can actually store up to the quota amount set on each of the volumes, where each limit is enforced separately.

When the user has data stored on both the primary and secondary volume, the user sees the amount of space used only on the primary volume, which does not accurately reflect the total of space used on the two volumes.

The administrator can check the combined space available on the shadow volume pair and on each volume separately by using Novell Remote Manager for Linux.

5.7.2 NSS Directory Quotas

Directory quotas are set on specific directories and specify how much data can reside in that specific directory. You can set a directory quota only on the primary volume. When a secondary volume is in a shadow volume pair, the directory quotas set on it are not enforced. The directory quota is enforced only for the space consumed on the primary volume.

The users can store up to the directory quota amount for the directory on the primary volume, and an unlimited amount up to the maximum volume size on the secondary volume.

Users see only the directory quota status for the primary volume. The directory quota information is not presented with a total for the directory across both volumes.

5.7.3 NSS User Quotas

User quotas are set on specific users and specify how much data a user can store on a specific volume. You can set a user quota for a user on the primary volume, secondary volume, or both volumes in the shadow volume pair. Quotas on each volume are enforced independently of the other.

Users see only the user quota status for the primary volume. The user quota information is not presented with a total space usage across both volumes. Users can actually store up to the user quota amount set on each of the volumes, where each limit is enforced separately.

5.8 Using DST Shadow Volumes with Novell Cluster Services

DST supports using DST shadow volumes with Novell Cluster Services for Linux for clusters of up to 16 nodes. Clustering is supported for NSS volumes on shared Fibre Channel and iSCSI devices. Users can access files via NCP and via either Novell CIFS or SMB/CIFS.

The following caveats apply:

- All nodes where you plan to fail over the shadow volume must be running OES 2 Linux and be configured for DST. The nodes must have the same configuration of file systems, access protocols, and so on.
- DST and the NCP Server services are not cluster aware. They must be installed and configured separately on each node in the cluster.
- Global policies for DST must have the same settings on each node in the server. To manage a global DST policy for a given node, open Novell Remote Manager for Linux by using the IP address of the node, not the cluster resource. For information about configuring DST global policies, the Chapter 3, "Installing Dynamic Storage Technology," on page 31.
- To manage shadow volume policies in a cluster, open Novell Remote Manager for Linux by using the IP address of the cluster resource. You can also open Novell Remote Manager by using the IP address of the physical node where the cluster resource is currently mounted if you know which node it is on.
- The individual shadow volume's policies fail over along with the shadow volume.
- The primary volume and the secondary volume are managed in the primary cluster resource load and unload scripts. This allows the configuration to be failed over or cluster migrated to a different node as a single resource.

For planning information about installing and configuring shadow volumes in a cluster, see. Chapter 13, "Configuring DST Shadow Volume Pairs with Novell Cluster Services," on page 139

5.9 Using Novell Distributed File Services with DST Shadow Volumes

Novell Distributed File Services (DFS) is installed automatically as part of the NSS file system. Dynamic Storage Technology supports using DFS junctions on the primary NSS volume in a shadow volume pair. The primary volume can also be the target of a junction. Primary NSS volumes that contain DFS junctions or are junction targets can reside in an Novell Cluster Services cluster.

DST does not support using DFS junctions on the secondary volume. The secondary volume cannot be the target of a junction.

Junctions that are created on a primary NSS volume behave normally as they would for a single NSS volume. The policy enforcer is designed to prevent junctions from being moved between the primary and secondary volumes when policies are run.

Table 5-4 summarizes the supported DST configurations for use with DFS:

Table 5-4   *DST Support for Novell DFS Features*

Novell DFS Features	Primary NSS Volume	Secondary NSS Volume	Cluster	File Access Protocol
Junctions	Yes	No	Yes	NCP
				Novell CIFS. DFS support must be enabled in CIFS. See "DFS Junction Support in CIFS Linux" in the *OES 2 SP3: Novell CIFS for Linux Administration Guide*.
				Linux Samba does not support DFS junctions for NSS volumes.
Junction targets	Yes	No	Yes	Not applicable
Move/split volumes	No	No	No	Not applicable

When you use DST shadow volumes in combination with Novell DFS junctions, consider the following caveats:

- Junctions are broken when they reside on secondary NSS volumes. If you use an existing NSS volume as a secondary volume, delete junctions on it before you create the shadow volume pair. Make a note of the paths of the junctions and their targets. After the shadow volume pair is working, you can re-create the junctions in the same path on the primary volume.

- If you use an existing NSS volume as a secondary volume, any junctions pointing to it are broken when you create the shadow volume pair. You must create a new junction that points to the same location on the primary volume of that shadow relationship. After the new junction is working, delete the junction that points to the secondary volume.

- Do not create a shadow relationship for an NSS volume if a DFS move volume or split volume job is in progress.

- You must remove the shadow volume before you start a DFS move or split volume job.

5.10   Using Virus Checking Utilities with DST Shadow Volumes

You can continue use of existing virus checking utilities that currently execute successfully against the designated file systems on the primary volume. DST is transparent to this operation. Because the only access to the secondary volume is through the primary volume, there is no need for a virus checking operation directly on the secondary volume unless the shadow volume is removed, allowing the volume to act independently again.

5.11   Using Backup Utilities with DST Shadow Volumes

Applications that directly access the local Linux file system see the primary file tree and the secondary file tree as independent directories. Thus, backup tools can apply one backup policy to the primary file tree and a different backup policy to the secondary file tree. The only operations that take place on the secondary volume are backup, or remove and archive.

Using shadow volumes allows backups of important data to be made faster and more frequently because you can apply different backup policies for the primary volume and secondary volume. For example, the server administrator can partition the volume's data into two categories:

- ◆ Important data that needs to be maintained on quality storage and backed up frequently.
- ◆ Less important data that can be stored on less expensive storage and backed up less frequently.

An analysis or inventory of a volume's data shows that a large portion of it is seldom used. Having a shadow volume allows the server administrator to spend more on the most important data and spend less on the less important data. The frequently used data can be backed up incrementally or fully each day. The seldom-used data can be backed up weekly or monthly. Getting the less important data out of the way enables the backups of your important data to run more quickly and efficiently. Partitioning your data in this way can significantly reduce the cost of hosting it.

Because the most important files are located in the primary storage area, disaster recovery can also be faster. The server administrator can restore the critical files by restoring the primary storage area first, then restore the secondary storage area. This lets the users quickly get the files they need most, and they do not need to wait while files they do not usually need are restored. In addition, more fault tolerant replication solutions can be deployed for the primary storage area where it matters most.

If you back up the NSS volume by using the NSS Extended Attributes (`XAttr`) settings to preserve the NetWare metadata (`netware.metadata`) for file system rights and attributes, this information can be restored only directly to an NSS volume. For information about using the NSS / `ListXattrNWmetadata` option and the security considerations involved, see "ListXattrNWmetadata Option" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

Backup utilities might also work against the ShadowFS merged view. However, because the ShadowFS merged view is a Linux mount point and is not seen by the backup software as an NSS volume, the file system rights and attributes are not preserved. It is not recommended or supported to back up NSS files from this Linux mount point.

6 Management Tools for DST

This section provides an overview of the management tools for Dynamic Storage Technology (DST) in Novell Open Enterprise Server (OES) 2 Linux.

6.1 Dynamic Storage Technology Plug-In for Novell Remote Manager for Linux

The Dynamic Storage Technology Options plug-in to Novell Remote Manager for Linux allows you to create, manage, and remove shadow volumes built with Novell Storage Services volumes. The plug-in is automatically installed in Novell Remote Manager when you install NCP Server and Dynamic Storage Technology on your OES 2 Linux server.

6.1.1 Accessing Novell Remote Manager

1 In a Web browser, go to the URL of the server that you want to manage.

For example, enter the following in the address (URL) field:

```
http://server_IP_address:8008 or other_configured_port_number
```

For example:

```
http://192.168.123.11:8008
```

```
https://192.168.123.11:8009
```

2 Log in to Novell Remote Manager as the `root` user of the server or as the Novell eDirectory administrator user who has sufficient rights to manage the server and its file systems.

The `root` user logs in as a local user of the server, not through eDirectory. If eDirectory, Linux User Management, or PAM are not working, the `root` user can still log in to NRM to manage the server. The `root` user can always log in directly to the server to manage it.

NRM is PAM-enabled, so any Linux-enabled user can log in. Depending on the user's trustee rights for the server, the user gets access only to the tasks the user has rights to perform.

6.1.2   Starting, Stopping, or Restarting Novell Remote Manager on Linux

Novell Remote Manager on Linux is installed and runs by default. If it hangs, you can use the `/etc/init.d/novell-httpstkd` script to get status or to stop, start, or restart `httpstkd`. For the latest information about `httpstkd`, see "Starting or Stopping HTTPSTKD" in the *OES 2 SP3: Novell Remote Manager for Linux Administration Guide*.

1 Open a terminal console, then log in as the `root` user.

2 At the terminal console prompt, enter the command for the task you need to perform:

Task	Command
Status	`rcnovell-httpstkd status`
Start	`rcnovell-httpstkd start`
Stop	`rcnovell-httpstkd stop`
Restart	`rcnovell-httpstkd restart`

6.1.3   Quick Reference for Dynamic Storage Technology Options

The Dynamic Storage Technology Options plug-in (shown in Figure 6-1) in Novell Remote Manager for Linux is the primary tool for configuring global policies for all DST shadow volumes, creating and managing DST shadow volumes, and configuring shadow volume policies.

Figure 6-1   *View File System > Dynamic Storage Technology Options*

Table 6-1 describes the management tasks available for the *View File Systems > Dynamic Storage Technology Options* task in Novell Remote Manager for Linux.

Table 6-1   *View File Systems > Dynamic Storage Technology Options*

Subtasks	Management Tasks
Volume Information	View a list of NCP volumes and NSS volumes on the server.
	Click the *Add Shadow* link next to an NSS volume to view information about where you can create a shadow volume.
	IMPORTANT: NCP volumes on Linux POSIX file systems are not supported as shadow volumes. This capability is planned for a future release.
	Click the *Inventory* link next to a shadow volume to view an inventory report for both the primary and secondary volumes.
	Click the *View Log* link next to an NSS volume to download a copy of the audit log for the selected volume.
Add Shadow link	This option takes you to the Share Information page. Scroll down to the *Volume Tasks* area to find the *Add Shadow Volume* task.
	The Share Information page and Add Shadow Volume page do not distinguish or validate whether the volumes you choose are actually supported file systems and available combinations.
	IMPORTANT: NSS volumes must already exist when you create the shadow volume. The *Create if not present* option is available for future support of NCP volumes on Linux file systems. Do not use this option for NSS volumes.
Inventory link	View statistics and graphical trend displays for the volume's files and directories. For a DST shadow volume, the report includes information for both the primary storage area (primary area) and the secondary storage area (shadow area).
Volume Information (Info icon)	NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics.
	Open files listed for each NCP connection.
	Add a shadow volume for the NCP volume.
	For unmounted DST shadow volumes, click the *Info* icon to access the dialog box to remove the shadow volume relationship. This removes the entry in the `ncpserv.conf` file, but does not delete the volume itself.
	To unmount a shadow volume, click *Manage NCP Services > Manage Shares*, then click the *Unmount* option next to the shadow volume.
Dynamic Storage Technology Policies	Create a new policy.
	View a list of existing policies.
	Click the *Policy Name* link to modify or delete the policy.
Duplicate File Resolution Options	Set a global policy for how to handle duplicate files.

Subtasks	Management Tasks
ShadowFS Configuration	Set a global policy for whether to automatically start FUSE and Shadow File System, which are needed to provide access to users via Samba.
	IMPORTANT: Do not enable ShadowFS if you are using Novell CIFS.

6.1.4 Quick Reference for NCP Server Options

Table 6-2 describes the DST tasks available for the *Manage NCP Services > Manage Shares* task in Novell Remote Manager for Linux. For a complete list of NCP Server management tasks, see "Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux" in the *OES 2 SP3: NCP Server for Linux Administration Guide*.

Table 6-2 *Manage NCP Services > Manage Shares*

Subtasks	Management Tasks
NCP/NSS Bindings	In the *Configuration* area, click *NCP/NSS Bindings* to view a list of NSS volumes on the server. Set the *NCP Available* setting to No for NSS volumes that you want to use as secondary storage locations for DST shadow volumes.
Mount/Unmount	Mount or unmount the primary volume for a shadow volume. The primary volume must be unmounted in order to access the Remove Shadow Volumes task.
Info > Remove Shadow Volume	For unmounted DST shadow volumes, click the *Info* icon to access the dialog box to remove the shadow volume relationship. This removes the entry in the ncpserv.conf file, but does not delete the two volumes and their data.

6.1.5 Quick Reference for DST Global Policy Settings

Table 6-3 describes the DST parameters available for the *Manage NCP Services > Manage Server* task in Novell Remote Manager for Linux. For descriptions of the parameters, see Section A.4.1, "Understanding DST Parameters for the SET Command," on page 190.

Table 6-3 *Manage NCP Services > Manage Server > Server Parameter Information*

Parameter Name	Default Value	Valid Values
SHIFT_MODIFIED_SHADOW_FILES	1	0 - Disable
		1 - Allow
SHIFT_ACCESSED_SHADOW_FILES	0	0 - Disable
		1 - Allow
SHIFT_DAYS_SINCE_LAST_ACCESS	1	0 - Disable
		1 to 365 (in days)

Parameter Name	Default Value	Valid Values
DUPLICATE_SHADOW_FILE_ACTION	0	0 - Show duplicate shadow files (default)
		1 - Hide duplicate shadow files
		2 - Rename duplicate shadow files
		3 - Delete duplicate files from shadow area
		4 - Move duplicate shadow files to `/._DUPLICATE_FILES`
DUPLICATE_SHADOW_FILE_BROADCAST	1	0 - Disable
		1 - Allow
REPLICATE_PRIMARY_TREE_TO_SHADOW	0	0 - Disable
		1 - Allow

6.1.6 Shadow Volume Inventory and Trustee Reports

In Novell Remote Manager, the Volume Inventory feature detects shadow volumes and displays information from the primary and secondary volumes. The complete inventory profile displays three categories of information: combined areas, primary area, and shadow area. With Novell Remote Manager's shadow volume inventory, you can also select files that meet specific criteria (such as files that have not been accessed for two years, files that have not been modified in a year, all `.mp3` files, and so on). Use the inventory information to profile each area's files and move them as needed.

For general information about the volume inventory feature, see "Generating Inventories for Directories or NCP Volumes" *OES 2 SP3: Novell Remote Manager for Linux Administration Guide*.

Novell Remote Manager also allows you to generate a trustee report for the shadow volume. For information, see "Generating and Viewing NCP Trustee Reports for NSS Volumes" *OES 2 SP3: Novell Remote Manager for Linux Administration Guide*.

6.2 NCP Console (NCPCON) Commands

You can optionally use the NCP Console (NCPCON, `ncpcon(8` command) to manage Dynamic Storage Technology pairs from a terminal console. For information, see Section A.1, "Using NCPCON for DST Commands," on page 183.

6.3 Management Tools for NSS Volumes

- Section 6.3.1, "Storage Plug-In for Novell iManager 2.7x," on page 62
- Section 6.3.2, "Files and Folders Plug-In for Novell iManager 2.7," on page 62
- Section 6.3.3, "NSS Management Utility (NSSMU)," on page 62

6.3.1 Storage Plug-In for Novell iManager 2.7x

Use the Storage plug-in for iManager to create and manage Novell Storage Services (NSS) volumes that you use as DST shadow volumes. For information, see "Novell iManager and Storage-Related Plug-Ins" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

6.3.2 Files and Folders Plug-In for Novell iManager 2.7

Use the Files and Folders plug-in for iManager to manage file system trustees, trustee rights, and inherited rights filters for files and directories on NSS volumes that you use as DST shadow volumes. You can also set file ownership, directory quotas, and file system attributes. For information, see "Files and Folders Plug-In Quick Reference" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

6.3.3 NSS Management Utility (NSSMU)

You can also use the NSS Management Utility (NSSMU, `nssmu(8)` command) to create and manage NSS volumes that you use in DST shadow volumes. For information, see "NSS Management Utility (NSSMU) Quick Reference" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

6.4 Management Tools for Clustering

Use the Clustering plug-in for Novell iManager 2.7 to create and manage the cluster resources, load scripts, and unload scripts for clustered NSS pools that contain the NSS volumes you use as DST shadow volumes. For information, see "Creating Cluster Resources" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

7 Managing Services for DST

The health of Dynamic Storage Technology depends on other services that are running on the Novell Open Enterprise Server (OES) 2 Linux server. This section identifies those dependencies and provides instructions for how to get them started again if they are not running.

- Section 7.1, "Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon," on page 63
- Section 7.2, "Restarting the Novell eDirectory (ndsd) Daemon," on page 63
- Section 7.3, "Starting and Stopping ShadowFS," on page 64

7.1 Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon

If NSS is installed, NCP Server runs the Novell NCP/NSS IPC (`/etc/init.d/ncp2nss`) daemon in order to synchronize its settings with NSS. When you modify NCP Server settings by using Novell Remote Manager for Linux, NCP Server automatically restarts `ncp2nss` so that the new settings are immediately synchronized with NSS. If you modify values for any of the DST global parameters for NCP Server by directly editing the `/etc/opt/novell/ncpserv.conf` file, you must manually restart `ncp2nss`.

1. On the OES 2 Linux server, open a terminal console, then log in as the `root` user.

2. At the terminal console prompt, enter

   `/etc/init.d/ncp2nss restart`

3. If ncp2nss restarts successfully, the following messages are displayed in the terminal console:

   `Shutting down Novell NCP/NSS IPC daemon...`

   `Exited`

   `Starting the Novell NCP/NSS IPC daemon.`

7.2 Restarting the Novell eDirectory (ndsd) Daemon

When you modify NCP Server settings by using Novell Remote Manager for Linux, NCP Server automatically restarts the Novell eDirectory daemon to apply the new settings. If you modify values for any of the DST global parameters for NCP Server by directly editing the `/etc/opt/novell/ncpserv.conf` file, you must restart the Novell eDirectory daemon to put the changes into effect.

Use the following steps to stop and start `ndsd` when a single instance is running. For information about stopping and starting `ndsd` when you are running multiple instances of it on the same server, see "Managing Multiple Instances" in the *Novell eDirectory 8.8 What's New* (http://www.novell.com/documentation/edir88/edir88new/data/front.html).

IMPORTANT: Restarting or stopping ndsd automatically disconnects all user connections and does not warn users before the connection is broken. Users can reconnect to the server after the service starts.

1 Use one of the following commands to stop `ndsd`:

```
rcndsd stop
```

```
/etc/init.d/ndsd stop
```

2 Use one of the following commands to start `ndsd`:

```
rcndsd start
```

```
/etc/init.d/ndsd start
```

7.3 Starting and Stopping ShadowFS

ShadowFS must be running in order to provide a merged view to SMB/CIFS users if you are using Novell Samba to provide file access to a DST shadow volume.

To configure a global policy to start ShadowFS at boot time, see .

Only one instance of ShadowFS should be loaded at a time. Before you attempt to manually start ShadowFS, ensure that you have stopped any running instances of it.

1 Log in as the `root` user, then open a terminal console.

2 Do one of the following:

- ◆ **Start:** Enter the following at a command prompt to start ShadowFS:

  ```
  /etc/init.d/novell-shadowfs start
  ```

- ◆ **Stop:** Enter the following at a command prompt to stop ShadowFS:

  ```
  /etc/init.d/novell-shadowfs stop
  ```

8 Configuring DST Global Policies

This section describes how to configure global policies for Dynamic Storage Technology (DST) on a Novell Open Enterprise Server (OES) 2 Linux server. Global policies apply to all shadow volumes on a DST server.

IMPORTANT: If you use shadow volumes in a cluster, ensure that you set the same global policies on each OES 2 Linux node in the cluster.

8.1 Replicating Branches of the Primary File Tree in the Secondary File Tree

You can create a global policy to control when branches in the primary file tree are replicated to the secondary file tree.

When a new directory is created, the folder is created in the primary file tree. A configurable option called *Replicate Primary Tree to Shadow* determines whether a matching path is automatically created at that time, or later when a policy is enforced that actually moves data in the folder to the secondary location. By default, the branches are not created in the secondary file tree until they are needed. Performance is better when the branches are created only as needed.

IMPORTANT: If you use shadow volumes in a cluster, ensure that you set the same global policies on each OES 2 Linux node in the cluster.

Valid settings for the Replicate Primary Tree to Shadow are:

- **Disabled (0, default):** Branches of the primary file tree are replicated to the secondary file tree as needed when data is moved from the primary storage area to the secondary storage area.
- **Enabled (1):** Branches of the primary file tree are replicated to the secondary file tree immediately as they are created on the primary file tree, even if they do not currently contain data in the secondary storage location. Paths in the primary file tree and secondary file tree are the same at all times.

To configure the Replicate Primary Tree to Shadow parameter:

1 Log in as the `root` user to Novell Remote Manager.

2 Select *Manage NCP Services > Manage Server* to view the *Server Parameter Information*.

3 Click the link for the REPLICATE_PRIMARY_TREE_TO_SHADOW setting.

4 In *New Value*, do one of the following:

- **Disable Immediate Path Replication:** Type 0 to replicate paths in the secondary file tree as they are needed when the data is actually moved to the secondary storage area.

- **Allow Immediate Path Replication:** Type 1 to replicate all paths in the secondary file tree immediately as they are created on the primary file tree.

5 Click *Change*.

6 On the *Server Parameter Information* page, verify that the new setting is displayed for the REPLICATE_PRIMARY_TREE_TO_SHADOW parameter.

For information about using the SET command to modify this global policy, see Section A.4, "Configuring Global DST Policies by Using the SET Command," on page 190.

8.2 Shifting Files from the Secondary File Tree to the Primary File Tree

You can configure global policies for how files in the secondary file tree are automatically moved back to the primary volume. By default, files are moved back to the primary if they are modified, but not if they are accessed.

- Section 8.2.1, "Understanding Shift Parameters," on page 66
- Section 8.2.2, "Configuring a Global Policy for Shifting Modified Shadow Files," on page 69
- Section 8.2.3, "Configuring a Global Policy for Shifting Accessed Shadow Files," on page 69
- Section 8.2.4, "Configuring a Global Policy for the Days Since Last Access," on page 70
- Section 8.2.5, "Using the SET Command to Set Global Policies," on page 70

8.2.1 Understanding Shift Parameters

You can control how files are automatically moved from the secondary storage area to the primary storage area by configuring three parameters:

- Shift Modified Shadow Files
- Shift Accessed Shadow Files
- Shift Days Since Last Access

IMPORTANT: If you use shadow volumes in a cluster, ensure that you set the same global policies on each OES 2 Linux node in the cluster.

This section describes the parameters, and recommends combinations of the policies to achieve different goals.

- "Shift Modified Shadow Files" on page 67
- "Shift Accessed Shadow Files" on page 67
- "Shift Days Since Last Access" on page 68
- "Use Cases for Shifting Shadow Files" on page 68

Shift Modified Shadow Files

When files in the secondary file tree are modified, a configurable global policy called *Shift Modified Shadow Files* allows the files to be moved to the primary file tree (default), or kept in the secondary file tree. When this parameter is enabled, the file is automatically moved back to the primary storage area when the file is closed. This global policy applies to all DST shadow volumes on a given server.

Valid settings for Shift Modified Shadow Files are:

- **Disabled (0):** When a file that resides on the secondary storage area is modified, it remains on the secondary storage area.

  > **IMPORTANT:** Applications are not aware that DST stores files in two locations. Depending on how an application works, a file might reside on the secondary storage when it is opened, and reside on the primary storage after it is modified.
  >
  > For example, when you open a file to modify it, Microsoft Word creates a new temporary file and copies the content to it. It saves any changes in the new file, and deletes the old one. Because DST creates all new files on the primary location, the temporary file is created and saved on the primary storage, and the old file is deleted on the secondary location.
  >
  > This behavior is not unique to Microsoft applications; other word processors and applications behave in the same fashion. When you plan your solution, you must be aware of how the applications you use actually work. If an application's behavior overrides your intended data locations in the shadow volume, you can use policies to achieve the desired separation.

- **Enabled (1, default):** If a file that resides on the secondary storage area is modified, it is automatically shifted to the primary storage area after it is closed. The file remains on the primary storage area until a policy is enforced that shifts it to the secondary storage area.

For example, if your policy is to place newer files in the primary file tree and to place older files in the secondary file tree, you want an older file in the secondary file tree to move to primary file tree if the file's content is modified. The Shift Modified Shadow Files parameter is enabled by default, so this is the default behavior.

On the other hand, if you are placing files of one type (such as `.doc` and `.ppt`) in the primary area and files of a different type (such as `.mp3` and `.jpg`) in the secondary area, you want files to stay where they are whenever they are modified. In this case, you should disable the Shift Modified Shadow Files parameter.

Shift Accessed Shadow Files

When files in the secondary file tree are accessed (but not changed), a configurable global policy called *Shift Accessed Shadow Files* allows the files to be left in the secondary file tree (default), or to be moved to the primary file tree. When this parameter is enabled, a file is shifted if it is accessed as read-only a second time during a specified period of time. The file is automatically moved back to the primary area when the file is closed. By default, the period of time is 1 day. Use the Shift Days Since Last Access parameter to specify the period of time. This global policy applies to all DST shadow volumes on a given server.

Valid settings for the Shift Accessed Shadow Files are:

- **Disabled (0, default):** When a file that resides on the secondary storage area is accessed twice in the specified period, it remains on the secondary storage area.

- **Enabled (1):** If a file that resides on the secondary storage area is accessed twice in the specified period, it is automatically shifted to the primary storage area after it is closed. The file remains on the primary storage area until a policy is enforced that shifts it to the secondary storage area.

For example, if you are placing files that are changing in the primary area and files that are not changing in the secondary area, you want files to stay where they are whenever they are accessed but not changed. The Shift Accessed Shadow Files parameter is disabled by default, so this is the default behavior.

On the other hand, if your policy is to place in-use files in the primary file tree and to place unused files in the secondary file tree, you want an in-use file in the secondary file tree to move to primary file tree if the file is accessed, whether it changes or not. In this case, you should enable the Shift Accessed Shadow Files parameter.

Shift Days Since Last Access

The Shift Days Since Last Access parameter specifies the number of days to use when determining if a file should be moved back to the primary storage area. When it is used with SHIFT_ACCESSED_SHADOW_FILES, the parameter sets the time when files are migrated back to the primary storage area after the second access within the specified elapsed time.

Valid settings for the Shift Accessed Shadow Files are:

◆ **Disabled (0):** Files are not shifted on access.
◆ **Number of Days (1 to 365):** If a file that resides on the secondary storage area is accessed twice in the specified period, it is automatically shifted to the primary storage area after it is closed. The default is 1 day.

Use Cases for Shifting Shadow Files

Table 8-1 describes use cases for shifting files based on the global policies.

Table 8-1   *Shift Behaviors for Files in the Secondary File Tree*

	Don't Shift Modified Shadow File to Primary	Shift Modified Shadow File to Primary (Default)
Don't Shift Accessed Shadow File to Primary (Default)	Files can be modified or accessed without being shifted to the primary file tree. For example, you can separate files by file type, with the less important files in the secondary area. Thereafter, the files remain where you moved them. You can periodically apply volume-level policies that move file types from the primary to the secondary. Back up the primary area more frequently because it contains the most important file types.	Modified files are shifted to the primary file tree, but accessed files are not. This is the default combination. Separate files so that recently modified files are located in the primary area. Older files remain in the secondary area. Back up the primary area more frequently because it contains all of the recently changed files.

	Don't Shift Modified Shadow File to Primary	Shift Modified Shadow File to Primary (Default)
Shift Accessed Shadow File to Primary	Files are shifted when they are accessed twice in a specified period, but not when they are modified. No use case exists for this combination.	Files are shifted when they are modified, or if they are accessed twice in a specified period. This is desirable for migration-on-demand solutions that move data gradually from an old volume to a new, higher-performance location. Unchanged, seldom-used files are available to users, but do not require frequent backups.

8.2.2 Configuring a Global Policy for Shifting Modified Shadow Files

To configure the Shift Modified Shadow Files parameter:

1 Log in as the `root` user to Novell Remote Manager.

2 Select *Manage NCP Services > Manage Server* to view the Server Parameter Information page.

3 Click the link for the SHIFT_MODIFIED_SHADOW_FILES setting.

4 In *New Value*, do one of the following:

- ◆ **Disable Modified Files from Shifting to Primary:** Type 0 to keep files on the secondary storage area when they are modified.

- ◆ **Allow Modified Files to Shift to Primary:** Type 1 to shift files on the secondary storage area to the primary storage area when they are modified. This is the default.

5 Click *Change*.

6 On the Server Parameter Information page, verify that the new setting is displayed for the SHIFT_MODIFIED_SHADOW_FILES parameter.

8.2.3 Configuring a Global Policy for Shifting Accessed Shadow Files

To configure the Shift Accessed Shadow Files parameter:

1 Log in as the `root` user to Novell Remote Manager.

2 Select *Manage NCP Services > Manage Server* to view the Server Parameter Information page.

3 Click the link for the SHIFT_ACCESSED_SHADOW_FILES setting.

4 In *New Value*, do one of the following:

- ◆ **Disable Accessed Files from Shifting to Primary:** Type 0 to keep files on the secondary storage area when they are accessed. This is the default.

- ◆ **Allow Accessed Files to Shift to Primary:** Type 1 to shift files on the secondary storage area to the primary storage area when they are accessed twice during a specified period.

5 Click *Change*.

6 On the Server Parameter Information page, verify that the new setting is displayed for the SHIFT_ACCESSED_SHADOW_FILES parameter.

8.2.4 Configuring a Global Policy for the Days Since Last Access

To configure the Shift Days Since Last Access parameter:

1 Log in as the `root` user to Novell Remote Manager.

2 Select *Manage NCP Services > Manage Server* to view the Server Parameter Information page.

3 Click the link for the SHIFT_DAYS_SINCE_LAST_ACCESS setting.

4 In *New Value*, do one of the following:

- ◆ **Disable:** Type 0 to disable this parameter.
- ◆ **Number of Days:** Type an integer value from 1 to 365 (in days) that specifies the number of days to wait for a second access of a shadow file. If the second access occurs during this period, the file can be moved if the SHIFT_ACCESSED_SHADOW_FILES parameter is also enabled.

5 Click *Change*.

6 On the Server Parameter Information page, verify that the new setting is displayed for the SHIFT_DAYS_SINCE_LAST_ACCESS parameter.

8.2.5 Using the SET Command to Set Global Policies

For information about using the SET command to modify these global policies, see Section A.4, "Configuring Global DST Policies by Using the SET Command," on page 190.

8.3 Resolving Instances of Duplicate Files

You might want to change the default policies for how duplicate files are resolved for DST shadow volumes.

- ◆ Section 8.3.1, "Understanding Conflict Resolution for Duplicate Files," on page 70
- ◆ Section 8.3.2, "Configuring a Global Policy for Actions to Resolve Duplicate Files Conflicts," on page 73
- ◆ Section 8.3.3, "Enabling or Disabling Broadcast Messages for Duplicate Files Conflicts," on page 74
- ◆ Section 8.3.4, "Resolving Instances of Duplicate Files in the /._DUPLICATE_FILES Directory," on page 75

8.3.1 Understanding Conflict Resolution for Duplicate Files

The Duplicate File Resolution policies are designed to handle the case where files with the same name are located in matching directories in both the primary storage location and the secondary storage location. Duplicate files typically are caused by restoring instances of the same file to both the primary storage location and the secondary storage location. If you back up the primary volume more frequently than the secondary volume, the instance of the file that is restored on the primary storage area should be the most current of the two files.

Figure 8-1 *Duplicate File Resolution Options (Defaults)*

IMPORTANT: If you use shadow volumes in a cluster, ensure that you set the same global policies on each OES 2 Linux node in the cluster.

The following global policies can be set to govern handling of duplicate files for all shadow volumes on the server:

- ◆ "Handling Instances of Duplicate Files" on page 71
- ◆ "Broadcasting Conflict Messages to NCP Users" on page 72
- ◆ "Recommended Policy Settings for Duplicate Files Conflict Resolution" on page 72

Handling Instances of Duplicate Files

Table 8-3 describes the options for handling duplicate instances of files. For information about configuring the *Actions to be taken* parameter, see Section 8.3.2, "Configuring a Global Policy for Actions to Resolve Duplicate Files Conflicts," on page 73.

Table 8-2 *Actions for Duplicate File Resolution*

Parameter Options	User View	Resolution
Show duplicate shadow files (default)	The file name appears twice in directory listings.	The administrator or user manually renames one of the files so the system can tell them apart. The user should then determine whether or not to delete one of the instances, and which instance to delete.
Hide duplicate shadow files	Only one instance of the file name is displayed in the directory listings. Client file operations are directed to the instance located on the primary area. If the client deletes the file, the instance in the primary area is deleted, and the instance in the secondary area is then visible.	The users are not aware that a conflict exists. However, the user might see files randomly reappear after they delete a file.
Rename duplicate shadow files	Automatically renames the duplicate file located on the secondary area by adding a unique extension to the name.	Both instances of the file (the file on the primary area and the renamed file on the secondary area) appear in directory listings. The user needs to be informed that such instances might occur so the user can determine which file instance to keep.

Parameter Options	User View	Resolution
Delete duplicate files from the shadow area	Automatically deletes duplicate files located on the secondary storage area.	The users are not aware that a conflict exists. Because duplicate files are typically caused by restoring instances of the same file to both the primary and secondary areas, the instance located on the primary area should be the most current of the two.
Move duplicate shadow files to / ._DUPLICATE_FILES	Causes the duplicate file located on the secondary storage area to be moved to the / ._DUPLICATE_FILES directory at the root of the secondary volume. If there is a file name conflict in the destination directory, then a unique extension is also added to the file name.	The users are not aware that a conflict exists. This option is less risky than automatically deleting duplicate files. It might require occasional cleanup work to be performed in the / ._DUPLICATE_FILES directory.

Broadcasting Conflict Messages to NCP Users

DST leverages the broadcast message capability of NCP Server for Linux. You can disable the broadcast messages option in DST if you choose not to broadcast messages when duplicate files are discovered. If the option is enabled, the messages are received only by client versions that support broadcast messages, and only if the client itself has broadcast messages enabled.

If the option is enabled, a message is broadcast by default to NCP users of the file, whenever duplicate file conflicts occur.

There are two prerequisites for using broadcast messages:

- ◆ **NCP Server:** NCP Server must be configured to support broadcast messages by setting the Disable Broadcast parameter for the SET command to 0 (disabled).
- ◆ **Novell Client:** The Novell Client version being used by the NCP users must be capable of receiving broadcast messages, and the client must be configured to receive broadcast messages.

  The broadcast message capability is called Send Message in the Novell Client. In OES 2 SP1, the Send Message feature is available in the Novell Client 4.91 SP4 for Windows XP/2003, the Novell Client 1.0 SP1 for Vista, and the Novell Client 2.0 for Linux.

For information about configuring the Broadcast Conflict Messages to Users parameter, see Section 8.3.3, "Enabling or Disabling Broadcast Messages for Duplicate Files Conflicts," on page 74.

Recommended Policy Settings for Duplicate Files Conflict Resolution

The settings for broadcasting messages and handling files are configured separately. Table 8-3 summarizes recommendations for combining the two. However, if users are SMB/CIFS users who cannot receive broadcast messages, or if the version of the Novell Client that is in use does not support receiving broadcast messages, you should simply disable broadcast, and select an action that makes sense in your environment.

For information, see "Handling Instances of Duplicate Files" on page 71.

Table 8-3   *Recommended Global Policies for Duplicate Files Resolution*

Action to be Taken	Broadcast Conflict Messages to Users
Show duplicate shadow files (default)	Enable broadcast (default)
Hide duplicate shadow files	Disable broadcast
Rename duplicate shadow files	Optionally enable broadcast
Delete duplicate files from the shadow area	Disable broadcast
Move duplicate shadow files to / ._DUPLICATE_FILES	Disable broadcast

8.3.2   Configuring a Global Policy for Actions to Resolve Duplicate Files Conflicts

You can set a global policy for the actions to be taken to resolve duplicate file conflicts.

By default, the *Actions to be taken* parameter is set to show duplicate shadow files to the user. For information about the other options, see "Handling Instances of Duplicate Files" on page 71.

For information about using the SET command to modify this global policy, see Section A.4, "Configuring Global DST Policies by Using the SET Command," on page 190.

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options*.

2 In the *Duplicate File Resolution Options* area, view the current setting for *Actions to be taken*.

3 From the *Actions to be taken* drop-down list, select one of the following options:

- *Show duplicate shadow files* (default)
- *Hide duplicate shadow files*
- *Rename duplicate shadow files*
- *Delete duplicate files from shadow area*
- *Move duplicate shadow files to* /._DUPLICATE_FILES

4 In the *Duplicate File Resolution Options* area, click *Submit* to save and apply the change.

8.3.3 Enabling or Disabling Broadcast Messages for Duplicate Files Conflicts
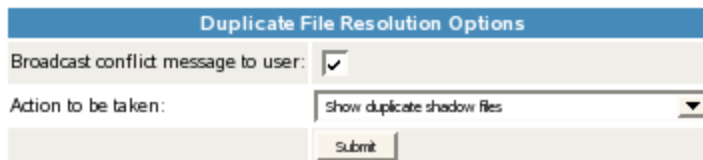
You can set a global policy that enables or disables broadcast messages to be sent to NCP clients when duplicate file conflicts are detected.

When *Broadcast Conflict Messages to Users* is enabled (the default setting), a message is broadcast to NCP users of the file when duplicate instances of the file occur on the primary storage location and secondary storage location. For information, see "Broadcasting Conflict Messages to NCP Users" on page 72 and "Recommended Policy Settings for Duplicate Files Conflict Resolution" on page 72.

IMPORTANT: In order for users to be able to receive the duplicate-file-conflict messages, NCP Server must be configured to support broadcast messages and the Novell clients must be configured to receive broadcast messages. For instructions, see "Enabling or Disabling Broadcast Message Support" in the *OES 2 SP3: NCP Server for Linux Administration Guide*.

For information about using the SET command to modify this global policy, see Section A.4, "Configuring Global DST Policies by Using the SET Command," on page 190.

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options*.

2 In the *Duplicate File Resolution Options* area, enable or disable *Broadcast Conflict Messages to Users* by selecting or deselecting the check box next to it. It is enabled by default.

3 In the *Duplicate File Resolution Options* area, click *Submit* to save and apply the change.

4 If you enabled Broadcast Conflict Messages, ensure that NCP Server is configured to support broadcast messages by verifying that the Disable Broadcast (DISABLE_BROADCAST) parameter for the SET command is disabled.

4a In Novell Remote Manager for Linux, select *Manage NCP Services*, then select *Manage Server*.

4b In the *Set Parameter Information* table, locate the DISABLE_BROADCAST parameter, then view the current value of the parameter. By default, the parameter is disabled (set to 0), which means that NCP Server supports broadcast messages.

4c If the DISABLE_BROADCAST parameter is enabled (set to 1), click the link for the value in the *Parameter Value* column to open a page where you can change the value.

4d In *New Value*, type 0, then click *Change* to save and apply the settings that disable the DISABLE_BROADCAST parameter, which enables broadcasting for NCP Server.

IMPORTANT: Messages are received only by logged-in users who are using Novell Client versions that are capable of receiving broadcast messages, and that are configured to receive them.

DISABLE_BROADCAST		
Current Value	**New Value**	
1	0	Change
	Back	

8.3.4 Resolving Instances of Duplicate Files in the /._DUPLICATE_FILES Directory

If you enable *Move duplicate shadow files to* `/._DUPLICATE_FILES` as the action to be taken when duplicate file conflicts occur, it might require occasional cleanup work to be performed in the `/._DUPLICATE_FILES` directory.

8.4 Loading ShadowFS

ShadowFS is required to provide a merged view access to DST volumes for users via SMB/CIFS or native Linux file access. You can start it manually, or set a policy to automatically load ShadowFS at boot time. For information about using and managing ShadowFS, see Chapter 12, "Using ShadowFS to Provide a Merged View for Novell Samba Users," on page 129.

By default, ShadowFS and FUSE are not started automatically at boot time. You can set the *ShadowFS Configuration > Load ShadowFS* option that starts them at boot time. It also starts them when you first enable the global policy if they are not already running. A single instance of ShadowFS should be running on a server. The setting applies for all DST volumes on the server.

IMPORTANT: If you use shadow volumes in a cluster, ensure that you set the same global policies on each OES 2 Linux node in the cluster.

- Section 8.4.1, "Using Novell Remote Manager to Set the Autostart of ShadowFS," on page 75
- Section 8.4.2, "Using the Command Line to Set the Autostart of ShadowFS," on page 76
- Section 8.4.3, "Manually Starting and Stopping ShadowFS," on page 76

8.4.1 Using Novell Remote Manager to Set the Autostart of ShadowFS

The *Load ShadowFS* option in Novell Remote Manager provides a GUI interface for setting up ShadowFS to start at boot time. It also starts ShadowFS when the option is first enabled if ShadowFS is not already running.

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options*.

2 In the *ShadowFS Configuration* area, view the current setting for *Load ShadowFS*.

3 Enable or disable *Load ShadowFS* by selecting or deselecting the check box.

4 In the *ShadowFS Configuration* area, click *Submit* to save and apply the change.

8.4.2 Using the Command Line to Set the Autostart of ShadowFS

You can set the service to autostart upon future reboots at the command line instead of using Novell Remote Manager:

1 Log in as the `root` user, then open a terminal console.

2 Do one of the following:

- **Enable Autostart:** Enter the following at a command prompt to enable the autostart of `novell-shadowfs`:

  `chkconfig novell-shadowfs on`

- **Disable Autostart:** Enter the following at a command prompt to disable the autostart of `novell-shadowfs`:

  `chkconfig novell-shadowfs off`

8.4.3 Manually Starting and Stopping ShadowFS

Only one instance of ShadowFS should be loaded at a time. Before you attempt to manually start ShadowFS, ensure that you have stopped any running instances of it.

1 Log in as the `root` user, then open a terminal console.

2 Do one of the following:

- **Start:** Enter the following at a command prompt to start ShadowFS:

  `/etc/init.d/novell-shadowfs start`

- **Stop:** Enter the following at a command prompt to stop ShadowFS:

  `/etc/init.d/novell-shadowfs stop`

9 Creating and Managing DST Shadow Volumes for NSS Volumes

Dynamic Storage Technology (DST) supports shadow volume pairs with two Novell Storage Services (NSS) volumes on Novell Open Enterprise Server (OES) 2 Linux. This section describes how to create and manage shadow volume pairs with NSS volumes.

9.1 Understanding DST Shadow Volumes

The DST shadow volume is a virtual NCP (NetWare Core Protocol) volume that consists of a primary storage area and a secondary storage area. The primary and secondary areas use NSS volumes.

9.1.1 Primary Volume

The primary volume is an NSS volume that is mounted on the OES 2 Linux server that is running DST. Shadow volumes are known by their primary volume name. Typically, the primary volume is on the higher-performance device.

When the primary volume has a state of *Shadowed*, the volume ID that is assigned as its NCP volume ID represents the DST shadow volume pair of volumes. The secondary volume does not have a separate volume ID while it is in the shadow relationship.

9.1.2 Secondary Volume

The secondary volume is an NSS volume that is mounted on the OES 2 Linux server that is running DST. This volume is also referred to as the *shadow path*. The secondary volume is also referred to as the *secondary file tree*.

The secondary volume is typically a new volume. It should have a similar setup as the primary volume for key attributes settings, such as Salvage, Encryption, and Lookup Namespace. For guidelines and caveats about using NSS volume attributes with Dynamic Storage Technology, see Table 5-2, "DST Support for NSS Volume Attributes," on page 49.

IMPORTANT: If a secondary volume has existing files that reside only on it, its files can end up as folders when they are moved from primary to secondary. To avoid this problem, ensure that you have applied the latest patches for DST on your server.

For information, see Section 14.5, "Files that initially reside only on the secondary volume can end up as directories on the primary volume," on page 178.

For information about using remote secondary volumes in a shadow volume, see Chapter C, "Technology Preview: Creating and Managing DST Shadow Volumes with Remote Secondary NSS Volumes," on page 199.

9.1.3 Merged View

The primary file tree and the secondary file tree have the same directory structure. A file can be located in either the primary file tree or the secondary file tree. The merged view presents these two file trees as a single file tree, as shown in Figure 1-1, "User View of the File System Directory," on page 16.

The NCP clients and management tools see a merged view of files on the DST shadow volume when they access the primary volume. In OES 2 SP3 Linux and later, Novell CIFS also provides a merged view for CIFS users that access CIFS shares on the primary volume.

If Novell Samba is used with DST shadow volumes, a SMB/CIFS user sees the merged view that is provided by the ShadowFS component of DST.

9.1.4 How Directories Are Created in the Shadow Volume

New directories are created in the primary file tree. A configurable global policy called *Replicate Primary Tree to Shadow* determines when the directory path is created in the secondary file tree:

  ◆ At the time when the directory is created in the primary file tree
  ◆ Only when files are moved based on policy enforcement

Performance is better when the branches are created only as needed. For information see Section 8.1, "Replicating Branches of the Primary File Tree in the Secondary File Tree," on page 65.

9.1.5 Global Policies

Global policies govern the behavior of DST, and apply to all shadow volumes on a given server. Before you configure shadow volumes on the server, ensure that you configure the global policies listed in Table 9-1.

Table 9-1   *Global Policies*

Global Policy Parameter	For Information
REPLICATE_PRIMARY_TREE_TO_SHADOW	Section 8.1, "Replicating Branches of the Primary File Tree in the Secondary File Tree," on page 65
SHIFT_MODIFIED_SHADOW_FILE SHIFT_ACCESSED_SHADOW_FILE SHIFT_DAYS_SINCE_LAST_ACCESS	Section 8.2, "Shifting Files from the Secondary File Tree to the Primary File Tree," on page 66
DUPLICATE_SHADOW_FILE_ACTION DUPLICATE_SHADOW_FILE_BROADCAST	Section 8.3, "Resolving Instances of Duplicate Files," on page 70

9.1.6 Shadow Volume Policies

Shadow volume policies manage how files are distributed across the shadow volume's primary and shadow areas. A Shadow Volume policy allows you to specify when the policy is enforced (one time, hourly, daily, weekly, and so on), which volumes the policy applies to, which direction files are moved (primary to shadow or shadow to primary), and which files are moved (file type, modify date, access date, size, and so on). Multiple policies can be applied to the same volumes and multiple policies can be scheduled to run concurrently.

For information about configuring global policies for DST, see Chapter 3, "Installing Dynamic Storage Technology," on page 31.

For information about creating or modifying Dynamic Storage Technology policies for shadow volumes, see Chapter 10, "Creating and Managing Policies for Shadow Volumes," on page 101.

9.1.7 File Inventory for the Shadow Volume

You can generate an inventory of the files located on the two volumes by selecting the *Inventory* link next to the primary volume on the Dynamic Storage Technology Options page. This provides statistics broken out for both volumes and for each volume separately. For information, see Section 11.3, "Viewing Statistics for the Shadow Volume," on page 124

9.1.8 Moving Specified Files between Volumes

The Inventory page allows you to navigate through the statistics reports to determine a list of files to be moved between the two volumes (primary to secondary, or secondary to primary). For information, see Section 11.4, "Using Inventory Detail Reports to Move, Copy, or Delete Files on the Shadow Volume," on page 124.

9.2 Creating a DST Shadow Volume with NSS Volumes

A DST shadow volume links two existing NSS volumes. Typically, one of the volumes contains data and one is newly created. For information about how to create NSS volumes, see the *OES 2 SP3: NSS File System Administration Guide for Linux*.

This section describes how to create unshared DST shadow volumes. For information about using shared NSS volumes to create a shared DST shadow volume in a cluster environment, see Chapter 13, "Configuring DST Shadow Volume Pairs with Novell Cluster Services," on page 139.

IMPORTANT: The following procedures use `VOL1` for the primary storage area, and `ARCVOL` as the secondary storage area. Ensure that you substitute the actual names of the NSS volumes you are using in each of the steps.

- Section 9.2.1, "Preparing the NSS Volumes for Use in the Shadow Volume," on page 80
- Section 9.2.2, "Disabling the NCP/NSS Bindings for the Secondary Volume," on page 81
- Section 9.2.3, "Adding a Shadow to the Primary NSS Volume," on page 82
- Section 9.2.4, "Moving Data between the Two Volumes," on page 83

9.2.1 Preparing the NSS Volumes for Use in the Shadow Volume

1 Open Novell Remote Manager for Linux in a Web browser, then log in to the DST server as the `root` user.

2 Select *View File System > Dynamic Storage Technology Options* to view a list of mounted volumes.

3 On the Dynamic Storage Technology page, ensure that the NSS volume that you want to use as the primary volume appears in the *Volume Information* list with a status of *Add Shadow*. If it is not listed, the NSS volume might be unmounted, or its NCP/NSS bindings might be disabled.

   3a Select *Manage NCP Services > Manage Shares* to view a list of active volumes.

   3b If the NSS volume is in the list but it is not mounted, the volume's name is not hyperlinked and a *Mount* button is located next to it.
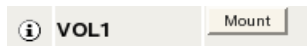
   To mount the volume, click the *Mount* button next to the volume name. Continue with Step 4.

   3c If the NSS volume does not appear in the list of active volumes, click *NCP/NSS Bindings* to view the *Available NSS Volumes* list. If the NSS volume is in the list, check the NCP/NSS Bindings parameter to see if it is disabled.

   If the *NCP Accessible* value is set to No, the volume's NCP/NSS binding is disabled. The most likely reason is that the volume is already being used as the secondary volume in another shadow volume. In that case, you must choose another volume to use as a primary volume.

   If you are certain that the volume is not being used in another shadow volume, you can enable the NCP/NSS Bindings setting:

      3c1 Select *Yes* in the *NCP Accessible* column for the NSS volume, then click *Save Selection* to save and apply the change.

      3c2 If the volume is not automatically mounted, select *Manage NCP Services > Manage Shares* to view the *Volume Information* list, then click the *Mount* button next to the volume name to mount it.

3d If the volume does not appear in the list of active volumes, and it does not appear on the NCP/NSS Bindings page in the *Available NSS Volumes* list, the volume probably is not mounted in NSS.

Exit Novell Remote Manager, then use NSSMU or the storage plug-in for Novell iManager to mount the volume in NSS. These tools automatically mount the volume for NSS and for NCP. When the volumes are mounted, return to Step 1 and begin again.

4 On the Dynamic Storage Technology page, ensure that the NSS volume that you want to use as the secondary volume appears in the *Volume Information* list with a status of *Add Shadow*.

The secondary volume must be mounted in NCP in order to perform the next step.

For example, the volume ARCVOL is the NSS volume that is planned to be used for the secondary volume. The volume is in the *Volume Information* list with a *Shadow Status* value of *Add Shadow*.

Volume Information		
Volume Name	**Shadow Status**	
ⓘ ARCVOL	Add Shadow	Inventory
ⓘ VOL1	Add Shadow	Inventory
ⓘ _ADMIN	No Shadow	Inventory
ⓘ SYS	Add Shadow	Inventory

5 (Optional) If the secondary volume contains data and the primary volume is a newly created volume, copy the trustee database file on the secondary volume to the primary volume before you create the shadow volume relationship.

Any existing file system trustee and rights settings on a secondary volume that contains data are not automatically re-used by DST for the shadow volume. Copying the existing trustee database allows you to leverage the current settings. Otherwise, you must reconfigure file system access rights from the merged view after you create the shadow volume.

For information, see Section 9.5, "Copying a Trustee Database to the Primary NSS Volume," on page 87.

6 Continue with Section 9.2.2, "Disabling the NCP/NSS Bindings for the Secondary Volume," on page 81.

9.2.2 Disabling the NCP/NSS Bindings for the Secondary Volume

1 Open Novell Remote Manager for Linux in a Web browser, then log in to the DST server as the root user.

2 Select *View File System > Dynamic Storage Technology Options* to view a list of mounted volumes.

3 Select *Manage NCP Services > Manage Shares*, click *NCP/NSS Bindings*.

4 In the *Available NSS Volumes* list, select *No* in the *NCP Accessible* column for the NSS volume that you want to use as the secondary volume.

Available NSS volumes		
NCP Accessible	**Volume Name**	**Mount point**
Yes: ○ No: ◉ Save Selection	ARCVOL	/media/nss/ARCVOL
Yes: ◉ No: ○ Save Selection	VOL1	/media/nss/VOL1

5 Click *Save Selection* to save and apply the change.

6 Go to the Dynamic Storage Technology page, and verify that the secondary volume (for example, ARCVOL) is no longer listed.

7 Continue with

9.2.3 Adding a Shadow to the Primary NSS Volume

1 Open Novell Remote Manager for Linux in a Web browser, then log in to the DST server as the root user.

2 Use one of the following methods to go to the volume's Share Information page of the NSS volume that you want to use as the primary storage area.

◆ Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page, then click the *Add Shadow* link next to the volume name of the NSS volume.

For example, click the *Add Shadow* link for VOL1.

Volume Information		
Volume Name	**Shadow Status**	
ⓘ VOL1	Add Shadow	Inventory
ⓘ _ADMIN	No Shadow	Inventory
ⓘ SYS	Add Shadow	Inventory

◆ Select *Manage NCP Services > Manage Shares* to open the Manage Shares page, then click the *Information* (i) icon next to the volume name of the NSS volume.

ⓘ **VOL1**   Unmount

3 On the volume's Share Information page, scroll down to the *Volume Tasks* area, then click *Add Shadow Volume*.

Volume tasks
Available Actions
Add Shadow volume

4 Specify the following information for the secondary storage area for the DST shadow volume, then click *Create* to define the shadow volume.

Create Shadow for Volume VOL1   �🛈

Shadow Path: _____

☐ Create if not present

_____

Create   Cancel

◆ **Shadow Path:** Type the Linux path for the NSS volume that you want to use as the secondary storage area. The default Linux path where NSS volumes are mounted is /media/nss/*volumename*.

For example, to specify the NSS volume named ARCVOL as the secondary storage area, type /media/nss/ARCVOL in the *Shadow Path* field.

◆ **Create If Not Present:** For NSS volumes, the volume must already exist. Make sure this option is deselected (not checked) when shadowing NSS volumes.

IMPORTANT: This option is a placeholder for future capabilities to support shadow volumes for NCP volumes on Linux POSIX file systems (such as Ext3, Reiser, and XFS).

---

5 On the volume's Share Information page, ensure that the *File System Shadow Path* information shows the shadow path you specified in Step 4.

6 Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page, then verify that the *Shadow Status* for the volume is set to *Shadowed* and the *View Log* link is available.

7 Continue with Section 9.2.4, "Moving Data between the Two Volumes," on page 83.

9.2.4 Moving Data between the Two Volumes

1 In Novell Remote Manager, select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page, then create one or multiple shadow volume policies for the shadow volume.

Shadow volume policies can be configured to move files according to the time since the file was last modified, accessed, or changed; by file names; by file types; or by file size. You can schedule policies to run automatically, or you can run them on demand.

For information about creating and scheduling shadow volume policies, see Chapter 10, "Creating and Managing Policies for Shadow Volumes," on page 101.

2 (Optional) Move selected data on demand by running customized inventory reports, then using the inventory detail reports to move selected files to either volume according to the time since the file was last modified, accessed, or changed; by file names; by file types; or by file size.

For information, see Section 11.4, "Using Inventory Detail Reports to Move, Copy, or Delete Files on the Shadow Volume," on page 124.

9.3 Giving Users a Merged View of the Shadow Volume

Users see a merged view of the data by accessing a share on the primary volume. The following user access is supported:

9.3.1 NCP

Configure file access for the NCP users on the primary NSS volume, just as you would for a single NSS volume. NCP automatically provides a merged view of the data.

9.3.2 Novell CIFS

Configure file access for the CIFS users on the primary NSS volume, just as you would for a single NSS volume. NCP automatically provides a merged view of the data.

9.3.3 Novell Samba with ShadowFS and FUSE

Configure file access for the Novell Samba users by configuring ShadowFS and FUSE, then create a share on the primary NSS volume. Linux Samba and the SMB/CIFS users must be enabled for Linux User Management.

For information, see Chapter 12, "Using ShadowFS to Provide a Merged View for Novell Samba Users," on page 129.

9.4 Configuring the NCP/NSS Bindings for an NSS Volume

The NCP/NSS Bindings parameter for an NSS volume governs whether the volume is automatically mounted on system restart in NCP Server. When the parameter is enabled, the NSS volume is automatically mounted for NCP Server. When it is disabled, the NSS volume is not mounted for NCP Server. The NCP/NSS Bindings parameter is enabled by default, making the volume NCP accessible.

NSS volumes are automatically mounted by default on system restart, first in NSS, then in NCP Server. This is the desired behavior for all independent NSS volumes that are not in shadow volumes, and for NSS volumes that you use as primary storage locations in a DST shadow volumes. When an NSS volume is used as the secondary storage area in a DST shadow volume, you want the NSS volume to be mounted in NSS, but not in NCP Server. This allows DST to control access to the secondary storage area via the primary storage area. Files in the secondary storage area cannot be directly accessed by users.

After you remove a shadow volume, the NCP/NSS Bindings parameter for the NSS volume that was used as the secondary storage area remains disabled until you enable it. You must enable the bindings and mount the volume in order to enable users to access the now independent volume.

9.4.1 Disabling the NCP/NSS Bindings for an NSS Volume

The volume's NCP/NSS Bindings parameter must be disabled for NSS volumes that you use as secondary storage locations in a DST shadow volumes.

1 In Novell Remote Manager for Linux, select *Manage NCP Services > Manage Shares*.

2 In the *Configuration* area of the NCP Shares page, click *NCP/NSS Bindings*.

Configuration
Create new share

Delete existing share

NCP/NSS Bindings
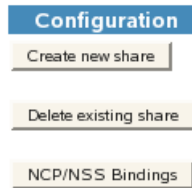
3 In the *Available NSS Volumes* list, locate the NSS volume that you want to disable.

4 In the *NCP Accessible* column, click *No* to make the NSS volume not accessible to NCP so that it is not mounted in NCP after it is mounted in NSS.

Available NSS volumes		
NCP Accessible	**Volume Name**	**Mount point**
Yes: ○ No: ● Save Selection	ARCVOL	/media/nss/ARCVOL
Yes: ● No: ○ Save Selection	VOL1	/media/nss/VOL1

5 Beneath the volume's setting for *NCP Accessible*, click *Save Selection* to save and apply the new setting.

6 Verify that the NSS volume is not available for NCP by selecting *Manage NCP Services > Manage Shares* to view a list of active volumes.

If the NCP/NSS Bindings parameter is successfully disabled, the NSS volume should not appear in the *Volume Information* list.

9.4.2 Enabling the NCP/NSS Bindings for an NSS Volume

The volume's NCP/NSS Bindings parameter must be enabled for NSS volumes that you use as primary storage locations in a DST shadow volumes, and for all independent NSS volumes that are not in shadow volumes. This is the default.

1 In Novell Remote Manager for Linux, select *Manage NCP Services > Manage Shares*.

Configuration
Create new share

Delete existing share
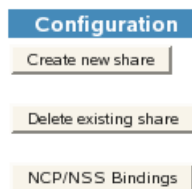
NCP/NSS Bindings

2 In the *Configuration* area of the NCP Shares page, click *NCP/NSS Bindings* to open the NCP/NSS Bindings page.

3 In the *Available NSS Volumes* list, locate the NSS volume that you want to enable.

4 If the volume's *NCP Accessible* setting is *No*, click *Yes* to make the NSS volume accessible to NCP so that the volume is automatically mounted in NCP after it is mounted in NSS.

5 Beneath the volume's setting for *NCP Accessible*, click *Save Selection* to save and apply the new setting.

The volume appears in the *Active Shares* list on the NCP Shares page.

6 Verify that the NSS volume is available for NCP by selecting *Manage NCP Services > Manage Shares* to view a list of active volumes.

If the NSS/NCP Bindings parameter is enabled, the NSS volume appears in the *Volume Information* list, and a *Mount* button is displayed next to it.

7 Click *Mount*.

When the volume is successfully mounted, the volume's name is hyperlinked, and an *Unmount* button is displayed next to it.

9.4.3 Enabling or Disabling NCP/NSS Bindings by Editing the /etc/opt/novell/ncp2nss.conf File

When the NCP/NSS bindings parameter is disabled for a volume, NCP Server adds an EXCLUDE_VOLUME entry to the `/etc/opt/novell/ncp2nss.conf` file. You can manually disable or enable the NSS volume's NCP/NSS bindings parameter by adding or removing this entry from the file, then restarting the NCP2NSS daemon.

1 Open the `/etc/opt/novell/ncp2nss.conf` configuration file in a text editor.

2 Do one of the following:

- **Disable the NCP/NSS Binding:** Add an EXCLUDE_VOLUME entry for the volume you plan to use as secondary NSS volume in order to exclude the volume from being automatically mounted for NCP Server.

  EXCLUDE_VOLUME *nss_volumename*

Replace *nss_volumename* with the name of the NSS volume. For example, to disable the bindings for the NSS volume named `ARCVOL:`, add the following line. Note that you do not include the colon after the volume name.

```
EXCLUDE_VOLUME ARCVOL
```

◆ **Enable the NCP/NSS Binding:** Locate the EXCLUDE_VOLUME entry for the NSS volume, then remove that line from the file.

3 Save the file.

4 Restart the Novell eDirectory daemon by entering the following commands:

```
rcndsd stop
```

```
rcndsd start
```

5 Restart the NCP/NSS IPC daemon to synchronize the changes you made to the `/etc/opt/novell/ncp2nss.conf` file:

5a At the terminal console prompt, enter

```
/etc/init.d/ncp2nss restart
```

5b If the NCP/NSS IPC daemon restarts successfully, the following messages are displayed in the terminal console:

```
Shutting down Novell NCP/NSS IPC daemon...
```

```
Exited
```

```
Starting the Novell NCP/NSS IPC daemon.
```

9.5 Copying a Trustee Database to the Primary NSS Volume

In a typical DST shadow volume, the primary volume contains data and the secondary volume is empty. If the secondary volume is the one with data, you should copy its existing trustee database to the primary volume before you create the shadow volume relationship. Otherwise, you must reconfigure the file system trustees and file access rights in the merged view before you allow users to access the shadow volume.

For all NCP volumes (NSS and NCP on Linux POSIX volumes), the trustee information is obtained at volume mount time from the `._NETWARE/.trustee_database.xml` file. For an NSS volume, the Linux path to the file is `/media/nss/*volumename*/._NETWARE/.trustee_database.xml`.

When the shadow relationship exists, all trustee changes are copied to both locations in order to keep the copies of the trustee information synchronized. When you remove a shadow volume, each volume has a complete copy of the trustee information.

1 In Novell Remote Manager, log in as the `root` user.

2 Select *Manage NCP Services > Manage Shares* to view a list of active volumes.

3 Dismount the NSS volumes that you will be using for DST from NCP Server by selecting the *Unmount* button next to each volume.

This dismounts the volumes from NCP, but they are still mounted by NSS.

4 In a file browser, rename or delete the `/media/nss/*primary_volumename*/._NETWARE/.trustee_database.xml` file on the primary volume.

5 Open a terminal console as the `root` user, then copy the trustee file from the secondary volume location to the primary volume location by entering the following at a terminal console prompt:

```
cp /media/nss/secondary_volumename/._NETWARE/.trustee_database.xml /media/nss/
primary_volumename/._NETWARE/.trustee_database.xml
```

For example:

```
cp /media/nss/ARCVOL/._NETWARE/.trustee_database.xml /media/nss/VOL1/
._NETWARE/.trustee_database.xml
```

6 Select *Manage NCP Services > Manage Shares* to view a list of active volumes.

7 Mount the primary volume and secondary volume for NCP Server by selecting the *Mount* button next to each volume.

8 At the terminal console prompt, enter the following command to synchronize the NSS trustee information that is now on the primary volume with NCP Server:

```
ncpcon nss resync=primary_volumename
```

9 Continue with .

9.6 Viewing a List of NCP Shares

In Novell Remote Manager, the NCP Server plug-in appears as the *Manage NCP Services* role in the left panel. This allows you to mount or unmount NCP volumes, NSS volumes, and DST shadow volumes from the NCP Server. Unmounting an NSS volume from NCP does not dismount the volume from NSS.

1 Open Novell Remote Manager, then log in to the DST server as the `root` user.

2 Use either of the following methods to view a list of NCP shares and their status:

   ◆ Select *Manage NCP Services > Manage Shares*.

   ◆ Select *View File System > Dynamic Storage Technology Options* to open the Volume Information report, then click *Share Management Home*.

9.7 Mounting and Dismounting DST Shadow Volumes

To mount or dismount the DST shadow volume for NCP Server, you mount or dismount the primary storage area. Unmounting an NSS volume from NCP does not dismount the volume from NSS.

To mount a shadow volume:

1 In Novell Remote Manager, click *Manage NCP Services > Manage Shares*, then click the *Mount* button next to the volume name of the primary storage area for the DST shadow volume you want to mount.
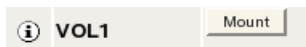
To dismount a shadow volume:

1 In Novell Remote Manager, click *Manage NCP Services > Manage Shares*, then click the *Unmount* button next to the volume name of the primary storage area for the DST shadow volume you want to dismount.
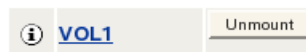
9.8 Viewing the Name and Path Information for a Shadow Volume

You can quickly get name and path information for the member volumes in the DST shadow volume by using the `ncpcon volume data` command.

1 Log in to the DST server as the `root` user, then open a terminal console.

2 At the terminal console prompt, enter

```
ncpcon volume data
```

This information is also available in Novell Remote Manager as described in Section 9.9.3, "Viewing the Share Information for a Shadow Volume," on page 90.

9.9 Viewing Information about a Shadow Volume

In Novell Remote Manager on the Dynamic Storage Technology Options page, the *Volume Information* report (as shown in Figure 9-1) contains information about all NCP volumes on the server. This includes NSS volumes (which are by default NCP volumes) and NCP shares on Linux POSIX file systems such as Ext3, Reiser, and XFS.

IMPORTANT: DST supports NSS volumes to be used in shadow volumes at this time.

Figure 9-1 *Volume Information Report*

The report does not distinguish between the underlying file systems for the NCP volumes. Make sure you create shadows only for NCP volumes based on the NSS file system. You can identify whether a volume is an NSS volume by clicking the *Information* icon next to the volume name, then viewing its underlying file system type.

To understand the information provided in the report, see the following sections:

- Section 9.9.1, "Accessing the Volume Information Report," on page 90
- Section 9.9.2, "Viewing the Shadow Status of a Volume," on page 90
- Section 9.9.3, "Viewing the Share Information for a Shadow Volume," on page 90

9.9.1 Accessing the Volume Information Report

1 Open Novell Remote Manager, then log in as the `root` user.

2 Select *View File System > Dynamic Storage Technology Options* to open the Volume Information report.

9.9.2 Viewing the Shadow Status of a Volume

In the *Volume Information* report, the *Shadow Status* column displays whether or not a volume has a shadow. There are three states:

Table 9-2 *Shadow Status in the Volume Information Report*

Shadow State	Description
No Shadow	The NSS `_ADMIN` volume cannot be shadowed, and displays a status of No Shadow.
Add Shadow	The volume is an NSS volume or an NCP volume that is eligible for shadowing. You must separately verify that the volume satisfies the guidelines and caveats that are specified in Chapter 5, "Planning for DST Shadow Volumes and Policies," on page 41. **IMPORTANT:** Select the *Add Shadow* link only for NCP volumes where the underlying file system is the NSS file system.
Shadowed	The volume is the primary volume in a DST shadow volume. To identify the secondary storage area for this volume, click the *Information* icon next to the volume name to go to the Share Information page, then view the *File System Shadow Path*.

9.9.3 Viewing the Share Information for a Shadow Volume

The Share Information page displays details about the NCP volume, such as its Linux file system path, the file system path of its shadow area (if it is shadowed), the file system type, and capacity.

Figure 9-2 *NCP Volume Share Information*

VOL1 Share Information

Information	
Description	**Value**
File system path	/media/nss/VOL1
File system shadow path	/media/nss/ARCVOL
File system type	NSS
NCP volume ID	2
Status	mounted, online, NSS, salvageable
Capacity	488.51 MB
Local cache	

Parameter	Value
trustee count	0
cached files	9
evicted files	0
cached folders	7
cache retrieved	59
cache retrieved locked	7

Pool name	POOL1
Pool attributes	2833362296
GUID	5f63e720-6afb-01dc-80-00-ac7e4c66ba5f

Table 9-3 describes each of the reported parameters on the Share Information page:

Table 9-3 *NCP Volume Share Information*

Parameter	Description
File System Path	The mount point of the selected volume.
File System Shadow Path	If the selected volume is shadowed, this is the mount point of its secondary storage area.
File System Type	The underlying file system type, such as NSS, Ext3, Reiser, or XFS.
NCP Volume ID	The unique identifier given to the volume by the NCP engine. Values range between 0 and 254 (up to 255 volumes mounted concurrently).
	When the primary volume has a state of *Shadowed*, its NCP volume ID represents the DST shadow volume pair of volumes. There is not a separate NCP volume ID assigned to the secondary volume while it is in the shadow volume relationship.
Status	The status of the selected volume, such as if it is mounted and online or offline for the NCP engine. For NSS volumes, it also shows which attributes are enabled, such as user quotas, directory quotas, and salvage.
Capacity	The total amount of space allocated to the volume.

Parameter	Description
Advanced Information	Click *View* to reveal the following information: **Local Cache:** Shows the current status of cache parameters, such as trustee count, cached files, evicted files, cached folders, cache retrieved, and cache retrieved locked. **Pool Name:** For NSS, the name of the NSS pool where the volume resides. **Pool Attributes:** For NSS, the attribute identifier for the volume's pool. **GUID:** The Novell eDirectory globally unique identifier for the selected volume.
Open Files	Reports the connection number (station) of the NCP client connection, the typeless fully distinguished eDirectory user name (such as user name.context) who opened the connection, and the files that are currently open for that connection. You manage NCP connections to the primary storage area of the DST shadow volume. Users do not connect directly to the secondary storage area. To manage connections, go to the *Manage NCP Services* role, then click *Manage Connections*.

9.10 Auditing File Move Events for the Shadow Volume

For volumes with a *Shadow Status* of *Shadowed*, all file moves between the primary volume and the secondary volume are logged to the shadow volume's audit file. An audit log for a DST shadow volume is located in the `._NETWARE` directory located at the root of the primary volume. For NSS volumes, the default file path for the log is `/media/nss/`*volumename*`/._NETWARE/`*volumename*`.audit.log`.

For example, if the primary area is named `VOL1`, the audit file is `/media/nss/`*VOL1*`/._NETWARE/`*VOL1*`.audit.log`.

1 In Novell Remote Manager for Linux, log in as the `root` user.

2 Select *View File System > Dynamic Storage Technology Options*, locate the volume in the list, then click the *View Log* link next to it.

Volume Information			
Volume Name	**Shadow Status**		
ⓘ VOL1	Shadowed	Inventory	View Log
ⓘ _ADMIN	No Shadow	Inventory	
ⓘ SYS	Add Shadow	Inventory	

3 When you are prompted, select whether to view the file in a text editor, or to save a copy to your local computer.

The "local computer" is the computer where you are running the Web browser for accessing the server via Novell Remote Manager.

9.11 Backing Up DST Shadow Volumes

9.11.1 Planning Your Backup Solution

Applications that directly access the local Linux file system see the primary file tree and the secondary file tree as independent directories. The backup utility does not see the merged view of the file tree that the end user sees. Thus, backup tools can apply one backup policy to the primary file tree and a different backup policy to the secondary file tree. In a DST volume, the only operations that take place directly on the secondary volume are backup (or remove and archive) and restore functions.

Using shadow volumes allows backups of important data to be made faster and more frequently because you can apply different backup policies for the primary volume and secondary volume.

For example, the server administrator can partition the volume's data into two categories:

- Important data that needs to be maintained on quality storage and backed up frequently.
- Less important data that can be stored on less expensive storage and backed up less frequently.

An analysis or inventory of a volume's data shows that a large portion of it is seldom used. Having a shadow volume allows the server administrator to spend more on the most important data and spend less on the less important data. The frequently used data can be backed up nightly. The seldom-used data can be backed up weekly or monthly.

Getting the less important data out of the way enables the backups of your important data to run more quickly and efficiently. Partitioning your data in this way can significantly reduce the cost of hosting it.

Because the most important files are located in the primary storage area, disaster recovery can also be faster. The server administrator can restore the critical files by restoring the primary storage area first, then restore the secondary storage area. This lets users quickly get the files they need most, and they do not need to wait while files they do not usually need are restored. In addition, more fault tolerant replication solutions can be deployed for the primary storage area where it matters most.

Ensure that policies are not being run during the backup window.

9.11.2 Planning Your Restore Solution

You can restore the data separately to each volume by using the backups you made of each area. If ShadowFS is running, you can also restore the data by using the ShadowFS local mount point in `/media/shadowfs/`*`volumename`* that presents a merged file tree that includes both volumes. The advantages and disadvantages of each restore option are described below.

- "Restoring Data Separately to the NSS Volumes" on page 94
- "Restoring Data to the ShadowFS File Tree" on page 94

Restoring Data Separately to the NSS Volumes

Consider the following advantages and disadvantages when restoring data separately to the NSS volumes. You restore data backed up from the primary path to the primary NSS volume. You restore data backed up from the secondary path to the secondary NSS volume.

- "Advantages" on page 94
- "Disadvantages" on page 94

Advantages

- Files are restored directly to the primary volume and secondary volume where they were when the files were backed up, so there is no need for the information to be transferred again through policies.
- There is no performance hit when you restore directly to each volume like there is when restoring to the ShadowFS file tree.
- The restoration size is not an issue because you are restoring to the proper volume rather than though the ShadowFS file tree view.
- You can back up the NSS volume by using the NSS Extended Attributes (XAttr) settings to preserve the NetWare metadata (netware.metadata) for file system rights and attributes, and restore that information to each volume as you restore data. For information about XAttr, see "Extended Attributes (XAttr) Commands" the *OES 2 SP3: NSS File System Administration Guide for Linux*.

Disadvantages

- Make sure no policy runs are in progress while data is being restored.
- Potential conflicts might occur if you restore duplicate versions of the file on each of the volumes. The duplicate files are resolved by DST global policies instead of being resolved by the backup software. By default, the duplicate files are allowed to coexist, and a conflict message is broadcast to users. For information about duplicate file resolution, see Section 8.3, "Resolving Instances of Duplicate Files," on page 70.
- When you restore partial data, you need to know whether the most recent version of the data is located on the backup for the primary volume or the secondary volume.

Restoring Data to the ShadowFS File Tree

If ShadowFS is running, you can also restore the data by using the ShadowFS local mount point in /media/shadowfs/*volumename* that presents a merged file tree that includes both volumes.

- "Advantages" on page 94
- "Disadvantages" on page 94

Advantages

- The backup software sees both volumes through the merged file tree view. You can restore the primary volume and secondary volume through this view, and let any duplicates be handled by your backup software.

Disadvantages

- Make sure no policy runs are in progress while data is being restored.

- The FUSE technology used by ShadowFS is slower than using the NCP view, but the backup software cannot see the NCP view.

- If you back up the NSS volume by using the NSS Extended Attributes (XAttr) settings to preserve the NetWare metadata (netware.metadata) for file system rights and attributes, this information cannot be restored through the shadowfs merged view of the data because XAttr requires that the destination location be an NSS volume. The shadowfs view is a mount point and is not seen by the backup software as an NSS volume. For information about XAttr, see "Extended Attributes (XAttr) Commands" the *OES 2 SP3: NSS File System Administration Guide for Linux*.

- All files restored through the ShadowFS file tree view are copied to the primary volume. The data that you restore from the backup for the secondary volume is not returned to the secondary volume until you run policies or use inventory scans to move the data back to the secondary volume.

- Because all data is restored to the primary volume when you restore through the ShadowFS file tree view, it is possible to run out of space. The primary volume must be large enough to accommodate holding both volumes worth of data unless you restore in phases; that is, restore some directories, then shift data to the secondary, then restore more directories.

9.11.3 Using the /etc/NCPVolumes XML File for Backup

A backup utility can use the /etc/NCPVolumes XML file to easily locate each mounted NCP volume and find its primary and secondary file trees. The file contains an entry for each mounted volume. It lists the volume's name and the path for the volume's primary file tree (PRIMARY_ROOT). If the volume is a shadow volume, it also shows the path for the secondary file tree (SHADOW_ROOT).

For example, the following XML entry defines the DST shadow volume named VOL1. The volumes are NSS volumes, with VOL1 as the primary storage location, and ARCVOL as the secondary storage location.

```
<VOLUME>

    <NAME>VOL1</NAME>

    <PRIMARY_ROOT>/media/nss/VOL1</PRIMARY_ROOT>

    <SHADOW_ROOT>/media/nss/ARCVOL</SHADOW_ROOT>

</VOLUME>
```

9.11.4 Configuring the Backup Attribute for NSS Volumes

You can use Novell Storage Management Services tools for backup and restore of NSS volumes. You can back up each NSS volume separately, and restore them separately. You need to be aware of the relationship on restore because you can get duplicate files. However, the mechanics of the backup and restore with SMS are the same as they are with any NSS volume. Refer to the SMS documentation for information about how to use SMS for NSS backup and restore.

The NSS Backup attribute must be enabled on the NSS volumes if you use SMS tools for backup of NSS volumes. The attribute is enabled by default when you create a new NSS volume.

To enable the Backup attribute for an existing NSS volume:

1 In iManager, click *Storage > Volumes*.

2 Select a server to manage to view a list of the NSS volumes on it.

3 In the *Volumes* list, select the volume that you want manage, then wait for the page to refresh to show the volume's details.

4 Click *Properties* to view the settings for the volume attributes.

5 On the *Attributes* tab, select the *Backup* attribute, then click *Apply*.

9.11.5 Configuring a Backup for Trustee Information on NSS Volumes on Linux

If you plan to use a backup utility with DST, you might need to add an NSS attribute that allows for backing up and restoring file system trustee assignments, trustee rights, and inherited rights filters. NSS provides the nss /ListXattrNWMetadata switch to enable this capability. For information, see "ListXattrNWmetadata Option" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

9.12 Removing the Shadow Relationship for a Non-Clustered DST Shadow Volume

Removing a DST shadow volume simply removes the relationship between the primary and secondary storage area. It does not remove the underlying volumes themselves. The files remain on whichever storage area they are on at the time when you remove the shadow relationship.

- Section 9.12.1, "Preparing to Remove a Shadow Volume," on page 96
- Section 9.12.2, "Removing the Shadow Volume Relationship by Using Novell Remote Manager," on page 97
- Section 9.12.3, "Removing a Shadow Volume by Editing Configuration Files," on page 98

IMPORTANT: If you are using clustered shadow volumes or remote volumes, use the procedures in the following sections:

- Section 13.9, "Removing the Shadow Relationship for a Clustered DST Volume Pair," on page 168
- Section C.7, "Removing a Shadow Relationship with a Remote NSS Volume," on page 209
- Section 13.9.3, "Removing the Shadow Definition and NCP/NSS Bindings Exclusion on All Nodes," on page 170.

9.12.1 Preparing to Remove a Shadow Volume

Before you remove a shadow volume relationship, ensure that you shift data between the two volumes that make up the shadow volume, according to where you want the data to reside after the DST shadow volume relationship is removed.

1 In Novell Remote Manager for Linux, log in as the root user.

2 Select *View File System > Dynamic Storage Technology Options*, locate the volume in the list, then click the *Inventory* link next to it.

View the volume inventory for the shadow volume to determine the space in use and the available space for both the primary and the secondary areas of the shadow volume. Ensure that there is sufficient fee space available in either location for the data that you plan to move to that location.

3 Use any combination of the following techniques to shift data between the two areas:

- ◆ **Shadow Volume Policies:** Run an existing shadow volume policy by using the *Execute Now* option in the *Frequency* area of the policy. You can also create a new shadow volume policy that moves specific data, and run the policy by using the *One Time* and *Execute Now* options in the *Frequency* area of the policy.

  For information about configuring policies to move data between the primary and secondary areas, see Chapter 10, "Creating and Managing Policies for Shadow Volumes," on page 101.

- ◆ **Inventories:** Use the detailed inventory reports or customized inventories to move specific files to either area.

  For information about using the volume customized inventory options to move data between the primary and secondary areas, see Section 11.5, "Generating a Custom Inventory Report," on page 125.

9.12.2 Removing the Shadow Volume Relationship by Using Novell Remote Manager

1 In Novell Remote Manager for Linux, log in as the `root` user.

2 Select *Manage NCP Services > Manage Shares* to go to the NCP Shares page.

3 Ensure that you know which NSS volume is being used as the secondary volume so that you can manage it independently later.

   3a On the NCP Shares page, locate the primary NSS volume in the *Active Shares* list, then click the *Information* icon next to the share name.

   3b On the primary volume's Share Information page, view the volume information in the *File System Shadow Path*.

   In the following example, `ARCVOL` is an NSS volume that is the secondary storage area in the shadow volume.

File system path	/media/nss/VOL1
File system shadow path	/media/nss/ARCVOL

4 On the NCP Shares page, locate the primary NSS volume in the *Active Shares* list, then click the *Unmount* button next to the share name.

ⓘ **VOL1**   Unmount

5 On the Manage Shares page, click the *Information* (i) icon next to the volume name of the NSS volume to access the *Remove Shadow Action Options*.

ⓘ **VOL1**   Mount

6 On the volume's Share Information page under *Volume Tasks > Remove Shadow Action Options*, click *Remove Shadow*.

VOL1 Share Information

Volume tasks
Available Actions

Remove Shadow

Share Management Home

After the shadow volume is removed, the page refreshes to report a successful removal.

Remove Shadow from Volume VOL1

Volume task has completed successfully

Share management

7 Select *Share Management* to go to the NCP Shares page, locate the volume that was the primary volume in the *Active Shares* list, then click the *Mount* button next to it.

ⓘ **VOL1**   Mount

8 Verify that the shadow volume was removed by using one of the following methods:

◆ Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page. The former primary volume now has an *Add Shadow* link next to it instead of a *Shadowed* link.

Volume Information		
Volume Name	**Shadow Status**	
ⓘ VOL1	Add Shadow	Inventory
ⓘ _ADMIN	No Shadow	Inventory
ⓘ SYS	Add Shadow	Inventory

◆ Select *Manage NCP Services > Manage Shares*, then click the *Information* icon next to the former primary volume's name. The *File System Shadow Path* field displays n/a (not applicable).

File system path	/media/nss/VOL1
File system shadow path	n/a

9 Enable the NCP/NSS Bindings on the volume that was used as the secondary volume (for example, `ARCVOL`) in order to mount the volume for NCP.

For information, see Section 9.4.2, "Enabling the NCP/NSS Bindings for an NSS Volume," on page 85.

9.12.3 Removing a Shadow Volume by Editing Configuration Files

1 Open a terminal console, then log in as the `root` user.

2 Edit the `/etc/opt/novell/ncpserv.conf` file to remove the following entry for your volume, then save your changes.

```
SHADOW_VOLUME primary_volumename secondary_volume_path
```

For example:

```
SHADOW_VOLUME VOL1 /media/nss/ARCVOL
```

3 Stop and restart the eDirectory `ndsd` daemon for the changes to take effect by entering

```
/etc/init.d/ndsd stop
```

```
/etc/init.d/ndsd start
```

4 Make the secondary NSS volume available for mounting in NCP by removing the EXCLUDE_VOLUME entry for the volume in the `/etc/opt/novell/ncp2nss.conf` file.

If necessary, edit the `/etc/opt/novell/ncp2nss.conf` file to remove the following entry for it:

```
EXCLUDE_VOLUME nss_volumename
```

An entry is automatically removed from the `/etc/opt/novell/ncp2nss.conf` file by using Novell Remote Manager for Linux to set the *Manage NCP Services > Manage Shares > NCP/NSS Bindings > NCP Accessible* option to Yes for the NSS volume. For instructions, see Section 9.4.2, "Enabling the NCP/NSS Bindings for an NSS Volume," on page 85.

5 Stop and restart the eDirectory `ndsd` daemon for the changes to take effect by entering

```
/etc/init.d/ndsd stop
```

```
/etc/init.d/ndsd start
```

6 Restart the NCP/NSS IPC daemon to synchronize the changes you made to the `/etc/opt/novell/ncp2nss.conf` file.

    6a At the terminal console prompt, enter

```
/etc/init.d/ncp2nss restart
```

    6b If ncp2nss restarts successfully, the following messages are displayed in the terminal console:

```
Shutting down Novell NCP/NSS IPC daemon...
```

```
Exited
```

```
Starting the Novell NCP/NSS IPC daemon.
```

10 Creating and Managing Policies for Shadow Volumes

This section describes how to configure and manage Dynamic Storage Technology policies for shadow volumes on a Novell Open Enterprise Server (OES) 2 Linux server.

For information about setting global policies for DST on the server, see Chapter 3, "Installing Dynamic Storage Technology," on page 31.

10.1 Understanding Shadow Volume Policy Options

Shadow Volume policies manage how files are distributed across the shadow volume's primary and secondary areas. A Shadow Volume policy allows you to specify when the policy is enforced (one time, hourly, daily, weekly, and so on), which volumes the policy applies to, which direction files are moved (primary area to its secondary area, or secondary area to its primary area), and which files are moved (by file name, file type, time stamps, or file size).

DST policies are configured in Novell Remote Manager for Linux. DST provides the following policy options:

10.1.1   Last Executed

For an existing policy, the *Last Executed* parameter reports the last time the policy ran successfully. This parameter is not configurable.

10.1.2   Description

Description is the user-defined name for the policy. It should be descriptive of the policy it represents, and meaningful to the administrator. This name appears in the *Dynamic Storage Technology Policies* table on the main *Dynamic Storage Technology Options* page.

Description (required): [   ]

10.1.3   Start Time

Start Time specifies the time of day to begin a run to enforce the policy. For hourly policies, the policy enforcement begins at the selected minutes past each hour. Time is specified based on a 24-hour clock. For example, 18:00 (6:00 p.m.) is the default start time.

Start Time: [18 ▼] : [00 ▼]

10.1.4   End Time

End Time specifies the time of day to stop work on an enforcement run. Specifying an end time for a scheduled run allows you to prevent policy enforcement from happening during busy work hours. Time is specified based on a 24-hour clock. For example, 07:00 (7:00 a.m.) is the default end time.

End Time: [07 ▼] : [00 ▼]

If the policy enforcement process is still running when the end time is reached, the policy's queued work is paused until the next scheduled run. When the policy run begins at its next scheduled time, it continues with the queued work, and adds new work to the end of the queue.

10.1.5   Start Day

For policies that run weekly, *Start Day* specifies the day of the week to enforce the policy. You can specify only one day of the week for a given policy. Options are *Saturday* (default), *Sunday*, *Monday*, *Tuesday*, *Wednesday*, *Thursday*, or *Friday*.

Start Day: [Saturday ▼] (for weekly commands)
                     [January ▼] [01 ▼] (for one time or monthly commands)

For policies that are run one time or monthly, *Start Day* specifies the month and day of the month when the policy is scheduled to be enforced.

10.1.6   Frequency

Frequency specifies how often the policy is enforced when the *Command Status* is set to *Active*. Table 10-1 describes each frequency option. The *Execute Now* option can be selected or deselected in combination with any one of the scheduled frequency options.

Frequency:
- ○ One Time
- ○ Hourly
- ○ Daily
- ● Weekly
- ○ Monthly
- ☐ Execute now

Table 10-1   *Frequency Options for DST Policies*

Option	Description
One Time	Whenever the policy's *Command Status* is set to *Active*, the policy runs one time, then changes the *Command Status* to *Inactive*. You can activate the policy to run again by changing its status.
Hourly	The policy enforcement process runs once each hour. It begins at the number of minutes past the hour specified by the *Start Time*. The process continues until it is done, or until the number of minutes past the hour specified by the *End Time*. Unfinished work is queued until the next run.
Daily	The policy enforcement process runs once each day. It begins at the time specified by the *Start Time*. The process continues until it is done, or until the time specified by the *End Time*. Unfinished work is queued until the next run.
Weekly (default)	The policy enforcement process runs once each week. It begins on the day of the week specified by the *Start Day*. The process continues until it is done, or until the time specified by the *End Time*. Unfinished work is queued until the next run.
Monthly	The policy enforcement process runs once each month. It begins on the month and day specified by the *Start Day*, then it runs every month afterwards on that day of the month. The process continues until it is done, or until the time specified by the *End Time*. Unfinished work is queued until the next run.
Execute Now	Select this option to run the policy now, in addition to its regularly scheduled runs. The policy enforcement process is initiated within a few minutes after the policy's *Command Status* is set to *Active* and saved (submitted). The process continues until it is done, or until the time specified by the *End Time*. Unfinished work is queued until the next run.

10.1.7   Command Status

Command Status governs whether a policy is actively enforced or inactive. Inactive policies can be changed back to active. New policies can be created and set to inactive without running them. Options are *Active* (default) and *Inactive*.

Command Status:
- ● Active
- ○ Inactive

10.1.8 Volume Selection

Volume Selection allows you to specify the shadow volumes affected by a given policy. You can select one or multiple shadow volumes from a drop-down list of existing shadowed volumes, or select *All Shadowed Volumes*. You can have multiple policies associated with a given shadow volume. A given policy can apply to multiple shadow volumes.

Volume Selection:

All Shadowed Volumes ▼

When you work with DST shadow volumes in a cluster, you should create separate policies for the shadow volumes that exist in a given cluster resource. A given policy can apply to multiple shadow volumes in the cluster resource. You can have multiple policies associated with a given shadow volume in the cluster resource.

10.1.9 Volume Operations

Volume Operations specifies the direction the files are moved between the primary storage location (primary area) and the secondary storage location (shadow area).

Volume Operations:

⦿ Move selected files from primary area to shadow area.

○ Move selected files from shadow area to primary area.
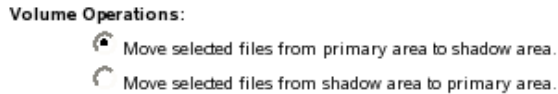
Table 10-2   *Volume Operations for a Policy*

Option	Description
Move selected files from primary area to shadow area (default)	When the policy is enforced, all files on the primary storage location that meet all of the search criteria are moved from the primary storage location to the secondary storage location.
Move selected files from shadow area to primary area	When the policy is enforced, all files on the secondary storage location that meet all of the search criteria are moved from the secondary storage location to the primary storage location.

10.1.10 Subdirectory Restrictions

In the *Subdirectory Restrictions* area, you specify the *Scope* and *Subdirectory List* information that determines whether the policy applies to everything in a volume, only to a specified directory (and its contents), or to all directories but the one specified.

Subdirectory Restriction:

Scope: Exclude subdirectory

Subdirectory list: (Example: /subdir1/subdir2)

/finance/mydatabase

of???arc

/projects/project abc/dev

The *Scope* options allows you to specify included paths or excluded paths in a given policy, but not both. Table 10-3 describes the options for *Scope*:

Table 10-3 *Subdirectory Restrictions for the Scope of a Policy*

Option	Description
None (default)	The policy is enforced for all subdirectories in the volume. Do not specify a path.
Apply only in subdirectory	The policy is enforced only for a specified subdirectory and its contents. You can specify multiple paths to be included when running the policy.
Exclude subdirectory	The policy is enforced for all subdirectories in the volume, except for the specified subdirectory and its contents. You can specify multiple paths to be excluded when running the policy. For OES 2 with the latest patches applied, the Exclude Subdirectory option also allows you to specify a directory name that might exist in multiple places on a volume. You indicate this intended action by specifying only a directory name with no forward slashes, and the directory name must contain at least one wildcard (such as ? and *). All instances of directories that match the specified directory name are excluded from the policy run.

The *Subdirectory List* allows up to 8 subdirectory paths on the primary volume to be specified for being included or excluded in a policy when it runs. Each additional path that you specify requires another pass through the data, so it increases the time needed to enforce the policy.

Specify the subdirectory paths relative to the root of the DST volume, not the full Linux path. Wildcards are not allowed in a subdirectory path. Each path must point to a valid subdirectory in the file system.

Precede subdirectory paths with a forward slash (/). For example:

```
/subdir1/subdir2
```

Directory names with spaces in them are supported in the subdirectory paths. For example:

```
/projects/project abc/dev
```

For OES 2 SP3 with the latest patches applied, the Exclude Subdirectory option supports using wildcards to specify a directory that might exist in multiple places on a volume. For example, to exclude all GroupWise archive subdirectories, specify the following directory name with wildcards:

```
of???arc
```

Table 10-4 demonstrates how to take advantage of the ability to specify subdirectory paths and directories that have multiple occurring instances in the DST volume.

Table 10-4   *Sample Extended Subdirectory Entries and Intended Actions*

Exclude Subdirectory Entry	Intended Action for the Policy
/test	The preceding forward slash indicates that this is a subdirectory path relative to the root of the volume. This entry excludes only the /test directory located at the root level of the DST volume.
tes?	The absence of a forward slash and the presence of a question mark wildcard (?) in the directory name indicates that this is a directory that might have multiple instances as subdirectories in the volume. This entry excludes all instances of directories with 4 characters in the name that match the first 3 characters, and any character in the 4th position of the directory name.
tes*	The absence of a forward slash and the presence of an asterisk wildcard (*) in the directory name indicates that this is a directory that might have multiple instances as subdirectories in the volume. This entry excludes all instances of directories with names of any length that match the first 3 characters, and any characters to the end of the directory name.
test	No actions are taken for this entry. It is not preceded by a forward slash, so it does not qualify as a subdirectory path. It does not contain a wildcard, so it does not qualify as a directory entry.

10.1.11   Search Criteria

Files must match all of the specified criteria in order to be moved between the primary storage location and secondary storage location. Criteria options include file name or extension, time stamp, and file size. The conditions are combined (and-ed) together, which means that all conditions must be true for a file before it is queued for moving to the other location. Specify any of the following search criteria:

Search Pattern

Search Pattern allows you to set criteria based on the file name or extension. You can specify characters and wildcards to search by file name. You can specify files by types by specifying a wildcard and an extension, such as *.mp3. The default entry is *.*, which applies the policy to all file names and all file types.

Search Pattern: *.*

You can specify up to 50 extensions in a given policy. Separate the multiple entries with a comma and no spaces. For example, to specify multiple image file extensions, type the following:

```
*.bmp,*.jpg,*.png,*.tif
```

For OES 2 SP3 with the latest patches applied, you can specify files with spaces in the name. Enter the file name without quotes.

```
filename with spaces.txt,another file with spaces.jpg,yet another file.doc
```

Time Stamp Restrictions

Time Stamp Restrictions identifies which time stamps to use when applying the policy.

Time Stamp Restrictions:
  Time Stamp:
        ☐ Last Modified Time
        ☐ Last Accessed Time
        ☐ Last Changed Time
  Time from now:
        Direction: [⩥ Greater than ▼]
        Days: [o ▼]
        Weeks: [o ▼]
        Months: [o ▼]
        Years: [o ▼]

The time stamp types are:

- ◆ **Last Time Modified:** Time of last content modification for the selected file.
- ◆ **Last Time Accessed:** Time of last access.
- ◆ **Last Time Changed:** Time of last file status change.

The default is no time restriction (all Time Stamp options are deselected), so the default policy applies the policy for all existing files.

These time stamps are defined by POSIX and supported by Linux. Many operations change more than one time stamp. NCP can modify the access time and the modify time, but cannot control whether the change time is reset. The Last Time Changed value is controlled automatically. For example, if you copy a file from one location to another, NCP preserves the access and modify times, but the change time is reset because the file's path changed. That is, it had a status change but the file was not opened for access and its data was not modified.

You must also specify the specific time period to use in *Time from Now*. Direction options are *Greater than* and *Less than*. Specify a direction, then select one of the time periods described in Table 10-5.

Table 10-5 *Time Periods for the Time Stamp Restrictions in a Policy*

Option	Description
Days	Specify 0 to 14 days. 0 days (the default) disables the option.
Weeks	Specify 0 to 10 weeks. 0 weeks (the default) disables the option.
Months	Specify 0 to 24 months. 0 months (the default) disables the option.
Years	Specify 0 to 24 years. 0 years (the default) disables the option.

For example, you can select all files that have a modified time greater than 6 months by selecting *Last Time Modified* in the *Time Stamp* field, *Greater than* for the *Direction* field, and 6 in the *Months* field.

File Size Restriction

Specifies the range of file sizes to search. *Direction* specifies to look for files that are greater than or less than the specified size in KB. Specify a value of 0 KB to disable the file size restriction. The default is no size restriction, which applies the policy for files of all sizes.

File Size Restriction:
Direction: Greater than ▼
Size (KB): 0

10.1.12 Stop

Beginning in OES 2 SP3 Linux, a *Stop* button is available on the policy's View/Edit Shadow Volume policy page when the policy is running. You can use this option to stop an individual currently running policy. For information, see Section 10.7, "Stopping a Running Policy," on page 113.

You can stop all currently running policies by using the *Stop all currently running policies* option on the Dynamic Storage Technology Options page.

10.2 Creating a Shadow Volume Policy

10.2.1 Prerequisite

In order to configure policies that apply only to a specific shadow volume, the shadow volume must already be defined.

10.2.2 Guidelines for Shadow Volume Policies

◆ For each Dynamic Storage Technology shadow volume, you must establish at least one policy that controls how files are migrated from the primary storage area to the secondary storage area of the shadow volume, or vice versa.

◆ Any given shadow volume policy is best kept to a simple goal. Complex combinations of rules in a single policy can lead to confusion on how they are executed.

◆ You can have multiple policies associated with a given shadow volume.

◆ A given policy can apply to multiple shadow volumes.

◆ Multiple policies can be scheduled to be run concurrently.

10.2.3 Creating a Shadow Volume Policy

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

Initially, no policies are defined, so you do not see a policy report.

After one or more policies are defined, the policies are reported in a table.

2 Beneath the list of *Dynamic Storage Technology Policies*, click *Create a New Policy* to open a page where you can configure a new storage policy.

3 On the *Create New Shadow Volume Policy* page, specify a name for the policy in the *Description* field.

The name should be descriptive of the policy it represents, and meaningful to the administrator.

For example, suppose you plan to create a policy for a shadow volume used by Project ABC, and exclude the path to the `contracts` directory. You might name the policy *Project ABC Exclude* `contracts`.

4 On the *Create New Shadow Volume Policy* page, configure policy settings.

For information about policy options, see Section 10.1, "Understanding Shadow Volume Policy Options," on page 101.

5 Specify the *Command Status* as *Active* or *Inactive*.

A policy's state must be active in order for it to run.

6 If you want the policy changes to be enforced sooner than the next scheduled run, ensure that you select *Execute Now* in the *Frequency* area.

The process is triggered for a run within a few minutes after you save (submit) the policy.

7 Click *Submit* (at the bottom of the page) in order to save the policy, and to schedule it if it is active.

The new policy is listed in the *Dynamic Storage Technology Policies* report on the Dynamic Storage Technology Options page.

Dynamic Storage Technology Policies			
Name	**Volume**	**Last Executed**	**Total Files Moved**
ProjectABC Exclude contracts	All Shadowed Volumes	Not executed	0

Create a new policy

10.3 Modifying a Shadow Volume Policy

You can modify a shadow volume policy at any time. For example, if the planned migration activity for a policy is not completed in the allowed time, you can adjust the policy run times and frequency until it meets your workload needs. Modified policies take effect the next time the policy runs, and do not affect currently running processes.

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

Dynamic Storage Technology Policies			
Name	**Volume**	**Last Executed**	**Total Files Moved**
ProjectABC Exclude contracts	All Shadowed Volumes	Not executed	0

Create a new policy

2 In the list of *Dynamic Storage Technology Policies*, click the *Name* link for the policy in order to view and modify the individual settings for the policy.

3 On the View/Edit Shadow Volume Policy page, view and modify the policy settings.

For information about policy settings, see Section 10.1, "Understanding Shadow Volume Policy Options," on page 101.

4 Specify the *Command Status* as *Active* or *Inactive*.

A policy's state must be active in order for it to run.

5 If you want the policy changes to be enforced sooner than the next scheduled run, ensure that you select *Execute Now* in the *Frequency* area.

If the policy is not currently running, the policy runs within a few minutes after you click *Submit* in Step 6.

If the policy is currently running, the updated policy does not run until the current run stops. That means the updated policy process is triggered within a few minutes after the currently running process completes or reaches the previously set *End Time*.

6 If you make any changes, you must click *Submit* (at the bottom of the page) in order for the changes to take effect at the next scheduled run.

10.4 Running a Policy On Demand

You can run a policy on demand by enabling the *Execute Now* option in the policy's *Frequency* settings. If the policy is not currently running, the policy run is triggered within a few minutes after you save (submit) the policy change. Otherwise, it begins a few minutes after the currently policy run ends.

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

2 In the list of *Dynamic Storage Technology Policies*, click the *Name* link for the policy to open the View/Edit Shadow Volume Policy page.

3 In the *Frequency* area, select *Execute Now*.

4 Scroll to the bottom of the page, then click *Submit*.

If the policy is not currently running, the policy runs within a few minutes after you click *Submit*.

If the policy is currently running, the on-demand run begins a few minutes after the currently running process completes or reaches the policy's scheduled *End Time*.

10.5 Viewing DST Policies and Policy Status

After you create DST policies, the Dynamic Storage Technology Policies table reports a list of policies, and information such as the shadow volumes to which the policy applies, when the policy was last executed, and the total number of files moved in the last run for that policy.

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

Initially, no policies are defined.

After one or more policies are defined, the policies are reported in a table.

2 View the following summary of information about all current policies on the server:

Parameter	Description
Name	The administrator-defined description of the policy. You specify the name in the *Description* field in the policy form.
Volumes	A list of shadow volumes to which the policy applies. These are specified in *Volume Selection* field of the policy form.
Last Executed	The time the policy was last enforced.
Total Files Moved	The number of files moved between the primary storage location and the secondary storage location the last time the policy ran.

3 Click the *Name* link for the policy to view or modify the individual settings for the policy.

4 On the View/Edit Shadow Volume Policy page, view or modify the policy settings.

For information about policy settings, see Section 10.1, "Understanding Shadow Volume Policy Options," on page 101.

5 If you make any changes, you must click *Submit* (at the bottom of the page) in order for the changes to take effect.

10.6 Viewing Information about the Files Moved During a Policy Run

If a file is moved during a policy run, the event is logged in the primary volume's log file. It is also tracked in the volume's audit log file (`/media/nss/<primary_volume_name>/.NETWARE/<primary_volume_name name>.audit.log`).

To view the primary volume's log file by using Novell Remote Manager:

1 In Novell Remote Manager, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

2 Under *Volume Information*, locate the shadow volume, then click the link to its log file.

3 In the log file, look for entries for the file moves.

For example, the following entry shows that the `/finance/rosebud_annual_report.pdf` file was successfully moved from the primary volume to the secondary volume:

```
<libncpengine name="volumeAuditOperations" timestamp="Wed Jun  8 18:00:21 2011
PM CEST" errno="0">
  <Move_status type="string">Successfully moved file</Move_status>
  <Direction type="string">primary to shadow</Direction>
  <File_path type="string">/finance/rosebud_annual_report.pdf</File_path>
</libncpengine>
```

10.7 Stopping a Running Policy

Beginning in OES 2 SP3 Linux, options are available to stop all currently running policies, or to stop an individual running policy. When a policy run begins, the policy is enforced on each of the shadow volumes that are specified in the policy's *Volume Selection* parameter. Therefore, the stop command applies to all shadow volumes that are associated with the policy. It is not possible to stop the policy for only one of multiple associated shadow volumes.

It takes some time (several seconds to a few minutes) for a policy to stop gracefully. For each of its associated shadow volumes, the policy run stops after it completes the move for the file that is currently being moved. The list of files to be moved for each associated shadow volume is discarded.

You cannot restart the policy from the point where you stopped a policy run. The next time that the policy is started, it scans its associated shadow volumes to create new lists of files to be moved.

Use the procedures in this section to stop one or all of the currently running shadow volume policies.

- Section 10.7.1, "Stopping All Running Shadow Volume Policies," on page 113
- Section 10.7.2, "Stopping a Running Individual Shadow Volume Policy," on page 113

10.7.1 Stopping All Running Shadow Volume Policies

The *Stop all running policies* option on the Dynamic Storage Technology Options page can be used to stop all currently running Shadow Volume storage policies. This option is available whether or not there are any currently running policies.

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

2 Click *Stop all running policies*.

3 Click *Yes* to confirm that you want to stop all currently running Shadow Volume storage policies.

 The status for each policy changes after its run is stopped gracefully for each of its associated shadow volumes.

10.7.2 Stopping a Running Individual Shadow Volume Policy
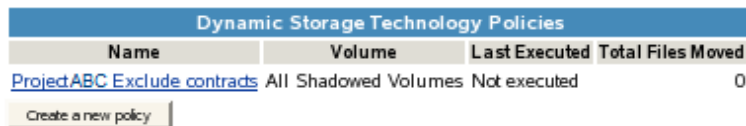
The *Stop* button on the View/Edit Shadow Volume Policy page can be used to stop a currently running individual Shadow Volume Policy rather than stopping all running policies. The *Stop* button is visible only while the policy is running.

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

2 In the list of *Dynamic Storage Technology Policies*, click the *Name* link for the policy in order to view the policy.

3 On the View/Edit Shadow Volume Policy page, scroll to the bottom of the page.

 If the policy is idle, the *Stop* button is not shown.

 If the policy is currently running, the *Stop* button is available.

4 Click *Stop*.

5 Click *Yes* to confirm that you want to stop the selected currently running Shadow Volume policy.

 The policy's status changes after the run is stopped gracefully for each of its associated shadow volumes.

10.8 Deleting a Shadow Volume Policy

You can delete a shadow volume policy at any time. If a policy is currently running, the policy is deleted after the process completes its run or reaches the previously set End Time.

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

2 In the list of *Dynamic Storage Technology Policies*, click the *Name* link for the policy in order to view the policy.

Dynamic Storage Technology Policies			
Name	Volume	Last Executed	Total Files Moved
ProjectABC Exclude contracts	All Shadowed Volumes	Not executed	0

Create a new policy

3 On the View/Edit Shadow Volume Policy page, scroll to the bottom of the page, click *Delete*, then click *Yes* to confirm the deletion.

If the policy is not currently running, it is deleted immediately.

If the policy is currently running, it is deleted after the process stops.

11 Generating a File Inventory for DST Shadow Volumes

In Novell Remote Manager for Linux, you can view reports for the DST shadow volume, with statistics and information about files in the primary file tree and secondary file tree.

11.1 Understanding the File Inventory for a Shadow Volume

The inventory provides key statistics about the files in the selected volume, such as files scanned and the available space trends. The inventory includes the following information:

11.1.1 Inventory Summary

The inventory summary lists the number of files scanned on the primary storage area and the secondary storage area. It also lists key statistics for the primary storage area, the secondary storage area, and both areas combined as the shadow volume.

Key Statistics	Description
Total Subdirectories	The total number of subdirectories in the volume.
Total Files	The total number of files in the volume.
Space in Use	The amount of space currently in use in the volume for data and metadata. On NSS volumes where salvage is enabled, the space in use includes space used by deleted files and directories.
Space Available	The amount of free space in the volume.

Key Statistics	Description
File Types	The number of different file types in use throughout the entire volume.
Soft Link Files	The NSS file system and NCP Server do not support soft links to files. This is a placeholder for future non-NCP support.
Soft Link Subdirectories	The NSS file system and NCP Server do not support soft links to subdirectories. This is a placeholder for future non-NCP support.

The following figure is an example of the summary:
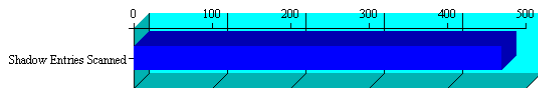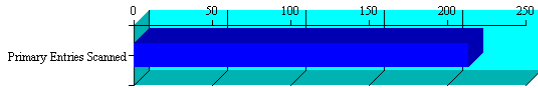
Primary Volume Tree: /media/nss/NSS1
Shadow Volume Tree: /media/nss/NSS2

Available space trend graph
File type profiles
File owner profiles
Last modified profiles
Last accessed profiles
Change time profiles
File size profiles
Links to specific reports
Custom Shadow Volume Options

Key Statistics	Totals	Primary Area	Shadow Area
Total Subdirectories:	70	35	35
Total Files:	614	179	435
Space In Use:	437 MB	41 MB	395 MB
Space Available:	-	20,377 MB	20,080 MB
File Types:	75	49	59
Soft Link Files:	0	0	0
Soft Link Subdirectories:	0	0	0

11.1.2 Available Space Trends

The *Available Space Trends* report shows the trends for space usage on the primary storage area and the secondary storage area. The following figure is an example of the *Available Space Trend* graphs:

Available space trend graph (Primary Area):
Start Time: Sat Feb 10 16:00:00 2007
End Time: Tue May 15 11:00:00 2007
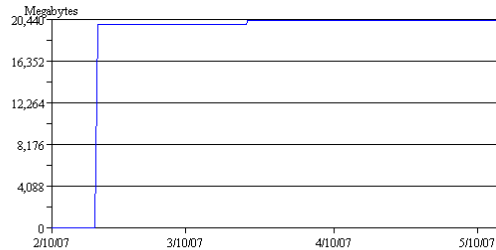
Available space trend graph (Shadow Area):
Start Time: Sat Mar 3 12:00:00 2007
End Time: Tue May 15 11:00:00 2007
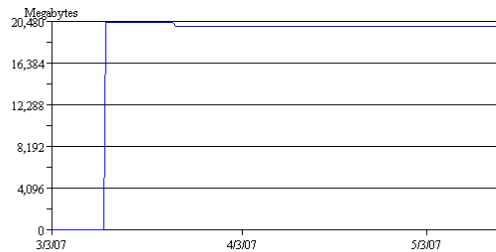
11.1.3 Graphical Profiles

The *Profiles* portion of the inventory report graphically displays information about the shadow volume. Graphical profiles are displayed by size in bytes and file count for the following categories:

- "File Type Profiles" on page 117
- "File Owner Profiles" on page 118
- "Time Stamp Profiles" on page 119
- "File Size Profiles" on page 120

File Type Profiles

File Type Profiles indicates storage space usage by file types that are actually in use on your system, such as LOG, TDF, DAT, XML, EXE, and so on.

The following figure is an example of the *File Type Profiles* graphs:

File Types (By Bytes In Use)
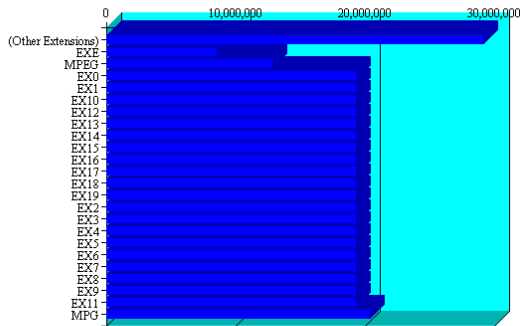
File Types (By File Count)
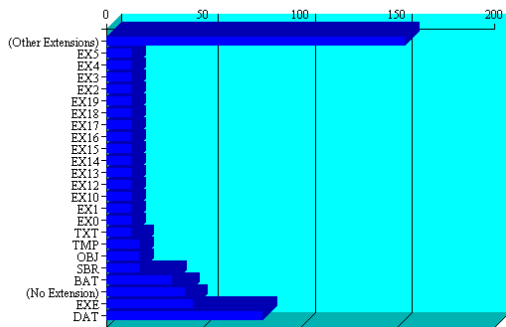
File Owner Profiles

File Owner Profiles indicates storage space usage by the designated owner of the file. It is not unusual in NCP to see the `root` user as the owner of files. For NCP volumes and NSS, file access is governed by the file system trustees assigned to the file, not the file owner. Trustees are users who have User objects defined in Novell eDirectory, and who have been granted file system rights for the file. NCP tracks ownership via the user's eDirectory GUID.

The following figure is an example of the *File Owner Profiles* graphs.

File Owners (By Bytes In Use)
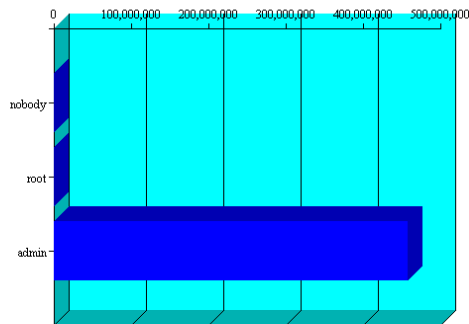
File Owners (By File Count)
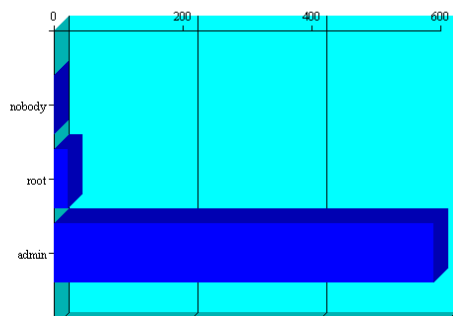
Time Stamp Profiles

Three time stamp profiles are generated:

- ◆ **Files Modified Profiles:** Modified dates indicate the last time someone changed the contents of a file.
- ◆ **Files Accessed Profiles:** Access dates indicate the last time someone accessed a file, but did not change the contents if this differs from the modified date.
- ◆ **Files Changed Profiles:** Change dates indicate the last time someone changed the metadata of a file, but did not change the contents if this differs from the modified date.

Time stamps are grouped by the following time periods:

More than 2 years
1 year to 2 years
6 months to 1 year
4 months to 6 months
2 months to 4 months
1 month to 2 months
2 weeks to 1 month
1 week to 2 weeks
1 day to 1 week
Within last day

The following figure is an example of the *File Modified Profiles* graphs. Similar graphs are created for *File Accessed Profiles* and *File Changed Profiles*.

Last Modified Times (By Bytes In Use)
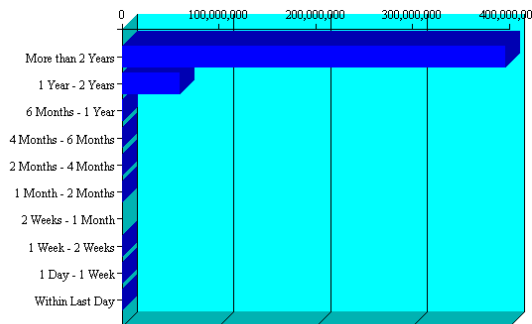
Last Modified Times (By File Count)
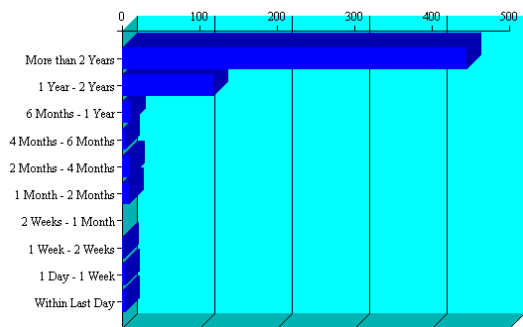
File Size Profiles

File Size Profiles reports the size of files, grouped by the following size ranges:

More than 256 MB
64 MB to 256 MB
16 MB to 64 MB
4 MB to 16 MB
1 MB to 4 MB
256 KB to 1 MB
64 KB to 256 KB
16 KB to 64 KB
4 KB to 16 KB
1 KB to 4 KB
Less than 1 KB

The following figure is an example of the *File Size Profiles* graphs:

File Size Chart (By Bytes In Use)
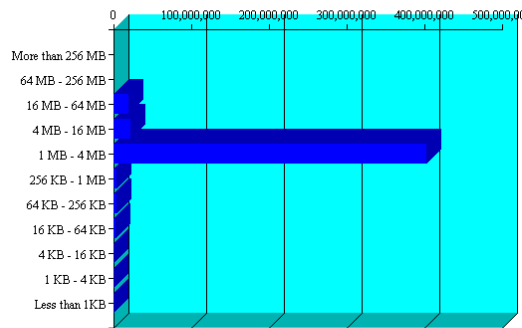
File Size Chart (By File Count)
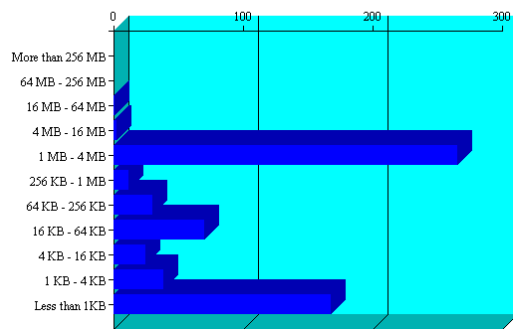
11.1.4 Tabular Profiles

Statistical data used to create the graphs is also available in tables that report statistics for the primary area, the secondary area, and both areas combined as the shadow volume. The count for file entries for the primary area and shadow (secondary) area are linked to detail reports that list the files matching that particular category and group. From the file lists, you have the option to copy, move, or delete one or multiple files.

For example, the following figure shows a few lines of a file-type information table:

File Extension	Total Space In Use	Total File Count	Primary Space	Primary Files	Shadow Space	Shadow Files
MPG	20,460,496	1	0	0	20,460,496	1
EX0	19,358,676	13	1,335,920	1	18,022,756	12
EX1	19,358,676	13	1,335,920	1	18,022,756	12

11.1.5 Inventory Detail Reports

An *Inventory Detail Report* lists all of the files that match a particular category and group for a file count entry in the tabular reports in the shadow volume inventory. You can select one or multiple files in the list, then select one of the following operations to be performed:

◆ Move the selected volumes to the other file tree.

- Move the selected files to a specified path on the server.
- Copy the selected files to a specified path on the server.
- Delete the selected files.

The action is performed on the selected files, and a confirmation list is displayed.

Volume Inventory

Moved: /media/nss/ARCVOL/hello~

Total files moved: 1

The following figure is an example of a detail report for file types that reside on the secondary volume:

Inventory Detail Report
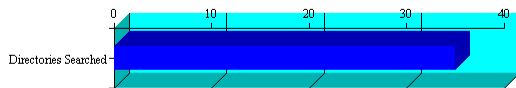
Inventory Detail Report for: /media/nss/NSS2
- Shadow Volume Tree
All files with extension: MPG

| Check All | Uncheck All | Delete Checked Files |

| Move Checked Files To Primary Volume Tree |

| Move Checked Files To: |

| Copy Checked Files To: |

☐ 🔍 /media/nss/NSS2/test/file-types/take_command.mpg
   OWNER: admin,
   Size: 20,460,496, Modified: 03-31-2006 10:55:08, Accessed: 05-15-2007 03:58:50, Changed: 03-23-2007 14:17:23,

Entries Found: 1

11.1.6 Custom Shadow Volume Options

The *Custom Shadow Volume Options* section of the volume inventory allows you to generate reports based on key statistics of interest, and perform actions on them.

Volume Operations

You can perform one of the following volume operations on the files that match the search criteria you specify:

- List primary area selected files
- Move selected files from primary area to shadow area.
- List shadow area selected files.
- Move selected files from shadow area to primary area.

Search Patterns

In *Search Patterns*, you can specify wildcards and characters to select files by file names or extensions.

File Owner Restrictions

In *File Owner Restrictions*, select *None* or a user name. The search applies only to files where the file owner matches the specified owner.

Time Stamp Restrictions

You can specify one or multiple time stamps to consider for the search:

- Last Modified Time
- Last Accessed Time
- Last Changed Time

If no time stamp is selected, time stamps are not considered in the search criteria.

If a time stamp is selected, you can specify one or multiple time ranges to consider for the search:

Within last day
1 day to 1 week
1 week to 2 weeks
2 weeks to 1 month
1 month to 2 months
2 months to 4 months
4 months to 6 months
6 months to 1 year
1 year to 2 years
More than 2 years

File Size Restrictions

You can specify one or multiple ranges of file sizes to consider for the search:

Less than 1 KB
1 KB to 4 KB
4 KB to 16 KB
16 KB to 64 KB
64 KB to 256 KB
256 KB to 1 MB
1 MB to 4 MB
4 MB to 16 MB
16 MB to 64 MB
64 MB to 256 MB
More than 256 MB

11.2 Accessing the Shadow Volume Inventory

1 Open Novell Remote Manager for Linux in a Web browser, then log in as the `root` user.

2 Use one of the following methods to view the volume inventory:

◆ Select *View File System > Dynamic Storage Technology Options*, locate the volume in the list, then click the *Inventory* link next to it.

Volume Information			
Volume Name	**Shadow Status**		
ⓘ VOL1	Shadowed	Inventory	View Log
ⓘ _ADMIN	No Shadow	Inventory	
ⓘ SYS	Add Shadow	Inventory	

◆ Select *View File System > Volume Inventory*, locate the volume in the *NCP Volumes Available for Inventory* list, then click the *Volume* link for the volume.

Volume Inventory ?

NCP Volumes available for Inventory	
Volume	**Mount Point**
SYS	(/usr/novell/sys)
_ADMIN	(/_admin)
VOL1	(/media/nss/VOL1)

11.3 Viewing Statistics for the Shadow Volume

1 In Novell Remote Manager, access the volume inventory for the shadow volume.

For information, see Section 11.2, "Accessing the Shadow Volume Inventory," on page 124.

2 In the inventory summary area, click a link to go directly to one of the following reports, or scroll to view the reports. For information about each statistical report, see Section 11.1, "Understanding the File Inventory for a Shadow Volume," on page 115.

◆ Available space trend graph

◆ File type profiles

◆ File owner profiles

◆ Last modified profiles

◆ Last accessed profiles

◆ Change time profiles

◆ File size profiles

◆ Links to specific reports

◆ Custom shadow volume options

3 Click the *Data Tables* link for a profile to jump directly to the tabular display of the information that was used to generate the graph.

11.4 Using Inventory Detail Reports to Move, Copy, or Delete Files on the Shadow Volume

1 In Novell Remote Manager, access the volume inventory for the shadow volume.

For information, see Section 11.2, "Accessing the Shadow Volume Inventory," on page 124.

2 In the summary area, click *Links to Specific Reports*, or scroll down to the *Links to Specific Reports* section to view the tabular reports of information used to generate the profiles.

3 Review the following categories to locate the files of interest:

- Last modified range
- Last accessed range
- Change time range
- File size range
- File owner
- File extension

4 Click the link of the data entry for the files that you want to manage. Files are grouped by Primary area and by shadow (secondary) area.

5 In the *Inventory Detail Report*, select one or multiple files in the list, then do one of the following:

- Move the selected volumes to the other file tree (primary or shadow (secondary) file tree).
- Move the selected files to a specified path on the server.
- Copy the selected files to a specified path on the server.
- Delete the selected files.

11.5 Generating a Custom Inventory Report

You can customize the inventory report to limit the search sizes and times reported. The reporting criteria can be combinations of the specific categories described in Section 11.1.6, "Custom Shadow Volume Options," on page 122.

1 In Novell Remote Manager, access the volume inventory for the shadow volume.

For information, see Section 11.2, "Accessing the Shadow Volume Inventory," on page 124.

2 Scroll down to the *Custom Shadow Volume Options* area at the end of the shadow volume inventory.

Custom Shadow Volume Options

Volume Operations:

- ⦿ List primary area selected files.
- ○ Move selected files from primary area to shadow area.
- ○ List shadow area selected files.
- ○ Move selected files from shadow area to primary area.

Search Pattern: `*.*`

File Owner Restriction: None ▾

Time Stamp Restrictions:

    Time Stamp:
- ☐ Last Modified Time
- ☐ Last Accessed Time
- ☐ Last Changed Time

    Range:
- ☐ Within Last Day
- ☐ 1 Day - 1 Week
- ☐ 1 Week - 2 Weeks
- ☐ 2 Weeks - 1 Month
- ☐ 1 Month - 2 Months
- ☐ 2 Months - 4 Months
- ☐ 4 Months - 6 Months
- ☐ 6 Months - 1 Year
- ☐ 1 Year - 2 Years
- ☐ More than 2 Years

File Size Restriction:
- ☐ Less than 1KB
- ☐ 1 KB - 4 KB
- ☐ 4 KB - 16 KB
- ☐ 16 KB - 64 KB
- ☐ 64 KB - 256 KB
- ☐ 256 KB - 1 MB
- ☐ 1 MB - 4 MB
- ☐ 4 MB - 16 MB
- ☐ 16 MB - 64 MB
- ☐ 64 MB - 256 MB
- ☐ More than 256 MB

[Start Scan]

3 In *Volume Operations*, select one of the following actions to perform on the files that meet the search criteria you specify for the scan in later steps.

- ◆ List primary area selected files
- ◆ Move selected files from primary area to shadow area.
- ◆ List shadow area selected files.
- ◆ Move selected files from shadow area to primary area.

4 In *Search Patterns*, specify wildcards and characters to select files by file name or extension. The default is *.*, which does not restrict the search to specific file names or extensions; all files are considered.

5 (Optional) In *File Owner Restrictions*, select *None*, or select a user name from the drop-down list.

If *None* is selected, file ownership is not considered for the search. If a user name is specified, the search applies only to files where the file owner matches the specified owner.

6 (Optional) In *Time Stamp*, specify one or multiple time stamps to be searched. If none are selected, the time stamps are not considered when searching.

- ◆ Last Modified Time
- ◆ Last Accessed Time
- ◆ Last Changed Time

7 In *Range*, if you specified a time stamp restriction, specify one or multiple ranges to be searched.

Within last day
1 day to 1 week
1 week to 2 weeks
2 weeks to 1 month
1 month to 2 months
2 months to 4 months
4 months to 6 months
6 months to 1 year
1 year to 2 years
More than 2 years

8 (Optional) In *File Size Restrictions*, specify one or multiple file sizes to be searched.

Less than 1 KB
1 KB to 4 KB
4 KB to 16 KB
16 KB to 64 KB
64 KB to 256 KB
256 KB to 1 MB
1 MB to 4 MB
4 MB to 16 MB
16 MB to 64 MB
64 MB to 256 MB
More than 256 MB

9 After you specify the volume operation and search criteria, click *Start Scan*.

10 If you chose to list the files, an Inventory Detail Report is generated where you can move, copy, or delete files.

  10a Select one or multiple files in the list, then select one of the following actions:

  - ◆ *Move the selected volumes to the other file tree.*
  - ◆ *Move the selected files to a specified path on the server.*
  - ◆ *Copy the selected files to a specified path on the server.*
  - ◆ *Delete the selected files.*

  10b Click *OK* to confirm the action.

  The action is performed on the selected files, then a confirmation list of the files and the number of files moved is displayed.

Volume Inventory   ?

Moved: /media/nss/ARCVOL/hello~

Total files moved: 1

If you chose to move selected files from one volume to another, the files that meet the search criteria are automatically moved, then a confirmation list of the files and the number of entries moved is displayed.

Volume Inventory

Custom file move from Primary tree to Shadow tree
All files matching selected filter:

Moved: /media/nss/VOL1/dir1/hello
Moved: /media/nss/VOL1/dir2/hello
Moved: /media/nss/VOL1/hello
Moved: /media/nss/VOL1/hello~
Entries Moved: 4

11 If you view the inventory chart again after the move, you can see that the files that matched the specified criteria before the move are now reported on the other volume.

12 Using ShadowFS to Provide a Merged View for Novell Samba Users

The Shadow File System (ShadowFS) provides a merged file tree view of the data on a Novell Dynamic Storage Technology (DST) shadow volume for Novell Samba users. This section describes how ShadowFS works and how to configure it with Novell Samba.

IMPORTANT: Novell CIFS works directly with NCP Server to provide a merged view for CIFS users. It is not necessary to install or set up ShadowFS.

12.1 Understanding ShadowFS

Shadow File System (ShadowFS) provides a merged file tree view of the DST volume for Novell Samba users. It allows users to access data on both locations via a share on the primary storage area by using the SMB/CIFS protocol instead of the NetWare Core Protocol (NCP). It is necessary to load ShadowFS only if Novell Samba is implemented on the server and SMB/CIFS users are given a merged view access to shadow volumes.

IMPORTANT: Performance for the Novell Samba clients to access the data via ShadowFS is slower than for NCP clients and Novell CIFS clients. For information, see Table 5-1, "Performance for File Access Protocols Used with DST Volumes," on page 44.

The ShadowFS technology is implemented on the FUSE (File Systems in Userspace) virtual file system. FUSE is an open source software package that is delivered in OES 2 Linux (or later), and is installed automatically when you install Dynamic Storage Technology.

When ShadowFS loads, it checks the /etc/NCPVolumes file to see what NCP shadow volumes exist, then it automatically creates a local mount point in /media/shadowfs/*volumename* that presents a merged file tree that includes both volumes. A mount point is created for every DST volume on the server. The local mount point allows Novell Samba and other local Linux applications to see the same merged view that NCP clients see when they access a shadow volume.

Each instance of ShadowFS runs as a separate process. Only a single instance of ShadowFS should be running.

The ShadowFS configuration file is /etc/opt/novell/shadowfs.conf.

The ShadowFS log file is /var/opt/novell/log/shadowfs.log.

12.2 Prerequisites for Using ShadowFS

❐ Before using ShadowFS, ensure that the following services have been installed and configured:

- ◆ NCP Server and Dynamic Storage Technology
- ◆ Novell eDirectory
- ◆ Novell Samba
- ◆ Linux User Management
- ◆ FUSE
- ◆ Novell Remote Manager for Linux
- ◆ Novell iManager for Linux

For information about these services, see Section 3.1, "Installation Requirements for Dynamic Storage Technology," on page 31.

❐ There must be at least one functional shadow volume on the server that is mounted in NCP. For information, see Section 9.2, "Creating a DST Shadow Volume with NSS Volumes," on page 80.

12.3 Preparing Your System for Using ShadowFS

Configure Novell Samba to prepare your system for using ShadowFS. For detailed instructions for installing, configuring, or setting up Novell Samba, see the *OES2 SP3: Samba Administration Guide*.

1 Verify that Novell Samba services are installed and functioning properly:

- ◆ Samba server is running.
- ◆ Shares can be created.
- ◆ Users can access Samba shares.

Use the Novell Samba plug-in for iManager to configure and verify Samba services. In iManager, go to the *File Protocols > Samba > General* page with the server selected.

2 Novell Samba users must be Linux-enabled through Linux User Management in order to access data.

IMPORTANT: You must Linux-enable users before adding a Samba Password policy assignment for the Samba server. If you attempt to add a user to a group, and the user is not already Linux-enabled, you cannot continue.

The users must be members of a primary group that is Linux-enabled on the target server or workstation object where both the Primary Group ID and Primary Group Name are assigned to the user. This is the primary group that is later assigned rights to the Samba share. Only primary groups can be assigned as the Directory group for the Samba share.

Adding users to Samba automatically Linux-enables them with Linux User Management (LUM), and it also Samba enables them. You can also Linux-enable users by using Linux User Management.

To verify Linux-enabled users, go to the *Modify User > Linux Profile > General* page with the server selected. Ensure that the values match the users' Group Assignment.

3 Make sure users have a Samba Password policy assignment at the eDirectory user, group or container level.

4 Make sure users have a Universal Password.

Users must have a Universal Password set in order for Samba to work properly.

5 Linux-enable the group with Linux User Management.

You must assign a Unix Workstation object for the group. To verify, use iManager to go to the *Modify Group > Linux Profile > General* page, confirm that the *Enable Linux Profile* option is enabled, and confirm that a *Unix Workstation* object is assigned and has a Group ID.

NOTE: For the purposes of testing, you can PAM-enable services on the server, so that test users can SSH into the server and validate access to directory paths to shares. For information about configuring SSH for a user, see *SSH Services on OES 2* in the *OES 2 SP3: Planning and Implementation Guide*.

12.4   Installing ShadowFS and FUSE

ShadowFS and FUSE are installed automatically when you install Dynamic Storage Technology. The following instructions are provided if you need to install it manually.

1 Open YaST as the `root` user.

2 In YaST, select *Software Management.*

3 In *Software Management*, search for *shadow* to find the `novell-shadowFS` package.

4 Select *novell-shadowFS*, click *Install*, click *Accept* to install it, then when prompted, accept its dependencies (such as FUSE).

5 Load FUSE by entering the following at a terminal console as the `root` user:

```
cd /opt/novell/ncpserv/sbin
modprobe fuse
```

There is no command line feedback to indicate if the command is successful.

6 Start ShadowFS by entering the following at a terminal console as the `root` user:

```
/opt/novell/ncpserv/sbin ./shadowfs
```

IMPORTANT: Make sure you run only a single instance of `shadowfs` at a time. Do not enter the command multiple times.

For example, if the primary storage location is an NSS volume named VOL1 and the secondary storage location is an NSS volume named ARCVOL, the output would look similar to this:

```
               SHIFT_ON_MODIFY: 1
               SHIFT_ON_ACCESS: 0
SHIFT_DAYS_SINCE_LAST_ACCESS: 1
               Primary Tree 0: /media/nss/VOL1
                Shadow Tree 0: /media/nss/ARCVOL
               shadowfs root 0: /media/shadowfs/VOL1
```

Loading ShadowFS creates the ShadowFS root volume /media/shadowfs/VOL1 where it creates the ShadowFS volumes. If multiple NCP volumes have shadow volumes, each of them is shadowed with ShadowFS and is reported. You cannot control whether to shadow only one or some of them.

12.5 Setting Rights to ShadowFS Shares

Grant POSIX rights for users so they can access files on the ShadowFS volume via the SMB/CIFS protocol. Rights are granted based on need. You set rights so that users can read, write, and execute in the ShadowFS volume's root location in the /media/shadowfs directory. Do not set POSIX rights to the actual NCP shares for the primary and secondary volumes.

1 Open a terminal console, then log in as the root user.

2 Go to the ShadowFS volume root location of /media/shadowfs by entering the following at the terminal prompt:

```
cd /media/shadowfs
```

3 Set directory ownership for the group-level access to the ShadowFS volume root by entering the following:

```
chown :groupname shadowfs_volumename
```

For example, if the *groupname* is marketing and the *shadowfs_volumename* is USERS, enter

```
chown :marketing USERS
```

4 Set POSIX rights for the directory group by entering the following:

```
chmod mode shadowfs_volumename
```

For example, to grant POSIX read, write, and execute permissions for the user and group levels, and to set read and execute only for the others (world) level, set the *mode* to 775 by entering:

```
chmod 775 USERS
```

You are setting directory rights for /media/shadowfs/USERS as drwxrwxr-x.

5 Visually verify POSIX rights by entering

```
ll
```

Continuing the example, the results should look like this:

```
drwxrwxr-x  3 root marketing  80 May 16 15:48 USERS
```

6 Verify that the SMB/CIFS user can access the ShadowFS volume and can create directories.

6a Decide which user identity you want to use to test the setup. For example, you could assign the admin user as a user of the SMB/CIFS group, or use iManager to create a temporary user identity for a test user in the group.

6b Use iManager to ensure that the test user is Linux-enabled with Linux User Management, and grant the user SSH rights for accessing the server.

For information about configuring SSH for a user, see "SSH Services on OES 2" in the *OES 2 SP3: Planning and Implementation Guide*.

6c Use iManager to set eDirectory permissions on the volume or path for the test user.

6d Use Secure Shell (SSH) to log in to the volume as a user in the group.

For example, use `ssh` to connect to the server and log in:

```
ssh username@server.context.com
```

```
password:********
```

6e Go to the ShadowFS volume location by entering

```
cd /media/shadowfs/USERS
```

The user should be able to `cd` to and see the directory. If not, recheck the preceding steps to ensure that you followed the steps correctly.

6f As the user, create a directory. For example, enter

```
mkdir username
```

If the directory `/media/shadowfs/USERS/username` is created, the rights are working as expected.

12.6 Creating a Samba Share

Create a Samba share that points to the newly created ShadowFS root, so that users can access it. Rights do not need to be set at the Primary and Shadow volumes themselves, unless they are not visible or accessible to the user or group assignment.

1 Log in to iManager as the administrator user.

2 In iManager, click *File Protocols > Samba > Shares*.

3 Select a server to manage.

4 On the *Shares* page, click *New*.

5 Specify the following information:

- **Share name:** Specify a share name that does not conflict with existing shares that are defined in the `smb.conf` file. To continue earlier examples in this section, USERS has been used, so the Samba share name must differ. For example, `usertest`.
- **Path:** Specify the context-sensitive path of the ShadowFS root location for the USERS volume, such as `/media/shadowfs/USERS`.
- **Comment:** Specify a description of the share, such as "User file storage for Windows users."
- **Inherit ACLs:** Enable this option to allow POSIX inheritance of access control lists and rights.

6 Click *Finish* to create the Samba share.

If the share is created successfully, it is listed on the *Shares* page.

12.7 Adding a User to Samba

If Linux-enabled users who need access are not already added to Samba, add them to the Samba server.

1 Log in to iManager as the administrator user.

2 In iManager, click *File Protocols > Samba > Shares*.

3 Select a server to manage, then click the *Users* tab.

4 On the *Shares > Users* page, click *Add*, then locate and select the users you want to add to Samba.

If a user is added successfully, the user name is listed on the *Users* page. The user should be listed with the default Samba user group *hostname*-W-SambaUserGroup and with the primary Linux-enabled user group to which the user was added earlier.

Users are automatically added to *hostname*-W-SambaUserGroup when they are added as Samba users via the Samba Management plug-in for iManager. If a user is already a member of another Linux-enabled group, adding the user to Samba adds the Samba group as the user's primary group.

If the user's previous primary group gave the user specific access to PAM-enabled services, the user likely loses those access rights, because the default Samba group gives users no rights to any PAM-enabled services. If this occurs, you can remove the user from the default Samba user group and reassign the user back to his or her previous primary group. This is done by modifying the user's properties.

5 If you need to modify a user's properties, go to *User > Modify > Linux Profile*, and change the *Primary Group Name* back to the previous group name. This also changes the *Primary Group ID*.

6 If you encounter problems with Samba, you can start, stop, or restart the Samba server from the *File Protocols > Samba > Shares > General* page.

12.8 Connecting Users to the Share

At this point, the Samba share users should be able to attach to server from a Windows client or other CIFS/SMB client. The procedure in this section explains the steps for a Windows XP client. Use a similar method on other Windows operating systems.

1 On a Windows XP computer, open *My Network Places*.

2 Select *Add Network Place*, then click *Next*.

3 Select *Choose another network location*, then click *Next*.

4 Type the location as \\servername*Samba_sharename*(such as \\svr1\usertest), then click *Next*.

Connecting to the server can take a few seconds to minutes, depending on network speed, discovery of server and share, and so on.

5 When prompted, enter your user name (DN only, not FDN) and password.

6 Specify the name of this network place, or use the default place name, then click *Next*.

7 Enable *Open this network place when I click Finish*, then click *Finish*.

If the connection is good, an Explorer window opens for the mapped location.

8 Make sure the rights are working by creating a new folder (right-click, then select *New > Folder*.

If the user can create a folder, rights are working.

12.9 Testing Shadow Volume Policies

If you are not familiar with policies on shadow volumes, you should test them against a test data set to understand how to use them to your advantage.

Add files of several different types to the new share, then either create a DST policy to move the files, or do an inventory to search for specific file types, then move them to the shadow.

SSH in as the user, or root, and look at the primary, shadow, and Shadowfs root paths to see if things are where you expect them to be.

12.10 Enabling or Disabling ShadowFS

By default, ShadowFS and FUSE are not started unless you start them manually. You can set a global policy for *ShadowFS Configuration* that starts them automatically.

IMPORTANT: If you use shadow volumes in a cluster, ensure that you set the same global policies on each OES 2 Linux node in the cluster.

- Section 12.10.1, "Loading ShadowFS and FUSE," on page 135
- Section 12.10.2, "Verifying ShadowFS Commands in the init.d Script," on page 135

12.10.1 Loading ShadowFS and FUSE

1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options*.

2 In the *ShadowFS Configuration* area, view the current setting for *Load ShadowFS*.

ShadowFS Configuration

☐ Load ShadowFS (enable only if using Samba)
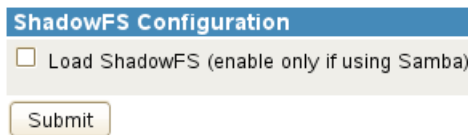
[Submit]

This command executes the `init.d` script, which puts the necessary commands in the boot sequence.

3 Enable or disable *Load ShadowFS* by selecting or deselecting the check box.

4 In the *ShadowFS Configuration* area, click *Submit* to save and apply the change.

12.10.2 Verifying ShadowFS Commands in the init.d Script

In *ShadowFS Configuration* on the Dynamic Storage Technology page, you can enable the *Load ShadowFS* check box to execute the init.d script. This puts the commands `shadowfs` and `fuse` startup commands in the boot sequence.

You can verify that the commands are available by viewing the script in a text editor. The following lines should be in the `init.d` script:

```
modprobe fuse
/opt/novell/ncpserv/sbin/shadowfs
```

12.11 Starting and Stopping ShadowFS Manually

FUSE (`fuse`) and ShadowFS (`shadowfs`) are required when Novell Samba users are accessing NSS volumes via SMB/CIFS. If FUSE or ShadowFS stop running, you must start them manually. Only one instance of `shadowfs` should be running at a time.

12.11.1 Starting FUSE and ShadowFS

Loading ShadowFS creates a ShadowFS root `/media/shadowfs/<volumename>` directory for each of the mounted DST shadow volumes. The *volumename* is the same as volume name of the primary volume. The ShadowFS root directory contains the merged file tree view of the primary and secondary locations in the DST volume. A root is created for all of the mounted DST volumes; you cannot control whether to shadow only one or some of them.

1 On the server, open a terminal console, then log in as the `root` user.

2 At the terminal console prompt, start FUSE by entering

```
cd /opt/novell/ncpserv/sbin
modprobe fuse
```

There is no command line feedback to indicate if the command is successful.

3 At the terminal console prompt, start ShadowFS by entering

```
/opt/novell/ncpserv/sbin ./shadowfs
```

The output identifies the primary volume, secondary volume, and the `shadowfs` volume.

For example, if the primary storage location is an NSS volume named `VOL1` and the secondary storage location is an NSS volume named `ARCVOL`, the output would look similar to this:

```
              SHIFT_ON_MODIFY: 1
              SHIFT_ON_ACCESS: 0
SHIFT_DAYS_SINCE_LAST_ACCESS: 1
               Primary Tree 0: /media/nss/VOL1
                Shadow Tree 0: /media/nss/ARCVOL
              shadowfs root 0: /media/shadowfs/VOL1
```

12.11.2 Starting FUSE and ShadowFS with novell-shadowfs

1 On the server, open a terminal console, then log in as the `root` user.

2 At the terminal console prompt, start FUSE and ShadowFS by entering

```
/etc/init.d/novell-shadowfs start
```

12.11.3 Stopping Shadowfs

1 On the server, open a terminal console, then log in as the `root` user.

2 At the terminal console prompt, stop the shadowfs process by entering

```
/etc/init.d/novell-shadowfs stop
```

If the process does not stop, you need to kill the process. Enter

```
killall shadowfs
```

12.12 Configuring Trustee Rights for Novell Samba Users

When you use ShadowFS to provide a merged view to the Novell Samba users, file access is controlled by the Novell trustee model for user access. You must use NCP rights management tools to set trustees, just as you do for NCP clients. For example, you can use the Files and Folders plug-in to iManager 2.7*x*, the Novell Client, or the `ncpcon rights` command to set trustees, trustee rights, and inherited rights filters for files and folders.

13 Configuring DST Shadow Volume Pairs with Novell Cluster Services

Dynamic Storage Technology shadow volume pairs can be configured as cluster resources with Novell Cluster Services. This section describes two methods for configuring the cluster resource, how to manage the shadow volume in a cluster, and how to remove a shadow relationship from a cluster resource.

13.1 Planning for DST in a Cluster

In addition to the requirements described in Section 3.1, "Installation Requirements for Dynamic Storage Technology," on page 31, use the requirements in this section to configure DST on nodes in a Novell Cluster Services cluster.

13.1.1   Novell Open Enterprise Server 2 SP3

Ensure that each node in the cluster is running the same release version of OES 2 SP3 with the latest patches applied.

13.1.2   Novell Cluster Services

Ensure that each node is running the same release version of Novell Cluster Services with the latest patches applied.

When you use clustered DST volumes, special steps are needed when you upgrade the cluster from OES 2 SP3 to OES 11 or later. For information, see "Upgrading a Cluster with DST Resources from OES 2 SP3 to OES 11x" in the *OES 11 SP1: Dynamic Storage Technology Administration Guide*.

13.1.3   NCP Server and Dynamic Storage Technology

The NCP (NetWare Core Protocol) Server and the Dynamic Storage Technology software are not cluster aware. They must be installed on every node in the cluster where you plan to migrate or fail over the cluster resource that contains shadow volumes. You do not cluster NCP Server or DST services. You can cluster the DST shadow volume pair by creating a DST pool cluster resource that manages the primary and secondary disks, pools, and volumes.

13.1.4   Novell Storage Services File System

Dynamic Storage Technology supports shadow volumes created with pairs of shared Novell Storage Services (NSS) volumes. Install NSS on each node in the cluster. For information, see the *OES 2 SP3: NSS File System Administration Guide for Linux*.

You must create the two NSS pools and volumes on separate shared disks before you create the shadow volume relationship for the two volumes. The primary pool must be cluster-enabled. The secondary pool must be shared. You can cluster-enable the secondary pool, but its Cluster objects and IP address are not used while the two NSS volumes are in the shadow relationship.

13.1.5   Novell Remote Manager for Linux

You do not use Dynamic Storage Technology Options page in Novell Remote Manager to create a clustered DST shadow volume pair. The `ncpcon mount` command in the load script creates the DST shadow volume pair on the node where the resource is brought online.

When you use Novell Remote Manager for Linux to manage policies for the shadow volume, you typically connect to the IP address of the DST pair cluster resource. You can also connect to the IP address of the server node where the cluster resource is currently mounted.

13.1.6   Merged View Access with NCP

NCP Server allows NCP users to access a merged view of the clustered DST volume pair when the cluster resource is online. As with any clustered volume, the files are not available when the cluster resource is offline.

13.1.7 Merged View Access with Novell CIFS

Novell CIFS supports Dynamic Storage Technology merged view of DST volume pairs comprised of two NSS volumes. CIFS users can access a merged view of the clustered DST volume pair when the cluster resource is online. As with any clustered volume, the files are not available when the cluster resource is offline. Novell CIFS does not require users to be Linux enabled with Linux User Management (LUM).

You must install and configure Novell CIFS on every node in the cluster where you plan to give users CIFS access to the shared cluster resource. For information, see *OES 2 SP3: Novell CIFS for Linux Administration Guide*.

You want Novell CIFS to be available on the node where the DST shadow volumes is active. To do this, you add Novell CIFS as an advertising protocol for the primary NSS pool resource as you cluster-enable it.

In the primary NSS pool cluster resource load script, the following command binds Novell CIFS to provide access to the shared resource through the virtual server IP address when the resource is mounted on a node.

```
exit_on_error novcifs --add --vserver=virtualserverFDN --ip-addr=virtualserverip
```

In the primary NSS pool cluster resource unload script, the following command unbinds Novell CIFS from the DST pool cluster resource when the resource is failed over or cluster migrated to another node in the cluster.

```
ignore_error novcifs --remove --vserver=virtualserverFDN --ip-addr=virtualserverip
```

In the primary NSS pool cluster resource monitor script, the CIFS `monitor` command helps to keep CIFS up and running.

```
exit_on_error rcnovell-cifs monitor
```

In addition, the following CIFS attributes are automatically added to the NCS:NCP Server object for the virtual server on the primary pool cluster resource:

- ◆ nfapCIFSServerName (read access)
- ◆ nfapCIFSAttach (read access)
- ◆ nfapCIFSComment (read access)
- ◆ nfapCIFSShares (write access)

For information, see "Configuring CIFS with Novell Cluster Services for an NSS File System" in the *OES 2 SP3: Novell CIFS for Linux Administration Guide*.

13.1.8 Merged View Access with Novell Samba and ShadowFS

ShadowFS and FUSE (File System in Userspace) can be used with Novell Samba to allow SMB/CIFS users to access a merged view of the clustered DST volume pair. Novell Samba is an alternative to Novell CIFS; they cannot be used together on the same server. Novell Samba requires users to be Linux enabled with LUM.

You must install and configure Novell Samba and ShadowFS for each node in the cluster. For information about setting up SMB/CIFS access on each node, see Chapter 12, "Using ShadowFS to Provide a Merged View for Novell Samba Users," on page 129.

Additional commands for managing FUSE for the resource must be added manually in the cluster load/unload scripts of the primary pool cluster resource You must also add the following lines in the load script of the primary NSS pool cluster resource to allow time for ShadowFS to start:

```
# If shadowfs is used, wait for shadowfs to start
for (( c=1; c<=10; c++ )) do
if [ ! -d /media/shadowfs/VOLUME/._NETWARE ]; then sleep 5; fi
done
```

You must add the following line to the unload script of the primary NSS pool cluster resource to unload the volume in FUSE:

```
#unload the volume in FUSE
ignore_error fusermount -u /media/shadowfs/VOLUME
```

13.1.9   No Merged View Access for AFP

Novell AFP does not support a merged view of files on the DST volume pair. AFP users see only the files on the primary volume. Do not give AFP users direct access to the secondary volume.

13.2   Planning for DST Shadow Volume Pairs and Policies in a Cluster

In addition to the requirements in Chapter 5, "Planning for DST Shadow Volumes and Policies," on page 41, your setup must meet the requirements in this section when you use DST in a Novell Cluster Services cluster.

- Section 13.2.1, "DST Pool Cluster Resource," on page 142
- Section 13.2.2, "Shadow Volume Definition in the /etc/NCPVolumes File," on page 143
- Section 13.2.3, "Shadow Volume Definition in the ncpserv.conf File," on page 143
- Section 13.2.4, "NCP2NSS Bindings for the Secondary Volume," on page 143
- Section 13.2.5, "NCPCON Mount Command for the Load Script," on page 144
- Section 13.2.6, "Load Order in the Load Script," on page 144
- Section 13.2.7, "Unload Order in the Unload Script," on page 144
- Section 13.2.8, "Monitoring Storage in the Monitor Script," on page 145
- Section 13.2.9, "Additional Volumes in the Primary Pool," on page 145
- Section 13.2.10, "Policies for DST Nodes and Volumes in a Cluster," on page 145

13.2.1   DST Pool Cluster Resource

The primary and secondary volumes must be able to fail over or cluster migrate together to other nodes in the cluster. Thus, a single DST pool cluster resource is used to manage the pair. Its resource scripts include commands that manage the two devices, pools, volumes.

The devices and pools that contain the primary volume and secondary volume in a clustered DST volume pair must be marked as shareable for clustering. The primary pool must be cluster-enabled for Novell Cluster Services. The secondary pool must be shared. You can cluster-enable the pool that contains the secondary volume, but its individual pool resource IP address and Cluster objects are not used in the load and unload scripts for the DST pool cluster resource.

13.2.2 Shadow Volume Definition in the /etc/NCPVolumes File

In a cluster, the DST volume pair is defined in the `ncpcon mount` command of the load script for the DST pool cluster resource. When the resource is brought online, the volume is mounted, and an entry is added to the `/etc/NCPVolumes` file. When the resource is taken offline, the volumes are dismounted when the pools are deactivated, and the entry is removed.

```
<VOLUME>
  <NAME>VOL1</NAME>
  <PRIMARY_ROOT>/media/nss/VOL1</PRIMARY_ROOT>
  <SHADOW_ROOT>/media/nss/ARCVOL1</SHADOW_ROOT>
</VOLUME>
```

13.2.3 Shadow Volume Definition in the ncpserv.conf File

In a cluster, the DST volume pair is defined with the `ncpcon mount` command in the load script for the DST pool cluster resource. You do not create a clustered DST volume by using the Dynamic Storage Technology Options page in Novell Remote Manager. When you bring the resource online on a node for the first time, a SHADOW_VOLUME line is automatically added to the `/etc/opt/novell/ncpserv.conf` file:

```
SHADOW_VOLUME primary_volumename secondary_volume_path
```

For example:

```
SHADOW_VOLUME VOL1 /media/nss/ARCVOL1
```

When the resource fails over or is cluster migrated to another node, the shadow volume definition remains defined on that server.

If you remove the shadow relationship from the cluster load script, the SHADOW_VOLUME entry is usually not needed in the `/etc/opt/novell/ncpserv.conf` file. To permanently unlink the two volumes, you must manually remove the line from the `/etc/opt/novell/ncpserv.conf` file and restart ndsd on each node. To disable clustering but keep the DST shadow volume pair on a specified node, you must manually remove the line from the configuration file and restart ndsd on all nodes except that one.

13.2.4 NCP2NSS Bindings for the Secondary Volume

The `EXCLUDE_VOLUME` line in the `/etc/opt/novell/ncp2nss.conf` file prevents the secondary NSS volume from being mounted in NCP. The allows the secondary volume to be mounted for NSS and Linux, but not in NCP. The users access the files on the secondary volume via the merged view of the DST volume pair, not directly.

In a cluster, the DST volume pair is defined with the `ncpcon mount` command in the load script for the DST pool cluster resource. When you bring the resource online on a node for the first time, an EXCLUDE_VOLUME line is automatically added to the `/etc/opt/novell/ncp2nss.conf` file as well as the temporary exclusion table in cache on that node.

```
EXCLUDE_VOLUME secondary_volumename
```

For example:

```
EXCLUDE_VOLUME ARCVOL1
```

If you remove the shadow relationship from the cluster load script, the `EXCLUDE_VOLUME` entry is usually not needed in the `/etc/opt/novell/ncp2nss.conf` file. To permanently unlink the two volumes, you must manually remove the line from the `/etc/opt/novell/ncp2nss.conf` file and

restart `ncp2nss` on each node. To disable clustering but keep the DST shadow volume pair on a specified node, you must manually remove the line from the configuration file and restart ncp2nss on all nodes except that one.

13.2.5 NCPCON Mount Command for the Load Script

The DST shadow volume pair is defined by the following `ncpcon mount` command in the DST pool cluster resource's load script. The volume pair is available only when the resource online.

```
exit_on_error ncpcon mount primary_volumename=volID,SHADOWVOLUME=secondary_volumename
```

Both NSS volumes must already exist. The mount location is /media/nss/`<primary_volume_name>`.

Replace *volID* with a volume ID that is unique across all servers in the cluster. Valid values are 0 to 254. By convention, the IDs are assigned from 254 and downward for clustered volumes.

When the primary volume has a state of *Shadowed*, the volume ID that you assign as its NCP volume ID represents the DST shadow volume pair of volumes. The secondary volume does not have a separate volume ID while it is in the shadow relationship.

For example, the following command mounts the primary NSS volume named `VOL1` with a volume ID of 254. The primary volume is mounted for NSS and NCP at /media/nss/VOL1. The secondary volume is an existing NSS volume named `ARCVOL1`. It is mounted for NSS at /media/nss/ARCVOL1.

```
exit_on_error ncpcon mount VOL1=254,SHADOWVOLUME=ARCVOL1
```

13.2.6 Load Order in the Load Script

The secondary pool must be mounted before the primary pool. This helps to ensure that the pool is activated and available when the DST volume pair is mounted.

IMPORTANT: If the secondary volume is not available when the shadow volume pair is mounted, the cluster load script does not fail and does not provide a warning. The DST shadow volume is created and appears to be working when viewed from Novell Remote Manager. However, until the DST shadow volume is mounted, the files on the secondary volume are not available to users and appear to be missing in the merged file tree view. After the secondary volume has successfully mounted, the files automatically appear in the merged file tree view.

If you observe that the pools are slow to mount, you can add a wait time to the load script before the mount command for the shadow volume pair.

For example, you add a `sleep` command with a delay of a few seconds, such as:

```
sleep 10
```

You can increase the sleep time value until it allows sufficient time for the pools to be activated and the volumes to be mounted in NSS before continuing.

IMPORTANT: If wait times are added to the load script or unload script, ensure that you increase the script timeout settings accordingly. Otherwise, the script might time out while you are waiting for the action.

13.2.7 Unload Order in the Unload Script

The primary pool must be deactivated before the secondary pool. This allows the DST volume pair to be dismounted before the secondary pool is deactivated.

13.2.8 Monitoring Storage in the Monitor Script

The monitor script for the DST pool cluster resource has monitoring commands for the primary pool, secondary pool, the primary volume, and advertising protocols for the primary volume.

You should not monitor the secondary volume in the monitor script. The EXCLUDE_VOLUME line in the /etc/opt/novell/ncp2nss.conf file makes it unavailable to NCP. Thus, the ncpcon volume command that is used to check its status is not able to see the secondary volume.

Ensure that you remove or comment out the following line from the resource monitoring script:

```
exit_on_error ncpcon volume primary_volume_name
#exit_on_error ncpcon volume secondary_volume_name
```

13.2.9 Additional Volumes in the Primary Pool

If you add a volume to the primary pool for a clustered DST volume pair, the mount command is added twice in the primary pool's cluster load script, once after the primary pool's activation command and once after the secondary pool's activation command. You must manually delete the instance that occurs after the secondary pool's activation, then offline and online the primary pool cluster resource to apply the modified load script.

For information, see "Adding a Volume to a Clustered Pool" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

13.2.10 Policies for DST Nodes and Volumes in a Cluster

In a cluster, the DST policies must be available on every node where a clustered DST pool cluster resource is brought online. As a best practice, you should create policies at the volume level for each clustered DST volume pair so that the volume's policies fail over with it when its DST pool cluster resource fails over or is cluster migrated to a different node.

- "Global Policies" on page 145
- "All-Shadow-Volumes Policies" on page 146
- "Volume Policies" on page 146

Global Policies

Global policies are NCP Settings for DST that you set at the server level. They govern how DST behaves for all DST volume pairs mounted on the server. Global policies are not cluster aware.

Ensure that the same global DST policies are configured on each node where you want to fail over the DST pool cluster resources. To manage a global DST policy, open Novell Remote Manager for Linux by using the IP address of the node. For information, see Chapter 8, "Configuring DST Global Policies," on page 65.

IMPORTANT: Whenever you modify global policies on a given node in the cluster, you must make those same changes on the other nodes.

All-Shadow-Volumes Policies

An all-shadow-volumes policy applies to any DST volume that is mounted on that server when the policy runs. All-shadow-volumes policies are not cluster aware.

If you select *All Shadowed Volumes* when you create a policy, the policy information is stored in the `/usr/novell/sys/._NETWARE/shadow_policy.xml` file. Ensure that the same all-shadow-volumes policies are configured on each node where you want to fail over the DST pool cluster resources. You can create the same all-shadow-volumes policies on each node in the cluster, or you can create it on one node and copy the `shadow_policy.xml` file to all nodes where you plan to bring the DST pool cluster resource online. To manage an all-shadow-volumes policy, open Novell Remote Manager for Linux by using the IP address of the node.

IMPORTANT: Whenever you modify all-shadow-volumes policies on a given node in the cluster, you must make those same changes on the other nodes.

Volume Policies

Volume policies apply only to specified DST volume pair. Volume policies are not cluster aware. They are stored with the volume and are available automatically on any node where the DST pool cluster resource is brought online. When you set up volume policies, the DST pool cluster resource must be online and the DST volume pair must be mounted.

If a policy applies to a specific volume, the policy information is stored in the `/media/nss/<primary_volumename>/._NETWARE/shadow_policy.xml` file. This file is stored on the volume itself and thereby automatically follows the volume as its DST pool cluster resource is failed over or cluster migrated to a different node. To manage a volume policy, open Novell Remote Manager for Linux by using the IP address of the resource or by using the IP address of the node where the resource is currently active.

13.3 Using the Clusters Plug-in for iManager 2.7.5 or Later

The Clusters plug-in for iManager 2.7.5 or later has been reorganized. For information, see "Clusters Plug-In Changes for Novell iManager 2.7.5" in the *OES 11 SP1: Novell Cluster Services 2.1 for Linux Administration Guide*.

13.4 Preparing the Nodes to Support DST in a Cluster Environment

For each OES 2 SP3 server, perform the following tasks to prepare them for hosting DST pool cluster resources in a cluster:

1. Install NCP Server and Dynamic Storage Technology. For information, see Chapter 3, "Installing Dynamic Storage Technology," on page 31.

2. Install and configure Novell Cluster Services for Linux. For information, see "Installing and Configuring Novell Cluster Services on OES 2 Linux" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

3. For each node, configure the same DST global policies by using Novell Remote Manager. For information, see Chapter 8, "Configuring DST Global Policies," on page 65.

13.5 Configuring the DST Pool Cluster Resource with Two Cluster-Enabled Pools

One way to set up the DST pool cluster resource is to cluster-enable both pools to create separate cluster resources. You copy the commands from the secondary pool resource scripts to the primary pool resource scripts in the proper load and unload order. The primary pool cluster resource manages the two pools and volumes.

The advantages of creating two cluster pool resources are:

 * You can copy and paste the lines of code you need from one script to the other.
 * The NCP Server object's name for the secondary volume is automatically renamed to use the cluster name instead of the node hostname. In a migration scenario, you can later remove the shadow relationship and start using the secondary pool immediately as an independent pool cluster resource. Ensure that the volume ID on the volume is unique across all nodes.

The disadvantages of this approach are:

 * The static IP address that is assigned to the secondary cluster pool resource is consumed but not used while the pool is in the shadow relationship.
 * The secondary cluster pool resource appears with a status of *Offline* and is not used.

IMPORTANT: After you modify the primary pool cluster resource, you use this resource to manage the secondary pool and volume. Do not bring the secondary resource online.

Use the information in the following sections to set up the DST pool cluster resource.

13.5.1 Overview of the Two Pool Cluster Resources

For this method, you need two NSS volumes, each in its own clustered-enabled pool. For instructions for creating the clustered pools and the NSS volumes, see *Configuring Cluster Resources for Shared NSS Pools and Volumes* in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

The cluster load scripts elsewhere in this section assume the following setup for NSS volumes in the clustered DST volume pair. Ensure that you use the actual information from your setup.

Parameter	Primary Cluster Resource	Secondary Cluster Resource
Server hostname for node 1	`server38`	`server38`
Cluster server name for node 1	`NCS1`	`NCS1`
Pool name	`POOL1`	`ARCPOOL1`
NSS volume name	`VOL1`	`ARCVOL1`
Cluster resource virtual server name	`NCS1-POOL1-SERVER`	NCS1-ARCPOOL1-SERVER (not used after you set up the primary resource for DST)

Parameter	Primary Cluster Resource	Secondary Cluster Resource
Cluster resource IP address	10.10.10.38	10.10.10.48
	You use the IP address for the primary pool's cluster resource for the shadow volume.	(not used after you set up the primary resource for DST)
Volume ID	254	253
		(not used after you set up the primary resource for DST)

When the primary volume has a state of *Shadowed*, its NCP volume ID represents the DST shadow volume pair of volumes. A second NCP volume ID is not assigned to the secondary volume while it is in the shadow volume relationship. You use only the ID on the primary volume in the `ncpcon mount` command in the cluster resource load script.

IMPORTANT: In the cluster load and unload scripts, the `add_secondary_ipaddress` and `del_secondary_ipaddress` commands refer to the cluster resource's IP address that is "secondary" to the node's IP address. It is not related to the DST volume's terminology.

13.5.2 Viewing the Scripts for the Two Pool Cluster Resources

After you create two clustered pools, view the scripts. Each of the two NSS pool cluster resources has its own set of load, unload, and monitor scripts. Save the script information for the secondary pool to a text file.

1 In iManager, select *Clusters*, then select *My Clusters*.

2 Select the name link of the cluster you want to manage.

If the cluster is not in your customized list, you can add it now. Click *Add*, browse to select the cluster, then click *OK*.

3 On the Cluster Manager page, click the *Name* link of the primary cluster resource to go to the Cluster Pool Properties page, then click the *Scripts* tab view the load, unload, and monitor scripts.

You can view the scripts for only one server at a time in the browser. View the properties of each resource in separate browsers to compare the scripts side-by-side.

The following table provides sample load, unload, and monitor scripts for the POOL1-SERVER resource for the primary clustered pool named POOL1. Novell CIFS can be configured as an advertising protocol when you set up the primary cluster pool.

Primary Pool Cluster Resource Scripts

Load Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

exit_on_error nss /poolact=POOL1

exit_on_error ncpcon mount VOL1=254

exit_on_error add_secondary_ipaddress 10.10.10.38
exit_on_error ncpcon bind --ncpservername=NCS1-POOL1-SERVER --ipaddress=10.10.10.38

#This line is added if Novell CIFS is used as an advertising protocol
#novcifs --add '--vserver=".cn=NCS1-POOL1-SERVER.ou=ncs.o=novell.t=AVALON_TREE."'
        --ip-addr=10.10.10.38

exit 0
```

Unload Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

#This line is added if Novell CIFS is used as an advertising protocol
#novcifs --remove --vserver=virtualserverFDN --ip-addr=virtualserverip

ignore_error ncpcon unbind --ncpservername=NCS1-POOL1-SERVER --ipaddress=10.10.10.38
ignore_error del_secondary_ipaddress 10.10.10.38

ignore_error nss /pooldeact=POOL1

exit 0
```

Primary Pool Cluster Resource Scripts

Monitor Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

exit_on_error status_fs /dev/pool/POOL1 /opt/novell/nss/mnt/.pools/POOL1 nsspool

exit_on_error status_secondary_ipaddress 10.10.10.38

exit_on_error ncpcon volume VOL1

exit_on_error rcnovell-cifs monitor

exit 0
```

The following are sample load and unload scripts for the ARCPOOL1-SERVER resource for the secondary clustered pool named ARCPOOL1.

Secondary Pool Cluster Resource Scripts

Load Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

exit_on_error nss /poolact=ARCPOOL1

exit_on_error ncpcon mount ARCVOL1=253

exit_on_error add_secondary_ipaddress 10.10.10.48

exit_on_error ncpcon bind --ncpservername=NCS1-ARCPOOL1-SERVER --ipaddress=10.10.10.48

exit 0
```

Unload Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

ignore_error ncpcon unbind --ncpservername=NCS1-ARCPOOL1-SERVER --ipaddress=10.10.10.48
ignore_error del_secondary_ipaddress 10.10.10.48

ignore_error nss /pooldeact=ARCPOOL1

exit 0
```

Sample Primary Monitor Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

exit_on_error status_fs /dev/pool/ARCPOOL1 /opt/novell/nss/mnt/.pools/ARCPOOL1 nsspool

exit_on_error status_secondary_ipaddress 10.10.10.48

exit_on_error ncpcon volume ARCVOL1

exit 0
```

4 Copy information from the secondary resource's scripts into a text file, and save the file.

You will work from this copy to add lines to the primary pool cluster resource.

5 At the bottom of the Scripts page, click *Cancel* to return to the Cluster Manager page.

6 Continue with Section 13.5.3, "Adding Commands for the Secondary Clustered Pool and Volume to the Primary Pool Cluster Resource," on page 151.

13.5.3 Adding Commands for the Secondary Clustered Pool and Volume to the Primary Pool Cluster Resource

The clustered DST shadow volume is defined and managed in the primary pool cluster resource. You must add lines from the secondary pool cluster resource scripts and modify the mount command to define the DST shadow volume.

1 In iManager, select *Clusters*, then select *My Clusters*.

2 Select the name link of the cluster you want to manage.

3 Offline the primary cluster resource. The secondary cluster resource should still be offline.

   3a On the Cluster Manager page, select the check box next to the resource.

   3b Click *Offline*.

4 Click the name link of the primary pool cluster resource to view its Cluster Pool Properties page, then click the *Scripts* tab.

Clusters > Cluster Manager

Cluster Pool Properties: POOL1_SERVER [?]

| Policies | Monitoring | Preferred Nodes | Scripts | Protocols | Business Continuity |

Load Script | Unload Script | Monitor Script

View or edit the load script for this cluster resource.

Script:

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs
exit_on_error nss /poolact=POOL1
exit_on_error ncpcon mount VOL1=254
exit_on_error add_secondary_ipaddress 10.10.10.38
exit_on_error ncpcon bind --ncpservername=NCS1-POOL1-SERVER
--ipaddress= 10.10.10.38
exit 0
```

Timeout: 1   Minutes ▼

OK   Cancel   Apply

5 On the *Scripts > Load Script* page, modify the load script for the primary cluster resource.

Use the following sample load script as a guide for where to add the lines for each of the items.

Sample DST Pool Resource Load Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# activate the secondary pool
exit_on_error nss /poolact=ARCPOOL1

# activate the primary pool
exit_on_error nss /poolact=POOL1

# Optional delay to allow time for pools to activate before mounting the volume
sleep 10

#comment out the original volume mount command
#exit_on_error ncpcon mount VOL1=254

# Use the ncpcon mount command to create the shadow volume on mount
exit_on_error ncpcon mount VOL1=254,shadowvolume=ARCVOL1

exit_on_error add_secondary_ipaddress 10.10.10.38

exit_on_error ncpcon bind --ncpservername=NCS1-POOL1-SERVER --ipaddress=10.10.10.38

#This line is added if Novell CIFS is used as an advertising protocol
#novcifs --add '--vserver=".cn=NCS1-POOL1-SERVER.ou=ncs.o=novell.t=AVALON_TREE."'
        --ip-addr=10.10.10.38

# If shadowfs is used, wait for shadowfs to start
#for (( c=1; c<=10; c++ )) do
# if [ ! -d /media/shadowfs/VOLUME/._NETWARE ]; then sleep 5; fi
#done

exit 0
```

5a Add a line to activate the secondary pool before the primary pool activation.

```
exit_on_error nss /poolact=ARCPOOL1
```

5b (Optional) Add a `sleep` command after the pool activation commands to allow both pools time to be activated before you mount the shadow volume pair.

For example:

```
sleep 10
```

Vary the time (in seconds) according to what is needed for your system.

IMPORTANT: If wait times are added to the load script or unload script, ensure that you increase the script timeout settings accordingly. Otherwise, the script might time out while you are waiting for the action.

5c Comment out (or remove) the individual mount command for the primary NSS volume by placing a pound sign (#) at the beginning of the line.

For example:

```
#exit_on_error ncpcon mount VOL1=254
```

5d Add the shadow volume mount command to the primary load script. This line provides the primary volume, and assigns the secondary volume to shadow the primary.

```
exit_on_error ncpcon mount VOL1=254,shadowvolume=ARCVOL1
```

5e If you are using `shadowfs` to provide the merged file tree view for SMB/CIFS users or for Linux services like `rsync`, you must allow time in the load script after mounting the shadow volume to allow `shadowfs` to become active before continuing.

Use one of the following approaches to add a wait time:

- Add a `sleep 10` command after mount command, and vary it manually until it allows sufficient wait time for shadowfs to start.

  ```
  # If shadowfs is used, wait for shadowfs to start
  sleep 10
  ```

- Add a script that varies the wait time by checking to ensure that `shadowfs` is started.

  For example:

  ```
  # If shadowfs is used, wait for shadowfs to start
  for (( c=1; c<=10; c++ )) do
   if [ ! -d /media/shadowfs/VOLUME/._NETWARE ]; then sleep 5; fi
  done
  ```

IMPORTANT: If wait times are added to the load script or unload script, ensure that you increase the script timeout settings accordingly. Otherwise, the script might time out while you are waiting for the action.

5f Click *Apply* to save your changes.

The changes do not take effect until the shadow volume cluster resource is brought online.

6 On the *Scripts > Unload Script* page, modify the unload script for the primary cluster resource.

Use the following sample unload script as a guide for where to add the lines for each of the items.

Sample DST Pool Resource Unload Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# This line is added if Novell CIFS is used as an advertising protocol
#novcifs --remove '--vserver=".cn=NCS1-POOL1-SERVER.ou=ncs.o=novell.t=AVALON_TREE."' --
ip-addr=10.10.10.38

# If shadowfs is used, unload the volume in FUSE
#ignore_error fusermount -u /media/shadowfs/VOL1

ignore_error ncpcon unbind --ncpservername=NCS1-POOL1-SERVER --ipaddress=10.10.10.38

ignore_error del_secondary_ipaddress 10.10.10.38

# Deactivate the primary pool
ignore_error nss /pooldeact=POOL1

# Deactivate the secondary pool
ignore_error nss /pooldeact=ARCPOOL1

exit 0
```

6a If you use `shadowfs` to provide a merged file tree view to Samba users or for Linux file protocols, you must unmount the FUSE-mounted file systems that are displayed in the `/media/shadowfs/VOLUME` directory. Add the following line just before the unbind command in the unload script:

```
#unload the volume in FUSE
# Include the following line only if shadowfs is used
ignore_error fusermount -u /media/shadowfs/VOLUME
```

6b Copy the pool deactivation command from the secondary pool's unload script into the primary pool's unload script after the line to deactive the primary pool.

```
ignore_error nss /pooldeact=ARCPOOL1
```

IMPORTANT: Ensure that you deactivate the primary pool before deactivating the secondary pool.

6c Click *Apply* to save your changes.

The changes do not take effect until the shadow volume cluster resource is brought online.

7 On the *Scripts > Monitor Script* page, modify the monitor script for the primary cluster resource.

Use the following sample monitor script as a guide for where to add the lines for each of the items.

Sample DST Pool Resource Monitor Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# Check the status of the secondary pool
exit_on_error status_fs /dev/pool/ARCPOOL1 /opt/novell/nss/mnt/.pools/ARCPOOL1 nsspool

# Check the status of the primary pool
exit_on_error status_fs /dev/pool/POOL1 /opt/novell/nss/mnt/.pools/POOL1 nsspool

exit_on_error status_secondary_ipaddress 10.10.10.38

# Check the status of the primary volume. Do not check secondary volume.
exit_on_error ncpcon volume VOL1

# This line is added if Novell CIFS is used as an advertising protocol
#exit_on_error rcnovell-cifs monitor

exit 0
```

7a Copy the pool status check command from the secondary pool's monitor script into the primary pool's monitor script before the line to check the status of the primary pool.

7b Do not add a check for the secondary volume.

7c Click *Apply* to save your changes.

The changes do not take effect until the shadow volume cluster resource is brought online.

8 Click *OK* to save all your changes and return to the Cluster Manager page.

9 Online the primary pool cluster resource. On the Cluster Manager page, select the check box next to the primary cluster resource, then click *Online*.

Leave the secondary resource offline.

10 Verify that the primary cluster resource is running by going to the *Cluster Manager* page.

The primary cluster resource is *Running*. The secondary cluster resource is reported as *Offline* because you are managing that cluster resource through the primary load script.

11 Verify that the shadow volume (`VOL1`) is mounted in NCP and is shadowed:

11a On the first node in the cluster, log in to Novell Remote Manager for Linux as the `root` user.

11b Select *View File Systems*, then verify that the secondary pool `ARCPOOL1` and the NSS volume `ARCVOL1` are listed under *File Systems*, but the secondary NSS volume is not listed under *NCP Volumes*.

11c Select *View File Systems > Dynamic Storage Technology Options*, then verify that the primary volume is listed under *Volume Information*, and that its status is *Shadowed*.

11d Select *Manage NCP Services > Manage Shares*, click *NCP/NSS Bindings*, then verify that the *NCP Accessible* parameter is turned off for the secondary volume, and turned on for the primary volume.

NCP / NSS Bindings ?

Warning:
When a NSS Volume is changed to be not accessible via NCP, it will be dismounted immediately as a NCP share point

Available NSS volumes		
NCP Accessible	**Volume Name**	**Mount point**
Yes: ○ No: ⊙ Save Selection	ARCVOL1	/media/nss/ARCVOL1
Yes: ⊙ No: ○ Save Selection	VOL1	/media/nss/VOL1

Share Management Home

You can also look for the EXCLUDE_VOLUME entry in the /etc/opt/novell/ncp2nss.conf file.

11e Continue with Section 13.8, "Configuring Shadow Volume Policies for the Clustered DST Volume Pair," on page 168.

13.6 Configuring the DST Pool Cluster Resource with a Cluster-Enabled Pool and a Shared Pool

An alternate way to set up the DST pool cluster resource is to cluster-enable the primary pool, then create a shared pool that is not cluster-enabled as the secondary location. You manually modify the primary cluster pool resource scripts with the commands needed to load and unload the secondary pool and volume. The primary pool cluster resource manages the two pools and volumes. The NCP Server object's name for the secondary volume keeps the hostname of the node where it was created.

The advantage of creating one clustered pool and one shared-but-not-cluster-enabled pool are:

◆ A static IP address is not consumed for the secondary pool.

◆ The secondary pool and volume are shared but not clustered. This can be useful in a migration scenario to move data to a secondary volume and move the volume to a different node. After you remove the shadow relationship, you mark the secondary pool's device as *Not Shareable for Clustering* to unshare the pool and volume, then use the Update eDirectory option in NSSMU to create storage objects with the new hostname. There are no Cluster objects to clean up.

There disadvantages of this approach are:

◆ You must manually enter the lines of code in the primary pool cluster resource's load, unload, and monitor scripts for the secondary pool.

◆ The option to create a pool on a shared device without cluster-enabling it is available only in NSSMU. You cannot use the Storage plug-in in iManager.

◆ To later use the secondary pool as an independent cluster resource requires a some extra steps. Use the Update eDirectory option in NSSMU to create storage objects with the new hostname, then cluster-enable the pool by using the Clusters plug-in in iManager.

IMPORTANT: After you modify the primary pool cluster resource, you use the resource to manage the secondary pool and volume.

Use the information in the following sections to set up the DST pool cluster resource.

13.6.1 Overview of the Pool Cluster Resource and Shared Pool

For this method, you need two NSS volumes: one in a clustered-enabled pool and one in a pool that is shared, but not cluster-enabled. For instructions for creating the cluster-enabled pool and the primary NSS volume, see *Configuring Cluster Resources for Shared NSS Pools and Volumes* in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

To create the secondary shared pool, see Section 13.6.3, "Creating a Shared Pool and Volume that Are Not Cluster-Enabled," on page 159.

The cluster load scripts elsewhere in this section assume the following setup for NSS volumes in the clustered DST volume pair. Ensure that you use the actual information from your setup.

Parameter	Primary Cluster Resource	Secondary Shared Pool
Server hostname for node 1	`server38`	`server38`
Cluster server name for node 1	`NCS1`	`NCS1`
Pool name	`POOL1`	`ARCPOOL1`
NSS volume name	`VOL1`	`ARCVOL1`
Cluster resource virtual server name	`NCS1-POOL1-SERVER`	None
Cluster resource IP address	10.10.10.38 You use the IP address for the primary pool's cluster resource for the shadow volume.	None
Volume ID	254	Automatically assigned when you create the volume locally

When the primary volume has a state of *Shadowed*, its NCP volume ID represents the DST shadow volume pair of volumes. A separate NCP volume ID is not assigned to the secondary volume while the volume is in the shadow volume relationship. You use only the ID on the primary volume in the `ncpcon mount` command in the cluster resource load script.

IMPORTANT: In the cluster load and unload scripts, the `add_secondary_ipaddress` and `del_secondary_ipaddress` commands refer to the cluster resource's IP address that is "secondary" to the node's actual IP address. It is not related to the DST volume's terminology.

13.6.2 Viewing the Scripts for Pool Cluster Resource

After you create a clustered pool, view the scripts.

1 In iManager, select *Clusters*, then select *My Clusters*.

2 Select the name link of the cluster you want to manage.

If the cluster is not in your customized list, you can add it now. Click *Add*, browse to select the cluster, then click *OK*.

3 On the Cluster Manager page, click the *Name* link of the primary cluster resource to go to the Cluster Pool Properties page, then click the *Scripts* tab view the load, unload, and monitor scripts.

Clusters > Cluster Manager

Cluster Pool Properties: POOL1_SERVER   [?]

| Policies | Monitoring | Preferred Nodes | **Scripts** | Protocols | Business Continuity |

Load Script | Unload Script | Monitor Script

View or edit the load script for this cluster resource.

Script:

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs
exit_on_error nss /poolact=POOL1
exit_on_error ncpcon mount VOL1=254
exit_on_error add_secondary_ipaddress 10.10.10.38
exit_on_error ncpcon bind --ncpservername=NCS1-POOL1-SERVER
--ipaddress= 10.10.10.38
exit 0
```

Timeout: [1]   [Minutes ▾]

[OK]   [Cancel]   [Apply]

The following table provides sample load, unload, and monitor scripts for the POOL1-SERVER resource for the primary clustered pool named POOL1. Novell CIFS can be configured as an advertising protocol when you set up the primary cluster pool.

Primary Pool Cluster Resource Scripts

Load Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

exit_on_error nss /poolact=POOL1

exit_on_error ncpcon mount VOL1=254

exit_on_error add_secondary_ipaddress 10.10.10.38
exit_on_error ncpcon bind --ncpservername=NCS1-POOL1-SERVER --ipaddress=10.10.10.38

#This line is added if Novell CIFS is used as an advertising protocol
#novcifs --add '--vserver=".cn=NCS1-POOL1-SERVER.ou=ncs.o=novell.t=AVALON_TREE."'
        --ip-addr=10.10.10.38

exit 0
```

Primary Pool Cluster Resource Scripts

Unload Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

#This line is added if Novell CIFS is used as an advertising protocol
#novcifs --remove --vserver=virtualserverFDN --ip-addr=virtualserverip

ignore_error ncpcon unbind --ncpservername=NCS1-POOL1-SERVER --ipaddress=10.10.10.38
ignore_error del_secondary_ipaddress 10.10.10.38

ignore_error nss /pooldeact=POOL1

exit 0
```

Monitor Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

exit_on_error status_fs /dev/pool/POOL1 /opt/novell/nss/mnt/.pools/POOL1 nsspool

exit_on_error status_secondary_ipaddress 10.10.10.38

exit_on_error ncpcon volume VOL1

exit_on_error rcnovell-cifs monitor

exit 0
```

4 At the bottom of the Scripts page, click *Cancel* to return to the Cluster Manager page.

5 Continue with .

13.6.3 Creating a Shared Pool and Volume that Are Not Cluster-Enabled

1 On the server where the primary pool cluster resource is assigned, log in as the root user.

2 Open a terminal console, and enter nssmu to open the NSS Management Utility.

3 From the NSSMU main menu, select *Devices* to go to the Device Management page.

4 Ensure that the device you want to use as the secondary location is available but is not currently shared.

   Do not mark the device as shareable at this time. If devices are present but not showing up for creating pools and volumes, you should initialize the disk.

5 From the NSSMU main menu, select *Pools* to go to the Pools Management page.

6 Create a pool on the device.

   Because the device is not yet shared, the *Cluster Information* page is not part of the pool setup process.

7 From the NSSMU main menu, select *Volumes* to go to the Volumes Management page.

8 Create a volume on the pool.

9 Exit NSSMU.

10 In a Web browser, open Novell Remote Manager for the server, then log in as the root user.

11 In Novell Remote Manager, disable the NCP/NSS Bindings for the NSS volume you created in Step 8.

For instructions, see Section 9.4.1, "Disabling the NCP/NSS Bindings for an NSS Volume," on page 85.

The NSS volume is removed from the list of volumes mounted in NCP. However, if you exit Novell Remote Manager and check the volume in NSSMU, you can see that it is still mounted by NSS.

12 Exit Novell Remote Manager.

13 At a command prompt, launch NSSMU.

`nssmu`

14 In the NSSMU main menu, select *Devices*.

15 Select the device that contains the secondary NSS pool and volume, then press F6 to mark the device as *Shareable for Clustering*.

This automatically changes the share status of all pools on the device to *Shareable for Clustering*.

16 In NSSMU, select *Pools* from the main menu.

17 Verify that the share status of the pool is *Shareable for Clustering*.

18 Exit NSSMU.

19 Continue with Section 13.6.4, "Adding Commands for the Secondary Shared Pool and Volume to the Primary Pool Cluster Resource," on page 160.

13.6.4 Adding Commands for the Secondary Shared Pool and Volume to the Primary Pool Cluster Resource

Initially, you have a load, unload, and monitor script for the primary pool cluster resource. You modify these scripts to also manage the secondary shared pool and volume so that the NSS volumes in the DST shadow volume pair can fail over or be cluster migrated together.

1 In iManager, dismount the secondary volume and deactivate the shared pool.

   1a Select *Storage > Volumes.*

   1b Click the *Object* browser, then locate and select the server where the secondary pool is active.

   1c Select the secondary volume, then click *Dismount*.

   1d Select *Storage > Pools.*

   1e Select the secondary pool, then click *Deactivate*.

2 In iManager, select *Clusters*, then select *My Clusters*.

3 Select the name link of the cluster you want to manage.

4 Offline the primary cluster resource.

   4a On the Cluster Manager page, select the check box next to the resource.

   4b Click *Offline*.

5 Click the name link of the primary pool cluster resource to view its Cluster Pool Properties page, then click the *Scripts* tab.

Clusters > Cluster Manager

Cluster Pool Properties: POOL1_SERVER

Policies \ Monitoring \ Preferred Nodes \ Scripts \ Protocols \ Business Continuity

Load Script | Unload Script | Monitor Script

View or edit the load script for this cluster resource.

Script:

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs
exit_on_error nss /poolact=POOL1
exit_on_error ncpcon mount VOL1=254
exit_on_error add_secondary_ipaddress 10.10.10.38
exit_on_error ncpcon bind --ncpservername=NCS1-POOL1-SERVER
--ipaddress= 10.10.10.38
exit 0
```

Timeout: 1   Minutes

OK   Cancel   Apply

6 On the *Scripts > Load Script* page, modify the load script for the primary cluster resource.

Use the following sample load script as a guide for where to add the lines for each of the items.

Sample DST Pool Resource Load Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# activate the secondary pool
exit_on_error nss /poolact=ARCPOOL1

# activate the primary pool
exit_on_error nss /poolact=POOL1

# Optional delay to allow time for pools to activate before mounting the volume
sleep 10

#comment out the original volume mount command
#exit_on_error ncpcon mount VOL1=254

# Use the ncpcon mount command to create the shadow volume on mount
exit_on_error ncpcon mount VOL1=254,shadowvolume=ARCVOL1

exit_on_error add_secondary_ipaddress 10.10.10.38

exit_on_error ncpcon bind --ncpservername=NCS1-POOL1-SERVER --ipaddress=10.10.10.38

#This line is added if Novell CIFS is used as an advertising protocol
#novcifs --add '--vserver=".cn=NCS1-POOL1-SERVER.ou=ncs.o=novell.t=AVALON_TREE."'
        --ip-addr=10.10.10.38

# If shadowfs is used, wait for shadowfs to start
#for (( c=1; c<=10; c++ )) do
# if [ ! -d /media/shadowfs/VOLUME/._NETWARE ]; then sleep 5; fi
#done

exit 0
```

6a Add a line before the primary pool activation that will activate the secondary pool.

```
exit_on_error nss /poolact=ARCPOOL1
```

6b (Optional) Add a `sleep` command after the pool activation commands to allow both pools time to be activated before you mount the shadow volume pair.

For example:

```
sleep 10
```

Vary the time (in seconds) according to what is needed for your system.

IMPORTANT: If wait times are added to the load script or unload script, ensure that you increase the script timeout settings accordingly. Otherwise, the script might time out while you are waiting for the action.

6c Comment out (or remove) the individual mount command for the primary NSS volume by placing a pound sign (#) at the beginning of the line.

For example:

```
#exit_on_error ncpcon mount VOL1=254
```

6d Add the mount command for the shadow volume to the primary load script.

```
exit_on_error ncpcon mount VOL1=254,shadowvolume=ARCVOL1
```

6e (Optional) If you are using `shadowfs` to provide the merged file tree view for SMB/CIFS users or for Linux services like `rsync`, you must allow time in the load script after mounting the shadow volume to allow `shadowfs` to become active before continuing.

IMPORTANT: Do not perform this step if you are using Novell CIFS to provide access to CIFS users.

Use one of the following approaches to add a wait time:

- ◆ Add a `sleep 10` command after mount command, and vary it manually until it allows sufficient wait time for shadowfs to start.

  ```
  # If shadowfs is used, wait for shadowfs to start
  sleep 10
  ```

- ◆ Add a script that varies the wait time by checking to ensure that `shadowfs` is started.

  For example:

  ```
  # If shadowfs is used, wait for shadowfs to start
  for (( c=1; c<=10; c++ )) do
   if [ ! -d /media/shadowfs/VOLUME/._NETWARE ]; then sleep 5; fi
  done
  ```

IMPORTANT: If wait times are added to the load script or unload script, ensure that you increase the script timeout settings accordingly. Otherwise, the script might time out while you are waiting for the action.

6f Click *Apply* to save your changes.

The changes to the script do not take effect until the cluster resource is taken offline and brought online.

7 On the *Scripts > Unload Script* page, modify the unload script for the primary cluster resource.

Use the following sample unload script as a guide for where to add the lines for each of the items.

Sample DST Pool Resource Unload Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# This line is added if Novell CIFS is used as an advertising protocol
#novcifs --remove '--vserver=".cn=NCS1-POOL1-SERVER.ou=ncs.o=novell.t=AVALON_TREE."' --
ip-addr=10.10.10.38

# If shadowfs is used, unload the volume in FUSE
#ignore_error fusermount -u /media/shadowfs/VOL1

ignore_error ncpcon unbind --ncpservername=NCS1-POOL1-SERVER --ipaddress=10.10.10.38

ignore_error del_secondary_ipaddress 10.10.10.38

# Deactivate the primary pool
ignore_error nss /pooldeact=POOL1

# Deactivate the secondary pool
ignore_error nss /pooldeact=ARCPOOL1

exit 0
```

7a If you use `shadowfs` to provide a merged file tree view to Samba users or for Linux file protocols, you must unmount the FUSE-mounted file systems that are displayed in the /media/shadowfs/VOLUME directory.

Add the following line before the unbind command in the unload script:

```
#unload the volume in FUSE
ignore_error fusermount -u /media/shadowfs/VOLUME
```

7b Add the following command to dismount the secondary pool after the command to dismount the primary pool.

```
ignore_error nss /pooldeact=ARCPOOL1
```

7c Click *Apply* to save your changes.

The changes to the script do not take effect until the cluster resource is taken offline and brought online.

8 On the *Scripts > Monitor Script* page, modify the monitor script for the primary cluster resource.

Use the following sample monitor script as a guide for where to add the lines for each of the items.

Sample DST Pool Resource Monitor Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# Check the status of the secondary pool
exit_on_error status_fs /dev/pool/ARCPOOL1 /opt/novell/nss/mnt/.pools/ARCPOOL1 nsspool

# Check the status of the primary pool
exit_on_error status_fs /dev/pool/POOL1 /opt/novell/nss/mnt/.pools/POOL1 nsspool

exit_on_error status_secondary_ipaddress 10.10.10.38

# Check the status of the primary volume. Do not check secondary volume.
exit_on_error ncpcon volume VOL1

# This line is added if Novell CIFS is used as an advertising protocol
#exit_on_error rcnovell-cifs monitor

exit 0
```

8a Add a command to check the status of the secondary pool.

```
# Check the status of the secondary pool
exit_on_error status_fs /dev/pool/ARCPOOL1 /opt/novell/nss/mnt/.pools/ARCPOOL1 nsspool
```

8b Do not add a check for the secondary volume.

8c Click *Apply* to save your changes.

The changes do not take effect until the shadow volume cluster resource is brought online.

9 Click *OK* to save all your changes and return to the Cluster Manager page.

10 Online the primary pool cluster resource. On the Cluster Manager page, select the check box next to the primary cluster resource, then click *Online*.

11 Verify that the primary cluster resource is running by going to the *Cluster Manager* page.

The primary cluster resource is *Running*.

12 Verify that the shadow volume (`VOL1`) is mounted in NCP and is shadowed:

12a On the first node in the cluster, log in to Novell Remote Manager for Linux as the `root` user.

12b Select *View File Systems*, then verify that the secondary pool `ARCPOOL1` and the NSS volume `ARCVOL1` are listed under *File Systems*, but the secondary NSS volume is not listed under *NCP Volumes*.

12c Select *View File Systems > Dynamic Storage Technology Options*, then verify that the primary volume is listed under *Volume Information*, and that its status is *Shadowed*.

12d Select *Manage NCP Services > Manage Shares*, click NCP/NSS bindings, then verify that the NCP Accessible parameter is turned off for the secondary volume, and turned on for the primary volume.

NCP / NSS Bindings

Warning:
When a NSS Volume is changed to be not accessible via NCP, it will be dismounted immediately as a NCP share point

Available NSS volumes

NCP Accessible	Volume Name	Mount point
Yes: ○ No: ⊙ [Save Selection]	ARCVOL1	/media/nss/ARCVOL1
Yes: ⊙ No: ○ [Save Selection]	VOL1	/media/nss/VOL1

[Share Management Home]

You can also look for the `EXCLUDE_VOLUME` entry in the `/etc/opt/novell/ncp2nss.conf` file.

13 Continue with Section 13.8, "Configuring Shadow Volume Policies for the Clustered DST Volume Pair," on page 168.

13.7   Sample Scripts for a DST Pool Cluster Resource

The cluster scripts in this section assume the following setup for NSS volumes in the clustered DST volume pair. Ensure that you use the actual information from your setup.

Setup	Primary NSS Volume	Secondary NSS Volume
Server name for node 1	`server38`	`server38`
Cluster name for node 1	`NCS1`	`NCS1`
Cluster pool name	`POOL1`	`ARCPOOL1`
NSS volume name	`VOL1`	`ARCVOL1`
Cluster resource virtual server name	`NCS1-POOL1-SERVER`	
Cluster resource IP address	10.10.10.38	
Volume ID on the cluster node	254	

- Section 13.7.1, "Sample Load Script for a DST Shadow Volume," on page 167
- Section 13.7.2, "Sample Unload Script," on page 167
- Section 13.7.3, "Sample Monitor Script for a DST Volume," on page 168

13.7.1 Sample Load Script for a DST Shadow Volume

The following is a sample load script for a DST pool cluster resource.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# activate the secondary pool
exit_on_error nss /poolact=ARCPOOL1

# activate the primary pool
exit_on_error nss /poolact=POOL1

# Optional delay to allow time for pools to activate before mounting the volume
sleep 10

#comment out the original volume mount command
#exit_on_error ncpcon mount VOL1=254

# Use the ncpcon mount command to create the shadow volume on mount
exit_on_error ncpcon mount VOL1=254,shadowvolume=ARCVOL1

exit_on_error add_secondary_ipaddress 10.10.10.38

exit_on_error ncpcon bind --ncpservername=NCS1-POOL1-SERVER --ipaddress=10.10.10.38

#This line is added if Novell CIFS is used as an advertising protocol
#novcifs --add '--vserver=".cn=NCS1-POOL1-SERVER.ou=ncs.o=novell.t=AVALON_TREE."'
         --ip-addr=10.10.10.38

# If shadowfs is used, wait for shadowfs to start
#for (( c=1; c<=10; c++ )) do
# if [ ! -d /media/shadowfs/VOLUME/._NETWARE ]; then sleep 5; fi
#done

exit 0
```

13.7.2 Sample Unload Script

The following is a sample unload script for a DST pool cluster resource.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# This line is added if Novell CIFS is used as an advertising protocol
#novcifs --remove '--vserver=".cn=NCS1-POOL1-SERVER.ou=ncs.o=novell.t=AVALON_TREE."' --ip-
addr=10.10.10.38

# If shadowfs is used, unload the volume in FUSE
#ignore_error fusermount -u /media/shadowfs/VOL1

ignore_error ncpcon unbind --ncpservername=NCS1-POOL1-SERVER --ipaddress=10.10.10.38

ignore_error del_secondary_ipaddress 10.10.10.38

# Deactivate the primary pool
ignore_error nss /pooldeact=POOL1

# Deactivate the secondary pool
ignore_error nss /pooldeact=ARCPOOL1

exit 0
```

13.7.3 Sample Monitor Script for a DST Volume

The following is a sample unload script for a DST pool cluster resource.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

# Check the status of the secondary pool
exit_on_error status_fs /dev/pool/ARCPOOL1 /opt/novell/nss/mnt/.pools/ARCPOOL1 nsspool

# Check the status of the primary pool
exit_on_error status_fs /dev/pool/POOL1 /opt/novell/nss/mnt/.pools/POOL1 nsspool

exit_on_error status_secondary_ipaddress 10.10.10.38

# Check the status of the primary volume. Do not check secondary volume.
exit_on_error ncpcon volume VOL1

# This line is added if Novell CIFS is used as an advertising protocol
#exit_on_error rcnovell-cifs monitor

exit 0
```

13.8 Configuring Shadow Volume Policies for the Clustered DST Volume Pair

After you have modified the scripts for the primary pool cluster resource to make it a DST pool cluster resource, you are ready to bring the resource online and create policies for it. For planning information, see "Installing DST on Nodes in a Novell Cluster Services for Linux Cluster" on page 37.

1 Create shadow volume policies for the clustered DST volume pair as described in Chapter 10, "Creating and Managing Policies for Shadow Volumes," on page 101.

2 If a shadow volume policy uses the *All Shadow Volumes* option, you must copy the policy information from the /usr/novell/sys/._NETWARE/shadow_policy.xml file to the same file on each node.

Copy only the entries for policies that you intend to apply for all DST shadow volume pairs across all nodes.

13.9 Removing the Shadow Relationship for a Clustered DST Volume Pair

Removing a clustered DST volume pair removes the shadow relationship between the primary and secondary storage area. You remove commands in the primary pool's cluster scripts that you added to manage the secondary pool and volume. Removing the shadow relationship does not remove the underlying volumes themselves. The files remain on whichever storage area they are on at the time when you remove the shadow relationship.

- Section 13.9.1, "Planning to Remove the Shadow Relationship for a Clustered DST Volume Pair," on page 169
- Section 13.9.2, "Preparing to Remove a Shadow Relationship," on page 169
- Section 13.9.3, "Removing the Shadow Definition and NCP/NSS Bindings Exclusion on All Nodes," on page 170
- Section 13.9.4, "Preparing the Primary Pool Cluster Resource for Independent Use," on page 171
- Section 13.9.5, "Preparing the Secondary Pool and Volume for Independent Use," on page 172

13.9.1 Planning to Remove the Shadow Relationship for a Clustered DST Volume Pair

As you plan to remove the shadow relationship for a clustered DST volume pair, consider the following short service outages that are involved:

- The data on the DST volume pair will be unavailable to users while you remove the shadow relationship in Section 13.9.3, "Removing the Shadow Definition and NCP/NSS Bindings Exclusion on All Nodes," on page 170, and until you have performed the tasks necessary for the two volumes to function independently.

- An NDSD restart is required after you remove the shadow volume and NCP/NSS bindings information on each node in turn. This results in a brief service outage for all NSS volumes and NCP volumes that are mounted on the node at that time.

- The primary volume is available to users as an independent volume after you perform the procedure described in Section 13.9.4, "Preparing the Primary Pool Cluster Resource for Independent Use," on page 171.

- The secondary volume is available to users as an independent volume after you perform one of the procedures described in Section 13.9.5, "Preparing the Secondary Pool and Volume for Independent Use," on page 172.

13.9.2 Preparing to Remove a Shadow Relationship

Removing a shadow relationship does not automatically move files in either direction between the two volumes. The files remain undisturbed. The volumes function independently after the shadow relationship is successfully removed. Ensure that the files are distributed as desired before you remove the shadow relationship.

To move files between the two volumes to achieve a desired distribution of files:

1 In Novell Remote Manager for Linux, log in as the `root` user.

2 Select *View File System > Dynamic Storage Technology Options*, locate the volume in the list, then click the *Inventory* link next to it.

View the volume inventory for the shadow volume to determine the space in use and the available space for both the primary and the secondary areas of the shadow volume. Ensure that there is sufficient free space available in either location for the data that you plan to move to that location.

3 Use any combination of the following techniques to move data between the two areas:

- **Shadow Volume Policies:** Run an existing shadow volume policy by using the *Execute Now* option in the *Frequency* area of the policy. You can also create a new shadow volume policy that moves specific data, and run the policy by using the *One Time* and *Execute Now* options in the *Frequency* area of the policy.

  For information about configuring policies to move data between the primary and secondary areas, see Chapter 10, "Creating and Managing Policies for Shadow Volumes," on page 101.

- **Inventories:** Use the detailed inventory reports or customized inventories to move specific files to either area.

  For information about using the volume customized inventory options to move data between the primary and secondary areas, see Section 11.5, "Generating a Custom Inventory Report," on page 125.

4 (Optional) While the DST pool cluster resource is online, you can delete volume-specific policies as described in Section 10.8, "Deleting a Shadow Volume Policy," on page 114.

Shadow volume policies that you configured for the DST volume do not run after you remove the shadow volume relationship. The policy information is stored in the `/media/nss/` `<primary_volumename>/._NETWARE/shadow_policy.xml` file. Policy information is not automatically removed from the file when you remove the shadow relationship. If you later define a new shadow volume relationship for the primary volume, the policies apply to it.

5 Continue with Section 13.9.3, "Removing the Shadow Definition and NCP/NSS Bindings Exclusion on All Nodes," on page 170.

13.9.3 Removing the Shadow Definition and NCP/NSS Bindings Exclusion on All Nodes

You must remove the shadow definition for the DST shadow volume pair and the NCP/NSS bindings exclusion for the secondary volume on each node in turn. This requires a restart of NDSD and NCP2NSS on each node, which creates a short service outage for all NSS volumes on the node. You can minimize the impact by cluster migrating the pool cluster resources for the other NSS volumes to other nodes while you are modifying the configuration files on a given node.

1 Log in as the `root` user to the node where the primary pool cluster resource is online, then open a terminal console.

2 Offline the DST pool cluster resource that is managing the clustered shadow volume.

```
cluster offline resource_name
```

This unloads the cluster resource and deactivates the cluster pools and their volumes so that the cluster is not controlling them. Do not bring the primary resource or secondary resource online, and do not locally mount the volumes on any node at this time.

3 Remove the shadow volume and NCP/NSS bindings exclusion information from each node in the cluster:

   3a Log in to the node as the `root` user.

   3b In a text editor, open the `/etc/opt/novell/ncp2nss.conf` file, remove the EXCLUDE_VOLUME line for the secondary volume from the file, then save the file.

   ```
   EXCLUDE_VOLUME secondary_volumename
   ```

   For example:

   ```
   EXCLUDE_VOLUME ARCVOL1
   ```

   3c In a text editor, open the `/etc/opt/novell/ncpserv.conf` file, remove the SHADOW_VOLUME line for the shadow volume from the file, then save the file.

   ```
   SHADOW_VOLUME primary_volumename secondary_volume_path
   ```

   For example:

   ```
   SHADOW_VOLUME VOL1 /media/nss/ARCVOL1
   ```

   3d Restart the Novell eDirectory daemon by entering the following commands:

   ```
   rcndsd stop
   ```

   ```
   rcndsd start
   ```

3e Restart the NCP/NSS IPC daemon to synchronize the changes you made to the `/etc/opt/novell/ncp2nss.conf` file. At the terminal console prompt, enter

```
/etc/init.d/ncp2nss restart
```

If the NCP/NSS IPC daemon restarts successfully, the following messages are displayed in the terminal console:

```
Shutting down Novell NCP/NSS IPC daemon...
Exited
Starting the Novell NCP/NSS IPC daemon.
```

3f Repeat these steps for each node in the cluster.

4 After the shadow and bindings information has been removed from all nodes, continue with Section 13.9.4, "Preparing the Primary Pool Cluster Resource for Independent Use," on page 171.

13.9.4 Preparing the Primary Pool Cluster Resource for Independent Use

In the primary pool cluster resource scripts, remove (or comment out) the lines for the management of the secondary pool, secondary volume, and `shadowfs`. This allows the pool cluster resource to function independently.

1 In iManager, select *Clusters*, then select *My Clusters*.

2 Select the name link of the cluster you want to manage.

3 On the Cluster Manager page, click the name link of the primary cluster resource to view its Cluster Pool Properties page, then click the *Scripts* tab.

4 On the *Scripts > Load Script* page, modify the load script of the primary pool cluster resource:

4a Remove or comment out the activation command for the secondary pool and the sleep command you added for the pool activation:

```
#exit_on_error nss /poolact=ARCPOOL1
#sleep 10
```

4b Remove or comment out the `ncpcon mount` command for the shadow volume:

```
#exit on error ncpcon mount VOL1=254,shadowvolume=ARCVOL1
```

4c Add (or uncomment) a command to mount the NSS volume:

```
exit_on_error ncpcon mount <volume_name>=<volume_id>
```

Replace *volume_name* with the primary NSS volume name, such as VOL1.

Replace *volume_id* with a number that is unique across all nodes in the cluster, such as 254.

For example:

```
exit_on_error ncpcon mount VOL1=254
```

4d If `shadowfs` was used, remove or comment out the wait time for `shadowfs` to start.

```
# If shadowfs is used, wait for shadowfs to start
#for (( c=1; c<=10; c++ )) do
# if [ ! -d /media/shadowfs/VOLUME/._NETWARE ]; then sleep 5; fi
#done
```

4e Click *Apply* to save your changes.

The changes do not take effect until the cluster resource is brought online.

5 On the *Scripts > Unload Script* page, modify the unload script of the primary pool cluster resource:

5a Remove or comment out the deactivation command for the secondary pool:

```
#ignore_error nss /pooldeact=ARCPOOL1
```

5b If shadowfs was used, remove or comment out the fusermount -u command.

```
# If shadowfs is used, unload the volume in FUSE
#ignore_error fusermount -u /media/shadowfs/VOL1
```

5c Click *Apply* to save your changes.

The changes do not take effect until the cluster resource is brought online.

6 On the *Scripts > Monitor Script* page, modify the monitor script of the primary pool cluster resource:

6a Remove or comment out the status command for the secondary pool:

```
# Check the status of the secondary pool
#exit_on_error status_fs /dev/pool/ARCPOOL1 /opt/novell/nss/mnt/.pools/ARCPOOL1
nsspool
```

6b Click *Apply* to save your changes.

The changes do not take effect until the cluster resource is brought online.

7 Click *OK* to return to the Cluster Manager page.

8 Online the revised pool cluster resource. On the Cluster Manager page, select the check box next to the pool cluster resource, then click *Online*.

The resource comes online as an independent pool and volume on a node in the resource's preferred nodes list.

If the resource goes comatose instead of coming online, take the resource offline, check the scripts, then try again.

9 Continue with Section 13.9.5, "Preparing the Secondary Pool and Volume for Independent Use," on page 172.

13.9.5 Preparing the Secondary Pool and Volume for Independent Use

When you defined the clustered DST shadow volume pair, you might have used a clustered pool or a shared-but-not-cluster-enabled pool.

Apply one of the following methods to use the pool and volume independently:

- ◆ "Modifying the Secondary Pool Cluster Resource" on page 173
- ◆ "Cluster-Enabling a Shared Secondary Pool" on page 173
- ◆ "Unsharing the Secondary Pool to Use It Locally on the Node" on page 175

Modifying the Secondary Pool Cluster Resource

If you used a clustered secondary pool cluster resource, ensure that the volume ID is unique across all nodes in the cluster before you bring the pool resource online as an independent pool.

IMPORTANT: If you deleted the secondary pool cluster resource after you merged its information in the primary pool cluster resource scripts, the secondary resource no longer exists. You can cluster-enable the shared-but-not-cluster-enabled pool as described in "Cluster-Enabling a Shared Secondary Pool" on page 173, or you can unshare the pool as described in "Unsharing the Secondary Pool to Use It Locally on the Node" on page 175.

---

1 In iManager, select *Clusters*, then select *My Clusters*.

2 Select the name link of the cluster you want to manage.

3 Go to the secondary resource's load script and verify that the volume ID is unique for the secondary volume.

If you have assigned the volume ID to another clustered volume while the secondary resource was unused, the duplicate volume ID will cause the secondary resource to go comatose when you try to bring it online.

   3a On the Cluster Manager page, click the name link of the secondary cluster resource to view its Cluster Pool Properties page, then click the *Scripts* tab.

   3b On the *Scripts > Load Script* page, check the volume ID to ensure it is unique:

```
exit_on_error ncpcon mount ARCVOL1=253
```

   3c Click *OK* to save your changes and return to the Cluster Manager page.

The changes do not take effect until the cluster resource is brought online.

4 Online the secondary pool cluster resource. On the Cluster Manager page, select the check box next to the primary pool cluster resource, then click *Online*.

The resource comes online as an independent pool and volume on a node in the resource's preferred nodes list.

If the resource goes comatose instead of coming online, take the resource offline, check the scripts, then try again.

If the resource goes online successfully, you are done.

Cluster-Enabling a Shared Secondary Pool

You can cluster-enable the shared pool and volume as an independent pool cluster resource:

- If you used a shared-but-not-clustered secondary pool. In this case, the Pool object name and Volume object name contain the name of the node where they were originally created.

- If you used a cluster-enabled deleted the secondary pool cluster resource after you merged its information in the primary pool cluster resource scripts. In this case, the Pool object name and Volume object name contain the cluster name, because the objects were recreated when you cluster-enabled them.

Before you attempt to cluster-enable the shared pool, you must update the Pool object and Volume object in Novell eDirectory to use the hostname of the server where you took the primary pool cluster resource offline.

1 In NSSMU, update the Novell eDirectory object for the shared pool and volume.

You can alternatively use the Storage plug-in for iManager to update the eDirectory objects. Select the server where you took the clustered DST pool resource offline. Ensure that you dismount the volume and deactivate the pool after you have updated their objects.

1a Log in as the `root` user on the node where you took the primary pool cluster resource offline, then open a terminal console.

1b Launch NSSMU. At the command prompt, enter

```
nssmu
```

1c Activate the pool and update its eDirectory object to create a Pool object that is named based on the hostname of the current node.

1c1 In the NSSMU menu, select *Pools*, then press Enter.

1c2 Select the secondary pool (ARCPOOL1), then press F7 to activate it.

1c3 Select the secondary pool, press F4 (*Update NDS*), then press y (Yes) to confirm that you want to delete the old Pool object and add a new Pool object.

1c4 Press Esc to return to the NSSMU menu.

1d Mount the volume, update its eDirectory object to create a Volume object that is named based on the hostname of the current node, then dismount the volume.

1d1 In the NSSMU menu, select *Volumes*, then press Enter.

1d2 Select the secondary volume (ARCVOL1), then press F7 to mount it.

1d3 Select the secondary volume, press F4 (*Update NDS*), then press y (Yes) to confirm that you want to delete the old Volume object and add a new Volume object.

1d4 Select the secondary volume, then press F7 to dismount it.

1d5 Press Esc to return to the NSSMU menu.

1e Deactivate the pool.

1e1 In the NSSMU menu, select *Pools*, then press Enter.

1e2 Select the secondary pool (ARCPOOL1), then press F7 to deactivate it.

1f Press Esc twice to exit NSSMU.

2 In iManager, select *Clusters > My Clusters*.

3 Select the name link of the cluster you want to manage.

4 Cluster-enable the shared pool.

For detailed instructions, see "Cluster-Enabling an Existing NSS Pool and Its Volumes" in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

4a Click the *Cluster Options* tab, then click *New*.

4b On the Resource Type page, select *Pool*, then click *Next*.

4c On the Cluster Pool Information page:

4c1 Browse to select the secondary pool, such as *<hostname>*_ARCPOOL1_POOL.

4c2 Specify a unique IP address.

4c3 Select the NCP, AFP, or CIFS check boxes for the advertising protocols that you want to enable for the volume.

NCP is selected by default and is required to support authenticated access to data via the Novell Trustee Model. If Novell CIFS or Novell AFP is not installed, selecting its check box has no effect.

4c4 If you enable CIFS, verify the default name in the *CIFS Server Name* field.

You can modify this name. The name must be unique and can be up to 15 characters, which is a restriction of the CIFS protocol.

4c5 *Online Resource After Creation* is disabled by default. This allows you to review the settings and scripts before you bring the resource online for the first time.

4c6 *Define Additional Properties* is enabled by default. This allows you to set resource policies and preferred nodes before the resource is brought online.

4c7 Click *Next*.

4d On the Resource Policies page, configure the policies for the start, failover, and failback mode, then click *Next*.

4e On the Resource Preferred Nodes page, assign and rank order the preferred nodes to use for the resource, then click *Finish*.

5 (Optional) Enable monitoring for the pool cluster resource.

5a On the Cluster Options page, select the name link for the resource to open its Properties page.

5b Click the *Monitoring* tab.

5c Select *Enable Resource Monitoring*, set the *Polling Interval*, *Failure Rate*, and *Failure Action*, then click *Apply*.

5d Click the *Scripts* tab, then click Monitor Script.

5e View the script settings and verify they are as desired.

5f If you modify the script, click *Apply*.

5g Click *OK*.

6 Bring the pool cluster resource online. Click the *Cluster Manager* tab, select the resource check box, then click *Online*.

If the resource goes online successfully, you are done.

Unsharing the Secondary Pool to Use It Locally on the Node

You can unshare the shared pool and volume and use them locally on the node:

- If you used a shared-but-not-clustered secondary pool. In this case, the Pool object name and Volume object name contain the name of the node where they were originally created.

- If you used a cluster-enabled deleted the secondary pool cluster resource after you merged its information in the primary pool cluster resource scripts. In this case, the Pool object name and Volume object name contain the cluster name, because the objects were recreated when you cluster-enabled them.

Before you attempt to use pool and volume locally, you must update the Pool object and Volume object in Novell eDirectory to use the hostname of the server where you took the primary pool cluster resource offline.

To mount the secondary volume as an independent local volume:

1 Log in as the `root` user on the node where you took the primary pool cluster resource offline, then open a terminal console.

2 Launch NSSMU. At the command prompt, enter

`nssmu`

3 In NSSMU, update the Novell eDirectory object for the shared pool and volume.

You can alternatively use the Storage plug-in for iManager to update the eDirectory objects. Select the server where you took the clustered DST pool resource offline.

   3a Activate the pool and update its eDirectory object to create a Pool object that is named based on the hostname of the current node.

      3a1 In the NSSMU menu, select *Pools*, then press Enter.

      3a2 Select the secondary pool (ARCPOOL1), then press F7 to activate it.

      3a3 Select the secondary pool, press F4 (*Update NDS*), then press y (Yes) to confirm that you want to delete the old Pool object and add a new Pool object.

      3a4 Press Esc to return to the NSSMU menu.

   3b Mount the volume, then update its eDirectory object to create a Volume object that is named based on the hostname of the current node.

      3b1 In the NSSMU menu, select *Volumes*, then press Enter.

      3b2 Select the secondary volume (ARCVOL1), then press F7 to mount it.

      3b3 Select the secondary volume, press F4 (*Update NDS*), then press y (Yes) to confirm that you want to delete the old Volume object and add a new Volume object.

      3b4 Press Esc to return to the NSSMU menu.

4 In the NSSMU menu, select *Devices*, then press Enter.

5 Disable sharing for the device. Select the device, press F6 to unshare the device, then press y (Yes) to confirm.

If NSSMU does not allow you to unshare the device, you can use the SAN management software to ensure that the device is allocated only to the current server, then try again.

6 In the NSSMU menu, select *Pools*, then press Enter.

7 Select the pool and verify that it is unshared.

8 Press Esc twice to exit NSSMU.

14 Troubleshooting for Dynamic Storage Technology

This section describes issues and possible workarounds for Dynamic Storage Technology (DST) for Novell Open Enterprise Server (OES) 2 Linux.

- Section 14.1, "My NCP server information is set to: LOCAL_CODE_PAGE CP437. Why is it not using UTF-8?," on page 177
- Section 14.2, "A File is listed twice in a directory," on page 177
- Section 14.3, "Users cannot see some files and directories," on page 178
- Section 14.4, "Cross-protocol locking stops working," on page 178
- Section 14.5, "Files that initially reside only on the secondary volume can end up as directories on the primary volume," on page 178

14.1 My NCP server information is set to: LOCAL_CODE_PAGE CP437. Why is it not using UTF-8?

All interaction with the Linux file system uses UTF-8. However, for backward compatibility with older Novell Clients, most of the NCPs use a server-defined local code page setting. The more recently defined Case 89 NCPs use UTF-8. We recommend that you configure your client to use them. If all of your clients are using the newer UTF-8 Case 89 NCPs, then there is no need to set the server's local code page.

14.2 A File is listed twice in a directory

If a file happens to be located in the same directory on both the primary and secondary storage, the file name is listed twice in the directory listing. However, all file operations are directed to the file on the primary system.

To resolve this problem, you can rename one instance of the file to make both versions of the file available under different names. Then open the files to determine which version to keep.

You can control how DST handles duplicate files by configuring global policies. For information, see Section 8.3, "Resolving Instances of Duplicate Files," on page 70.

14.3 Users cannot see some files and directories

If the secondary storage location becomes unavailable, it appears to users that some of their files and directories are suddenly missing. When the secondary storage location is back online, the files and directories are visible again.

Users might also observe that some files appear to be missing if NCP Server is having performance issues. Some tuning of NCP Server caching is recommended depending on the server RAM, volume size, number of files, and number of trustees accessing the volumes. For information about tuning issues for NCP Server, see *TID 7004888: NCP Performance Tuning on Open Enterprise Server 2 Linux* (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7004888) in Novell Support (http://www.novell.com/support).

14.4 Cross-protocol locking stops working

Cross-protocol locking allows SMB/CIFS users and NCP users to concurrently access files by allowing only one user at any time to open the file for write. Multiple users who are accessing via NCP and SMB/CIFS can open a file for read only.

> **WARNING:** Allowing users who access files via different protocols to concurrently open a file for write can lead to data corruption.

NCP Server for Linux provides cross-protocol locking for NCP and Linux SMB/CIFS users. Novell CIFS for Linux does not support cross-protocol locking in OES 2 SP1 Linux.

If cross-protocol locking is enabled for NCP Server for Linux but stops working for DST shadow volume pairs—that is, multiple users can open a file for read and write—it is probably because ShadowFS needs to be restarted. To resolve this problem, stop the shadowfs process, then start shadowfs. For information, see Section 12.11, "Starting and Stopping ShadowFS Manually," on page 136.

14.5 Files that initially reside only on the secondary volume can end up as directories on the primary volume

If a file and its associated directories in a DST volume initially reside only on the secondary volume, the file can show up as a directory when DST attempts to move from the secondary to the primary location, such as for a policy move. The original file remains intact on the shadow volume, but a directory with the same name is created on the primary. This causes the affected file to not be accessible for clients.

A patch that prevents this problem from happening is available in the OES 2 SP2 and OES 2 SP3 May 2011 Scheduled Maintenance patches.

For information about getting a script that can help find problem directories, remove them, and move the file from the shadow volume to the primary volume, see "Technical Information Document 7008532: Files initially only residing on the Shadow volume can end up as directories on the Primary volume" in the Novell Support Knowledgebase (http://www.novell.com/support/).

15 Security Considerations

This section describes security issues and recommendations for Dynamic Storage Technology (DST) for Novell Open Enterprise Server (OES) 2 Linux. It is intended for security administrators or anyone who is using DST and is responsible for the security of the system. It requires a basic understanding of NetWare Core Protocol (NCP) Server and DST. It also requires the organizational authorization and the administrative rights to carry out the configuration recommendations.

- Section 15.1, "Client Access," on page 179
- Section 15.2, "Linux-Enabled eDirectory Users," on page 179
- Section 15.3, "Using File System Trustees and Rights," on page 180
- Section 15.4, "Server-to-Server Access," on page 180
- Section 15.5, "Hidden Directories and Files," on page 180
- Section 15.6, "Shadow Volumes Audit Logs," on page 181
- Section 15.7, "Shadow File System Audit Logs," on page 181
- Section 15.8, "NCP Server Auditing and Log Files," on page 181
- Section 15.9, "Using Secure Remote Connections," on page 181

15.1 Client Access

NCP clients access the shadow volume through the NCP Engine.

SMB/CIFS clients access data on a shadow volume through ShadowFS. These users are Linux-enabled through Linux User Management.

Novell AFP and Novell CIFS for OES 2 SP1 Linux have not been tested with DST for the OES 2 SP1 Linux release, so they are not supported.

Other client protocols such as FTP, HTTP, and NFS are not supported.

15.2 Linux-Enabled eDirectory Users

Dynamic Storage Technology requires that all users of the shadow volume be users that are defined in Novell eDirectory. For information, see the *Novell eDirectory 8.8 SP7 Administration Guide*.

SMB/CIFS users must be enabled for Linux with Linux User Management. This is true for NCP volumes on Linux POSIX file systems (Ext3 and Reiser) and for NSS volumes on Linux and NetWare. The *OES 2 SP3: Novell Linux User Management Administration Guide* describes how to Linux-enable users for an OES 2 Linux server.

15.3 Using File System Trustees and Rights

Dynamic Storage Technology requires that file system access control for data be managed by using the Novell Trustee Model for file system trustees and trustee rights.

For all NCP volumes (NSS and NCP on Linux POSIX volumes), the trustee information is obtained at volume mount time from the `._NETWARE/.trustee_database.xml` file. When trustee changes are made, this trustee database file is updated. Because this file is located on the volume, it follows the volume from node to node as it moves around the cluster.

NCP trustee information is synchronized with the NSS file system. When an NCP user makes a trustee change, the NCP Server informs NSS of the change. When NSS changes a trustee assignment, it generates an event that the NCP Server listens for so NCP can keep up to date on NSS changes. When DST is involved, events from the secondary NSS volume are also noted, and trustee changes are also synchronized with it.

IMPORTANT: For NCP volumes, ensure that the *Inherit POSIX Permissions* option is disabled (the default setting). When this setting is disabled, the local Linux environment access is restricted to the `root` user and the file owner or creator, which is the most secure configuration. For information, see "Configuring Inherit POSIX Permissions for an NCP Volume" in the *OES 2 SP3: NCP Server for Linux Administration Guide*.

Rights and trustee management across multiple file systems should all be managed with the NCP tools. There are rights model mapping problems with using a POSIX rights model on NCP volumes, and vice versa.

15.4 Server-to-Server Access

iSCSI is the only protocol supported for server-to-server access that allows a remote volume to be used as a primary or secondary storage area for a shadow volume.

15.5 Hidden Directories and Files

- Section 15.5.1, "Trustee Database," on page 180
- Section 15.5.2, "Available Space Trends," on page 180

15.5.1 Trustee Database

A copy of the trustee database is placed in the `._NETWARE` subdirectory in both the primary tree and the shadow tree.

15.5.2 Available Space Trends

An available space trend data file is placed in the `._NETWARE` directory in both the primary tree and the shadow tree. It is used by the volume inventory option in Novell Remote Manager for Linux.

15.6 Shadow Volumes Audit Logs

An audit log for a DST shadow volume is located in the `._NETWARE` directory at the root of the primary volume. For NSS volumes, the default file path for the log is `/media/nss/`*volumename*`/._NETWARE/`*volumename*`.audit.log`. All moves between the primary storage area and the secondary storage area are logged as events to the shadow volume's audit log.

For example, if the primary area is named `VOL1`, the audit file is `/media/nss/`*VOL1*`/._NETWARE/`*VOL1*`.audit.log`.

15.7 Shadow File System Audit Logs

Audit logs for the Shadow File System are located in the `/var/opt/novell/log/shadowfs.log` file.

15.8 NCP Server Auditing and Log Files

The following log files are located in the `/var/opt/novell/log` directory:

- `ncpserv.log`
- `ncp2nss.log`
- `ncptop.log`

Log files are managed by `logrotate`. For information on usage, see its man page (`man logrotate`).

The control files for `logrotate` are:

- `/etc/logrotate.d/novell-ncpserv-log`
- `/etc/logrotate.d/novell-ncpserv-audit`
- `/etc/logrotate.d/novell-ncp2nss-log`
- `/etc/logrotate.d/novell-ncp2nss-audit`

By default, the rollover size is 16 MB and 5 compressed copies are kept.

15.9 Using Secure Remote Connections

If the primary storage area or secondary storage area is connected across remote connections, the connection must be secure. For example, use a virtual private network (VPN) or a private WAN connection.

IMPORTANT: iSCSI is the only protocol supported for remote server-to-server connections.

Ensure that authentication, encryption, and data integrity are secure when accessing and transferring data across the network. For example, if sensitive data is written to the primary volume, that data might be written to the secondary volume, depending on shadow policies in place. If there is an anonymous NFS mount for the shadow volume, the data is transferred in the clear over the network, where it might be prone to attacks or capture. In this case, you want to ensure that only authenticated users are able to access the NFS mount and that the connection between the servers is secure.

A
 Commands and Utilities for DST

This section describes commands and utilities for Dynamic Storage Technology (DST) for Novell Open Enterprise Server (OES) 2 for Linux.

A.1 Using NCPCON for DST Commands

The NetWare Core Protocol (NCP) Console Command (NCPCON) utility provides an interface for issuing NetWare commands in a Linux environment. You can issue commands via the NCPCON in three modes:

A.1.1 Interactive Mode

Open a terminal console, log in as the `root` user, then enter

`ncpcon`

This opens the NCPCON interactive console in the terminal console, so you can enter the NCP Server console commands. Enter `exit` to stop interactive mode.

Escaping the quotation mark character (`"`) is not required when you enter the command from the `ncpcon` prompt.

For example, enter the following commands from the `ncpcon` prompt:

`mount sys`

`shift VOL1:"path\file name with spaces.txt" shadow`

```
send "hello world" to all
```

A.1.2   Command Line Mode

For command line mode, issue an NCP Server command at a terminal console prompt by prepending the command with `ncpcon`:

```
ncpcon [command]
```

When you use `ncpcon` to issue commands directly from the console command prompt, you must escape the quotation mark character (") by preceding the character with a backslash (\), such as \".

For example, enter the following commands from the terminal console prompt:

```
ncpcon mount sys
```

ncpcon shift VOL1:\"path\file name with spaces.txt\" shadow

```
ncpcon send \"hello world\" to all
```

A.1.3   Scripting Mode

For scripting mode, issue the NCP Server command in the script by prepending the command with `ncpcon`, then placing quotation marks (") around the NCP Server command:

```
ncpcon "[command]"
```

If the command includes a field that must be contained in quotation marks (such as a file name), you must escape each internal quotation mark character (") with a backslash (\) character, such as \".

For example, place the following commands in a script file:

```
ncpcon "mount sys"
ncpcon "shift VOL1:\"path\file name with spaces.txt\" shadow"
ncpcon "send \"hello world\" to all"
```

A.2   DST Commands for NCPCON

The commands in this section can be used only with the NCP Console Command utility. You can issue the commands from the NCP Console interactive mode, or prepend the command with `ncpcon` when issuing it from a script or at a terminal console prompt as the `root` user. For information, see

create shadow_volume *<primary_volumename> <shadow_path>*/ID=*<volume_id>*

Creates a non-clustered shadow association between a primary NSS volume and secondary NSS volume, and adds the SHADOW_VOLUME mount information to the /etc/opt/novell/ ncpserv.conf file.

When you issue the command from the NCP Console, you do not need to restart `ndsd` in order for the changes to take effect. When you issue the command from a Linux prompt, you must restart `ndsd` in order for the changes to take effect.

OPTIONS

primary_volumename

Specifies the volume name for the primary NSS volume, such as VOL1.

shadow_path

Specifies the Linux path of the mount location for the secondary NSS volume, such as /media/nss/ARCVOL1.

/ID=<*volume_id*>

Specifies a unique volume ID (0 to 254) to use when mounting the shadow volume.

When the primary volume has a state of *Shadowed*, the volume ID that you assign as its NCP volume ID represents the DST shadow volume pair of volumes. The secondary volume does not have a separate volume ID when it is in the shadow relationship.

EXAMPLES

`create shadow_volume VOL1 /home/shadows/VOL1`

Creates a shadow volume where VOL1 is the primary storage area and /home/shadows/VOL1 is its mount point as a shadow volume.

`remove shadow_volume [/l] [/i] [/f] <primary_volumename>`

Removes the non-clustered shadow relationship between a primary NSS volume and a secondary NSS volume, and removes the SHADOW_VOLUME command from the /etc/opt/novell/ncpserv.conf file. You must unmount the volume before you issue the command.

IMPORTANT: You can use this command as part of the process to unlink the primary and secondary volumes of a non-clustered DST shadow volume. For information, see Section 9.12, "Removing the Shadow Relationship for a Non-Clustered DST Shadow Volume," on page 96.

Typically, you specify the /l option, which leaves the files in place on the primary volume and secondary volume, and removes the shadow relationship. This is equivalent to the *Volume Tasks > Remove Shadow Action Options > Remove Shadow* option in Novell Remote Manager.

When the /l option is not used, the command attempts to move all files on the secondary volume to the primary volume, and then removes the shadow relationship between the two volumes. Ensure that the primary volume has sufficient space to accommodate the files before you unmount the volume and issue the remove command. Moving the files can take some time, depending on how much data must be moved. If a file move fails, the unlinking of the shadow relationship also fails. You can use the /i option to ignore file move errors and allow the unlinking to succeed. After the files on the secondary volume have been moved to the primary volume, the shadow relationship is removed, and a summary report is created and displayed.

OPTIONS

primary_volumename

Specifies the volume name for the primary NSS volume, such as VOL1.

/l

Leaves the files in place on the two volumes and removes the shadow relationship.

/i

Ignores any file move errors that might occur if you issue the command without the /l option, and allows the unlinking of the shadow relationship to succeed.

For example, if there are duplicate files on the volumes, the duplicate instance on the secondary volume cannot be moved to the primary volume, and the shadow relationship cannot be unlinked. Using the /i option ignores the file move error and allows the relationship to be unlinked.

/f

Provides a full detail report of actions taken. Use this option to understand which file moves might be failing.

EXAMPLES

Issue the following commands from the NCP Console, or add `ncpcon` at the front of the command when issuing it from a script or at a terminal console prompt.

`ncpcon remove shadow_volume /i /f VOL1`

> Removes the shadow relationship for shadow volume `VOL1`, and moves all files from the secondary storage area to the primary storage area. You must dismount `VOL1` before you issue this command. File move errors are ignored. Full details of the actions taken are reported.

`remove shadow_volume /l VOL1`

> Removes the shadow relationship for shadow volume `VOL1`, and leaves files where they currently are on the secondary storage area and the primary storage area. You must dismount `VOL1` before you issue this command.

`shadow <primary_volumename> operation=<lp | ls | mp | ms> [options]`

Allows you to list files on the shadow volume, or to move files between the primary storage area and the secondary storage area based on specified criteria. All files on the selected shadow volume that match the criteria are moved. Use the command from within `cron` jobs to automate data partitioning.

OPERATION OPTIONS

lp

> Lists primary files. Lists all files currently residing on the primary storage area.

ls

> Lists shadow files. Lists all files currently residing on the secondary storage area.

mp

> Moves files to primary. Moves files that match the specified criteria to the primary storage area from the secondary storage area.

ms

> Moves files to shadow. Moves files that match the specified criteria to the secondary storage area from the primary storage area.

OPTIONS

primary_volumename

> Specifies the volume name for the primary NSS volume, such as `VOL1`.

`pattern="searchPattern"`

> Specifies the file pattern to match against.

`owner="username.context"`

> Specifies the Novell eDirectory user name and context of the owner of the files to match against.

`uid=uidValue`

> Specifies the Linux user ID to match against.

`time=[time_field]`

> Specifies which time field to match against, where the *time_field* is:
>
> [m] [a] [c]
>
> - **m:** Last time modified (content)
> - **a:** Last time accessed

- ◆ **c:** Last time changed (metadata)

range=[*time_period*]

Specifies which time period to match against, where the *time_period* is:

[a][b][c][d][e][f][g][h][i][j]

- ◆ **a:** Within last day
- ◆ **b:** 1 day to 1 week
- ◆ **c:** 1 week to 2 weeks
- ◆ **d:** 2 weeks to 1 month
- ◆ **e:** 1 month to 2 months
- ◆ **f:** 2 months to 4 months
- ◆ **g:** 4 months to 6 months
- ◆ **h:** 6 months to 1 year
- ◆ **i:** 1 year to 2 years
- ◆ **j:** More than 2 years

size=[*size_differential*]

Specifies the size differential to match against, where the *size_differential* is:

[a][b][c][d][e][f][g][h][i][j][k]

- ◆ **a:** Less than 1 KB
- ◆ **b:** 1 KB to 4 KB
- ◆ **c:** 4 KB to 16 KB
- ◆ **d:** 16 KB to 64 KB
- ◆ **e:** 64 KB to 256 KB
- ◆ **f:** 256 KB to 1 MB
- ◆ **g:** 1 MB to 4 MB
- ◆ **h:** 4 MB to 16 MB
- ◆ **i:** 16 MB to 64 MB
- ◆ **j:** 64 MB to 256 MB
- ◆ **k:** More than 256 MB

output="*filename*"

Outputs the search results to the specified file.

EXAMPLES

shadow VOL1 operation=ls pattern="*.exe"

Lists all files of type EXE that currently reside on the secondary storage area for the shadow volume VOL1.

shadow VOL1 operation=lp size=g

Lists all files of sizes between 1 MB to 4 MB that currently reside on the primary storage area for the shadow volume VOL1.

```
shadow VOL1 operation=ms time=m range=j
```

> Moves all files on the primary storage area that have not been modified in more than two years from the primary storage area to the secondary storage area for the shadow volume `VOL1`.

```
shift "primary_volumename:\path\filename" [primary | shadow]
```

Returns the specified file's location as being on the primary storage area or secondary storage area. Specify the primary or secondary options to move the specified file from its current location to the specified storage area.

IMPORTANT: The `shift` command works only at the command line, and not in `ncpcon` interactive mode. Enter the command as the `root` user at a terminal console prompt.

OPTIONS

primary

> Moves the specified file from the secondary storage area to the primary storage area. The file must be closed when you issue the command; otherwise, the command fails.

shadow

> Moves the specified file from the primary storage area to the secondary storage area. The file must be closed when you issue the command; otherwise, the command fails.

EXAMPLES

Enter the commands as the `root` user at a terminal console prompt.

```
ncpcon shift VOL1:"path\textfile.txt"
```

> Shows the specified file's storage area location in the shadow volume as primary (the primary storage area) or shadow (the secondary storage area) for the shadow volume `sys`.

```
ncpcon shift VOL1:"path\textfile.txt" primary
```

> Moves the specified file's storage area location from the secondary storage area to the primary storage area for the shadow volume `sys`.

```
ncpcon shift VOL1:"path\textfile.txt" shadow
```

> Moves the specified file's storage area location from the primary storage area to the secondary storage area for the shadow volume `sys`.

A.3 DST Commands for NCPCON for Use with Novell Cluster Services for Linux Clusters

NCPCON supports the commands in this section for use with Dynamic Storage Technology in combination with Novell Cluster Services for Linux clusters.

Use the syntax examples in this section in cluster load scripts to mount the volume in a cluster. With clustering, no changes are needed to the `ncpserv.conf` file for shadowing. The primary volume information should not be manually added to the `ncpserv.conf` file.

When the primary volume has a state of *Shadowed,* the volume ID that you assign as its NCP volume ID represents the DST shadow volume pair of volumes. The secondary volume does not have a separate volume ID when it is in the shadow relationship.

A.3.1   Scenario 1: Primary NSS and Shadow NSS

`ncpcon mount volumename=volID,SHADOWVOLUME=shadow_volumename`

> Use this command in a cluster load script when the primary volume is an NSS volume and the secondary volume is an NSS volume. Both NSS volumes must already exist and be mounted in NSS.
>
> Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.
>
> **EXAMPLE**
>
> `ncpcon mount VOL1=254,SHADOWVOLUME=ARCVOL1`
>
> > Mounts the NSS volume named VOL1 with a volume ID of 254. The primary volume is an existing NSS volume named VOL1 (/media/nss/VOL1). The secondary volume is an existing NSS volume named ARCVOL1 (/media/nss/ARCVOL1).

A.3.2   Scenario 2: Primary Non-NSS and Shadow Non-NSS (Not supported)

`ncpcon mount volumename=volID,SHADOWPATH=shadowpath,path=primarypath`

> Use this command when the primary volume is a non-NSS volume and the secondary volume is a non-NSS volume.
>
> Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.
>
> **EXAMPLE**
>
> `ncpcon mount VOL1=254,SHADOWPATH=/media/ncpvolumes/ARCVOL1,path=/media/`
> `ncpvolumes/VOL1`
>
> > Mounts the NCP volume named VOL1 with a volume ID of 254. The primary volume's path is /media/ncpvolumes/VOL1. The secondary volume's path is /media/ncpvolumes/ARCVOL1.

A.3.3   Scenario 3: Primary Non-NSS and Shadow NSS (Not supported)

`ncpcon mount volumename=volID,SHADOWVOLUME=shadow_volumename,path=primarypath`

> Use this command when the primary volume is a non-NSS volume and the secondary volume is an NSS volume. The NSS volume must already exist on the system and be mounted in NSS.
>
> Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.
>
> **EXAMPLE**
>
> `ncpcon mount VOL1=254,SHADOWVOLUME=ARCVOL1,path=/media/ncpvolumes/VOL1`
>
> > Mounts the NCP volume named VOL1 with a volume ID of 254. The primary volume's path is /media/ncpvolumes/VOL1. The secondary volume is an existing NSS volume named ARCVOL1 (mounted at /media/nss/ARCVOL1).

A.3.4   Scenario 4: Primary NSS and Shadow Non-NSS (Supported for the Remote Secondary NSS Volume in the Technology Preview)

`ncpcon mount volumename=volID,SHADOWPATH=shadowpath`

> Use this command when the primary volume is an NSS volume and the secondary volume is a non-NSS volume. The NSS volume must already exist on the system and be mounted in NSS.

Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

EXAMPLE

```
ncpcon mount VOL1=254,SHADOWPATH=/media/ncpvolumes/ARCVOL1
```

Mounts an NSS volume named `VOL1` with a volume ID of 254. The primary volume is an existing NSS volume named `VOL1` (`/media/nss/VOL1`). The secondary volume is an NCP volume named `ARCVOL1` that is mounted at `/media/ncpvolumes/ARCVOL1`.

A.4 Configuring Global DST Policies by Using the SET Command

DST provides several global parameters for the `SET` command that can be used to customize DST for a given server. These settings control how DST behaves for all shadow volumes on the server. Initially, the parameters and default settings are in force, but the parameters are not explicitly added to the `/etc/opt/novell/ncpserv.conf` file. After you modify its default setting, an entry for the parameter and its new setting are added to the file. The parameter entry remains in the file even if you modify the setting back to the default.

IMPORTANT: If you use DST shadow volumes in a cluster, ensure that you set the same global policies on each OES 2 Linux node in the cluster where you plan to fail over the shared volumes.

 * Section A.4.1, "Understanding DST Parameters for the SET Command," on page 190
 * Section A.4.2, "Using Novell Remote Manager to Configure DST Parameters for the SET Command," on page 192
 * Section A.4.3, "Using the ncpcon set Command to Configure DST Parameters," on page 193

A.4.1 Understanding DST Parameters for the SET Command

Table A-1 lists the DST parameters for the `SET` command with their default values and valid options.

Table A-1 *Manage NCP Services > Manage Server > Server Parameter Information*

Parameter Name and Description	Default Value	Valid Values
DUPLICATE_SHADOW_FILE_ACTION Controls how duplicate files conflicts are handled. For information, see Section 8.3.1, "Understanding Conflict Resolution for Duplicate Files," on page 70.	0	0 - Show duplicate shadow files (default) 1 - Hide duplicate shadow files 2 - Rename duplicate shadow files 3 - Delete duplicate files from shadow area 4 - Move duplicate shadow files to `/._DUPLICATE_FILES`

Parameter Name and Description	Default Value	Valid Values
DUPLICATE_SHADOW_FILE_BROADCAST Controls whether broadcast messages are sent to NCP users whenever duplicate files conflicts occur. For information, see Section 8.3.1, "Understanding Conflict Resolution for Duplicate Files," on page 70.	1	0 - Disable 1 - Allow
REPLICATE_PRIMARY_TREE_TO_SHADOW Controls how the primary tree is replicated from the primary tree to the shadow tree. By default, it is disabled, and paths are replicated to the secondary storage area when data is actually moved from the primary location to the secondary location. If it is enabled, the entire tree is replicated even if no files in a path have been moved to the secondary storage location. For information, see Section 8.1, "Replicating Branches of the Primary File Tree in the Secondary File Tree," on page 65.	0	0 - Disable 1 - Allow
SHIFT_MODIFIED_SHADOW_FILES Controls whether a file is moved from the secondary file tree to the primary file tree based on its modification time. For information, see "Shift Modified Shadow Files" on page 67.	1	0 - Disable 1 - Allow
SHIFT_ACCESSED_SHADOW_FILES Controls whether a file is moved from the secondary file tree to the primary file tree if it is accessed twice during a specific period of time. Use with SHIFT_DAYS_SINCE_LAST_ACCESS to specify the period of time. For information, see "Shift Accessed Shadow Files" on page 67.	0	0 - Disable 1 - Allow
SHIFT_DAYS_SINCE_LAST_ACCESS Specifies the number of days to use when determining if a file should be moved back to the primary storage area. When it is used with SHIFT_ACCESSED_SHADOW_FILES, the parameter sets the time when files are migrated back to the primary storage area after the second access within the specified elapsed time.	1	0 - Disable 1 to 365 (in days)

A.4.2 Using Novell Remote Manager to Configure DST Parameters for the SET Command

You can configure the DST parameters for the SET command by using Novell Remote Manager for Linux.

1 In Novell Remote Manager for Linux, select *Manage NCP Services*, then select *Manage Server*.

2 In the *Set Parameter Information* table, locate the DST parameter you want to configure.

The following server parameters are available. The settings shown are the default values. For information, see Section A.4.1, "Understanding DST Parameters for the SET Command," on page 190.

```
DUPLICATE_SHADOW_FILE_ACTION        0

DUPLICATE_SHADOW_FILE_BROADCAST     1

REPLICATE_PRIMARY_TREE_TO_SHADOW    0

SHIFT_ACCESSED_SHADOW_FILES         0

SHIFT_MODIFIED_SHADOW_FILES         1

SHIFT_DAYS_SINCE_LAST_ACCESS        1
```

3 Modify settings by clicking the link for the value in the *Parameter Value* column to open a page where you can change the value.

4 In *New Value*, type the value for the parameter, then click *Change* to save and apply the setting.

5 If you enabled DUPLICATE_SHADOW_FILE_BROADCAST, ensure that NCP Server is configured to support broadcast messages by verifying that the Disable Broadcast (DISABLE_BROADCAST) parameter for the SET command is disabled:

  5a In Novell Remote Manager for Linux, select *Manage NCP Services*, then select *Manage Server*.

  5b In the *Set Parameter Information* table, locate the DISABLE_BROADCAST parameter, then view the current value of the parameter. By default, the parameter is disabled (set to 0), which means that NCP Server supports broadcast messages.

  5c If the DISABLE_BROADCAST parameter is enabled (set to 1), click the link for the value in the *Parameter Value* column to open a page where you can change the value.

5d In *New Value*, type 0, then click *Change* to save and apply the settings that disable the DISABLE_BROADCAST parameter, which enables broadcasting for NCP Server.

> **IMPORTANT:** Messages are received only by logged-in users who are using Novell Client versions that are capable of receiving broadcast messages, and that are configured to receive them.

A.4.3 Using the ncpcon set Command to Configure DST Parameters

1 Open a terminal console on the Linux server, then log in as the `root` user.

2 At the terminal console prompt, enter

```
ncpcon set parameter_name=value
```

Replace *parameter_name* and *value* with the settings you want to change.

> **IMPORTANT:** Ensure that you enter the commands in lowercase.

For example, the following commands set the DST parameters to their default values.

```
ncpcon set duplicate_shadow_file_action=0
```

```
ncpcon set duplicate_shadow_file_broadcast=1
```

```
ncpcon set replicate_primary_tree_to_shadow=0
```

```
ncpcon set shift_modified_shadow_files=1
```

```
ncpcon set shift_accessed_shadow_files=0
```

```
ncpcon set shift_days_since_last_access=1
```

If the DUPLICATE_SHADOW_FILE_BROADCAST parameter is enabled, ensure that the DISABLE_BROADCAST parameter is disabled in order to allow broadcasting for NCP Server. For example, enter

```
ncpcon set disable_broadcast=0
```

A.5 DST Commands for /etc/opt/novell/ncpserv.conf

Use the commands in this section for the NCP Server configuration file (`/etc/opt/novell/ncpserv.conf`). The `ncpserv.conf` file is read only at Novell eDirectory startup time. If you modify this file directly, you must restart `ndsd` in order for the changes to take effect.

SHADOW_VOLUME *volume_name shadow_area_path*

Identifies a volume as having a secondary storage area and specifies the path to that secondary volume. Any NCP volume can have a shadow. The root directory for the shadow area needs to already exist; the rest of the directories in the secondary file tree is automatically created as needed. The volume shadow area is available next time the volume is mounted.

SHIFT_MODIFIED_SHADOW_FILES *value*

Enables a modified file to be moved from the secondary storage area to the primary storage area. The value can be either 0 (Disabled) or 1 (Allow). The default value is 1. When this parameter is on, and a file that is located in the secondary storage area is modified, the file is automatically moved back to the primary storage area when the file is closed.

SHIFT_ACCESSED_SHADOW_FILES *value*

Enables a file to be moved from the secondary storage area to the primary storage area if it is accessed as read-only a second time during a specified period of time. The value can be either 0 (Disabled) or 1 (Allow). The default value is 0. When this parameter is on, and a file that is located in the shadow area is accessed, if this is the second access within the configured SHIFT_DAYS_SINCE_LAST_ACCESS, the file is automatically moved back to the primary area when the file is closed.

SHIFT_DAYS_SINCE_LAST_ACCESS *value*

Specifies the number of days to use when determining if a file should be moved back to the primary storage area. The value may be 0 (Disable), or between 1 and 365 (in days). The default is 1. When it is used with SHIFT_ACCESSED_SHADOW_FILES, the parameter sets the time when files are migrated back to the primary storage area after the second access within the specified elapsed time.

DUPLICATE_SHADOW_FILE_ACTION *value*

Controls how duplicate files conflicts are handled. The default is 0.

0 - Show duplicate shadow files (default)

1 - Hide duplicate shadow files

2 - Rename duplicate shadow files

3 - Delete duplicate files from shadow area

4 - Move duplicate shadow files to /._DUPLICATE_FILES

DUPLICATE_SHADOW_FILE_BROADCAST *value*

Enables a message to be broadcast to an NCP user when a duplicate copy of a file is located on both the primary volume and the secondary volume. Valid settings are 0 (Disabled) and 1 (Allow). The default is Allow. The Novell Client version in use must support receiving broadcast messages in order for the user to receive the message.

REPLICATE_PRIMARY_TREE_TO_SHADOW *value*

Controls how the primary tree is replicated from the primary tree to the shadow tree. Valid settings are 0 (Disabled) and 1 (Allow). By default, it is disabled, and paths are replicated to the secondary storage area gradually as data is moved from the primary location to the secondary location. If it is enabled, the entire tree is replicated even if no files in a path have been moved to the secondary storage location.

A.6   DST Commands for /etc/opt/novell/shadowfs.conf

Use the commands in this section for the Shadow File System configuration file (/etc/opt/novell/shadowfs.conf).

SHADOW *root_path primary_area_path shadow_area_path*

Defines a shadow volume for ShadowFS. A shadow volume that is defined by the NCP engine is automatically mounted by ShadowFS and does not need to be defined in this configuration file.

SHIFT_ON_MODIFY *value*

Enables a modified file to be moved from the secondary storage area to the primary storage area. The value can be either 0 (Off) or 1 (On). The default value is 1. When this parameter is on, and a file that is located in the secondary storage area is modified, the file is automatically moved back to the primary area when the file is closed.

SHIFT_ON_ACCESS *value*

Enables a file to be moved from the secondary storage area to the primary storage area if it is accessed a second time during a specified time period. The value can be either 0 (Off) or 1 (On). The default value is 0. When this parameter is on, and a file that is located in the shadow area is accessed, if this is the second access within the configured SHIFT_DAYS_SINCE_LAST_ACCESS, the file is automatically moved back to the primary storage area when the file is closed.

SHIFT_DAYS_SINCE_LAST_ACCESS *value*

Specifies the number of days to use when determining if a file should be moved back to the primary storage area. The value may be 0 (Disable), or between 1 and 365 (in days). The default is 1. When it is used with SHIFT_ON_ACCESS, the parameter sets the time when files are migrated back to the primary storage area after the second access within the specified elapsed time.

A.7 DST EXCLUDE_VOLUME Command for /etc/opt/novell/ncp2nss.conf

Use the command in this section for the `/etc/opt/novell/ncp2nss.conf` file.

EXCLUDE_VOLUME *nss_volumename*

Prevents the named NSS volume from mounting in NCP Server. This command is added when you are using a specified NSS volume as the secondary storage area of a DST shadow volume.

An entry is automatically created in the `/etc/opt/novell/ncp2nss.conf` file by using Novell Remote Manager for Linux to set the *Manage NCP Services > Manage Shares > NCP/NSS Bindings > NCP Accessible* option to No for a given NSS volume that you want to use as a secondary storage location in a DST shadow volume. For instructions, see Section 9.4, "Configuring the NCP/NSS Bindings for an NSS Volume," on page 84.

In a cluster, you must manually copy the line to the `/etc/opt/novell/ncp2nss.conf` file on each node.

A.8 DST Shadow Volume Information in /etc/NCPVolumes

The `/etc/NCPVolumes` file is an XML file that contains an entry for each mounted volume. It lists the volume's name and the path for the volume's primary file tree (PRIMARY_ROOT). If the volume is a shadow volume, it also shows the path for the secondary file tree (SHADOW_ROOT). Using this data file, a backup utility can easily locate each mounted NCP volume and find its primary and secondary file trees.

For example, the following XML entry defines the DST shadow volume named VOL1:

```
<VOLUME>

    <NAME>VOL1</NAME>

    <PRIMARY_ROOT>/media/nss/VOL1</PRIMARY_ROOT>
```

```
<SHADOW_ROOT>/media/nss/ARCVOL</SHADOW_ROOT>
</VOLUME>
```

A.9 DST ShadowFS Volume Information in /etc/mtab.shadowfs

The /etc/mtab.shadowfs file is an XML file that contains an entry for each shadow volume mounted by ShadowFS. It lists the mount point, the path for the primary file tree, and the path for the secondary file tree.

For example, the following XML entry defines the DST shadow volume for ShadowFS named VOL1:

```
<SHADOWFS_MOUNTPOINTS>

    <MOUNTPOINT>

      <PATH>/media/shadowfs/VOL1</PATH>

      <PRIMARY_TREE>/media/nss/VOL1</PRIMARY_TREE>

      <SHADOW_TREE>/media/nss/ARCVOL</SHADOW_TREE>

    </MOUNTPOINT>

</SHADOWFS_MOUNTPOINTS>
```

B RPM Files for Dynamic Storage Technology

The following RPM files are installed for Dynamic Storage Technology for Novell Open Enterprise Server (OES) 2 Linux.

`novell-ncp.i386.rpm`

This RPM contains the NCP Server shared library (`libncpengine.so`) that runs as part of Novell eDirectory. This is the software that handles all client NetWare Core Protocol (NCP) requests.

`novell-ncpserv-nrm.i386.rpm`

This RPM contains the Novell Remote Manager for Linux plug-in provided by the NCP team (`libnrm2ncp.so`).

`novell-ncpserv.i386.rpm`

This RPM contains `ncpcon` and `ncptop` tools to help administrators manage the NCP Server. It also contains daemons that connect the `ncpserver` engine to other services on the server: `ncp2nss` and `lum2ncp`.

novell-nrm.i386

This RPM contains `httpstkd` and the shared library (`libnrm.so`) that creates Novell Remote Manager for Linux as an `httpstk` plug-in. It also contains other files used by Novell Remote Manager.

C Technology Preview: Creating and Managing DST Shadow Volumes with Remote Secondary NSS Volumes

This section describes how to configure and manage Novell Dynamic Storage Technology (DST) shadow volumes with remote secondary Novell Storage Services (NSS) volumes.

IMPORTANT: The remote secondary capability for DST shadow volumes is presented as a technology preview for Novell Open Enterprise Server (OES) 2 SP3 for Linux. It is not recommended for a production environment.

C.1 Understanding Remote Volume Support for the Technology Preview

In OES 2 SP3, Dynamic Storage Technology provides a technology preview for using a local primary NSS volume with a remote secondary NSS volume in a DST shadow volume pair. Figure C-1 illustrates the remote setup options. The DST server is an OES 2 SP3 Linux server running DST. The two primary NSS volumes reside on storage devices that are seen as local to the DST server, such as Fibre Channel, iSCSI, or direct-attached storage. The remote NSS volumes can reside on NetWare, OES 1 Linux, or OES 2 Linux servers that are in the same Novell eDirectory tree and partition as the primary NSS volumes. It does not matter if DST is also running on a remote OES 2 Linux server.

Figure C-1   *DST Remote Secondary Volume Support in the Technology Preview for OES 2 SP3 Linux*

MYCOMPANY_TREE
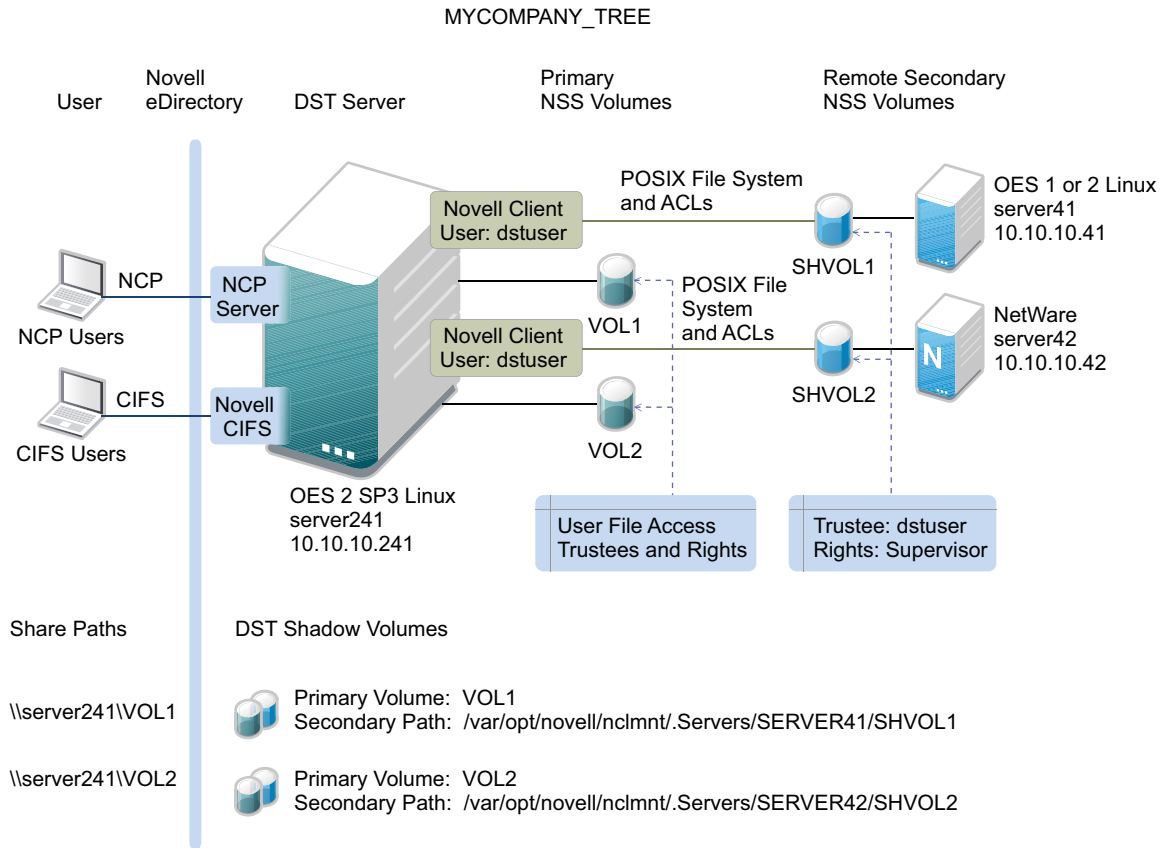
You use the Novell Client 2.3 for Linux (NCL) on the DST server to connect to a remote server. To allow DST to access data on the remote NSS volume, you must log in with the credentials (user name, password, context, and tree) of a user that is a file system trustee with the Supervisor right on the remote NSS volume. We recommend that you create a user identity to use only for this purpose. The full Linux path of the NCL mount point is used as the secondary path when you define the DST shadow volume pair.

NCL automatically mounts the remote volume as a native Linux POSIX file system, not as an NSS file system. This does not allow DST to exchange the full set of NSS file system and NCP (NetWare Control Protocol) access control lists (ACLs) when data is moved between the two volumes as DST does when the secondary NSS volume is local. Instead, NCL exchanges only the metadata that is compatible with the Linux POSIX file system and ACLs.

After you create a DST shadow volume, file system trustees and rights are set by using the merged view of the file trees. If the primary NSS volume contains data at create time, the current trustee and rights settings apply to files and folders in the primary and the secondary volumes. If the remote NSS volume contains data at create time, the settings are not automatically brought across to the primary volume. You must reset the file system trustees and rights from the merged view.

Because DST cannot push the metadata to the remote NSS volume through NCL, the NSS file system trustees and rights settings reside only on the primary volume. If you unlink the shadow volume pair, you must set up the file system trustees and rights for any data that remains on the remote NSS volume.

Both NCP users and Novell CIFS users can see a merged view of the data on the two NSS volumes. They access data via shares created on the primary NSS volume. DST controls access to the remote file system based on the file system rights of each user. It is not necessary to LUM enable the users.

An OES 2 SP3 patch release is planned that will allow DST to see the remote secondary NSS volumes as an NSS volume instead of a Linux POSIX file system. This will allow DST to exchange file system trustees and trustee rights with the remote NSS volumes so that both volumes have a synchronized copy of the settings. Figure C-2 illustrates the final vision for DST remote secondary NSS volume support.

Figure C-2   *DST Remote Secondary Volume Support that Allows NSS and NCP Metadata Exchange*
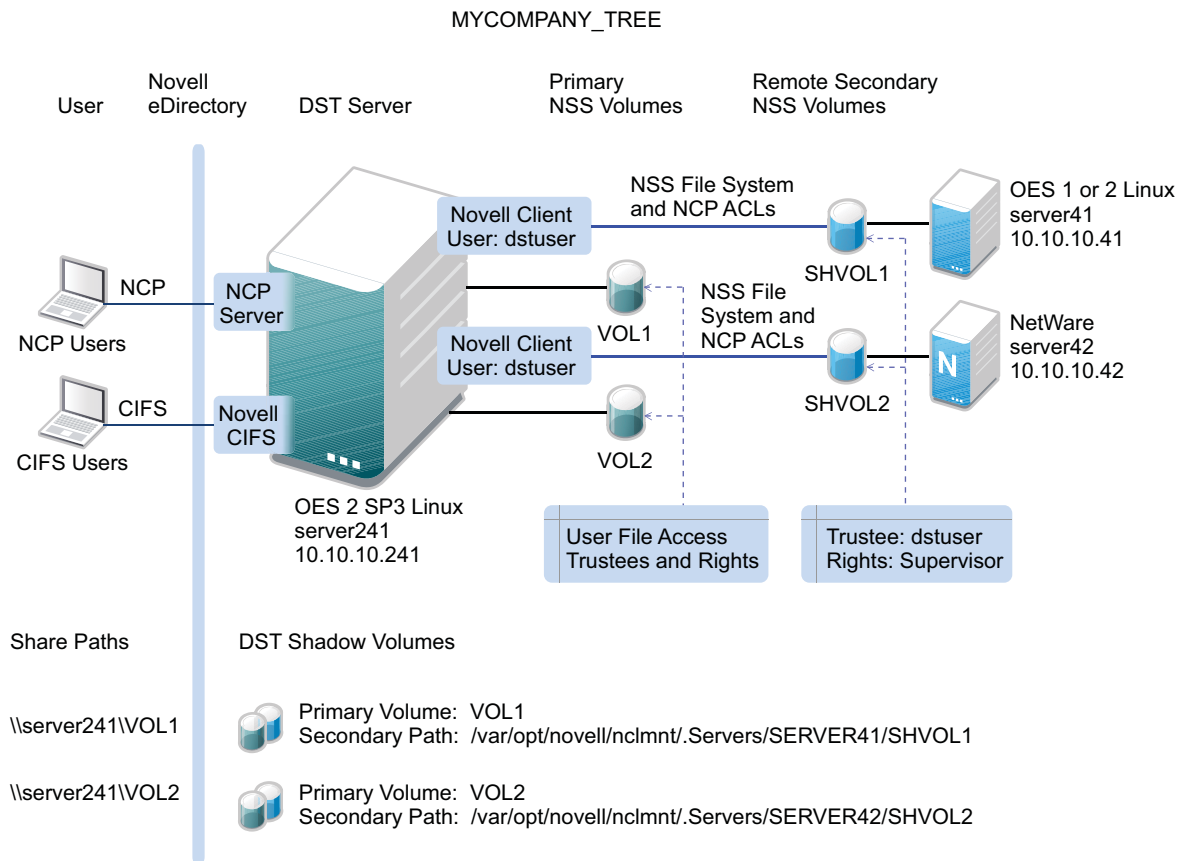
C.2   Requirements for Using a Remote Secondary NSS Volume

In addition to the requirements in Chapter 5, "Planning for DST Shadow Volumes and Policies," on page 41, your setup must meet the requirements in this section.

- Section C.2.1, "DST Server," on page 202
- Section C.2.2, "Remote Server," on page 202
- Section C.2.3, "Remote Secondary Volume," on page 202
- Section C.2.4, "DST User," on page 202
- Section C.2.5, "Novell Client for Linux," on page 203
- Section C.2.6, "User File System Access Rights," on page 204

C.2.1   DST Server

Dynamic Storage Technology must be installed and running on the primary OES 2 SP3 Linux server. For simplicity, this section refers to this server as the DST server.

C.2.2   Remote Server

Remote NSS volumes must reside in the same Novell eDirectory partition and tree as the DST server. It does not matter if DST is also running on a remote OES 2 Linux server. The following remote server platforms are supported:

- NetWare 6.5
- OES 1 Linux
- OES 2 Linux

Each remote server should have a globally unique hostname because the Novell Client uses the hostname when it mounts the remote volumes on the DST server.

C.2.3   Remote Secondary Volume

In a remote-volume scenario, the DST shadow volume uses the following:

- **Primary Volume:** An NSS volume that resides on devices that are seen as local drives on the DST server. This includes Fibre Channel, iSCSI, and direct-attached-storage devices.
- **Remote Secondary Volume:** An NSS volume that resides on devices that are seen as local drives on a remote server. The remote volume is mounted on the DST server by using the Novell Client for Linux.

C.2.4   DST User

You need an eDirectory user name and password to use for mapping remote NSS volumes to a DST server. The user name must be assigned as a trustee with the file system Supervisor right on the remote volume. The User object must reside in the same eDirectory partition and tree as the DST server. You can create a special-purpose user identity to be used only for mapping NSS volumes, such as `dstuser`.

IMPORTANT: The Novell Client allows only one user login to a given remote server. If you log in to multiple remote servers in the tree, you can use the same user identity or a different one for each server.

C.2.5 Novell Client for Linux

The Novell Client 2.0 SP3 for Linux (NCL) must be installed and running on the DST server. This is done by default on OES 2 Linux. For information about using NCL, see the Novell Client for Linux Documentation Web site (http://www.novell.com/documentation/linux_client/#20sp3).

The `nwlogin` command is used by the `root` user of the DST server to log in to the remote server. You need to supply the following information:

nwlogin Parameter	Description	Sample Value
Tree	eDirectory tree name that contains the two servers.	MYCOMPANY_TREE
Server	Hostname or IP address of the remote server. If the remote NSS volume is in a pool cluster resource, use the IP address of the cluster resource. If you supply an IP address, DST discovers the hostname of the server and uses it in the mount path on the DST server. Make sure your hostnames are globally unique so that the paths are unique on the DST server.	server41 10.10.10.41
User Name	User name of a user that is a file system trustee for the remote NSS volume with the Supervisor right. You can use any user name that has been configured with sufficient rights on the remote volume, or you can set up a special user for this login purpose, such as `dstuser`.	dstuser antonio
Context	eDirectory context for the specified user name.	users.context.mycomany
Password	Password for the specified user name.	password

The Novell Client automatically mounts the remote NSS volume as a native Linux POSIX file system. The default mount location is

`/var/opt/novell/nclmnt/.Servers/`*`remote_servername`*`/`*`remote_volumename`*

You must enable the Hidden Files view to see the `.Servers` folder in a file browser.

The *`remote_servername`* is the hostname of the remote server. The Novell Client creates the folder name for the remote server with uppercase characters. For example, if the server's hostname is `server41`, the folder name is `SERVER41`. The server folder contains the NSS volumes on the remote server and any system folders for the NSS file system. However, data access is restricted to the file system rights assigned for the user name you use to log in to the remote server.

The *`remote_volumename`* is the name of the NSS volume that you want to use as the secondary volume in a DST shadow volume pair. Supply the full Linux path for the volume when you specify it as the secondary path.

If the remote NSS volume is in a cluster, use the cluster IP address of the remote pool cluster resource when you map the NSS volume to the DST server. Because NCL uses the hostname of the remote server in the Linux path for the mount point, the mount point will change if the remote pool cluster resource fails over to another node in the remote cluster.

C.2.6 User File System Access Rights

The Novell Client for Linux mounts the remote NSS volume as a Linux POSIX file system. All access to data on the remote secondary volume is controlled by DST based on the NSS file system trustees and rights that are known to the primary NSS volume. After you create a DST shadow volume relationship, you must manage the file system trustees and file access rights only from the merged view.

In the technology preview, trustee and file system rights metadata remains with the primary volume. Only the primary volume has a copy of the trustee database file. The metadata is not pushed through the Novell Client to the remote NSS volume.

If the primary volume contains data at create time, DST applies the existing NSS file system trustee and rights settings to both the primary and secondary volumes. This is the same behavior as for local secondary volumes.

If the remote secondary volume contain data at create time, the file system trustees and rights for the secondary volume are not synchronized with the primary volume. You must set the file access rights for the data on the secondary volume from the merged view. Changes and settings on the primary volume are not pushed to the remote volume.

If the remote secondary NSS volume contains data and resides on an OES 1 Linux or OES 2 Linux server, its trustee and file system rights metadata is stored in the `../._NETWARE/ .trustee_database.xml` file at the root of the volume. If the primary NSS volume is empty, you can copy this file to a newly created primary volume to use as the initial settings for the DST shadow volume. For information, see .

C.3 Mounting a Remote NSS Volume with the Novell Client for Linux

You use the Novell Client for Linux to log in to the remote server. This mounts the remote NSS volume on the DST server. If there are multiple NSS volumes on the remote server, you need to log in only one time. Ensure that the login user name is assigned as a trustee and given the Supervisor right for each of those volumes. You can log in to multiple remote servers by using the same user name or a different user name for each server.

1 Log in to the DST server as the `root` user, then open a terminal console.

2 Open the Novell Client for Linux by entering

   `nwlogin`

3 Log in to the remote server by providing the following information in response to the prompts:

Parameter	Action	Sample Value
Tree	Enter the tree name.	EAST_TREE
Server	Enter the IP address or hostname of the remote server. If the remote volume is on a shared pool, enter the IP address of the pool cluster resource. This can create an oddly named file in the mount point that is a shortened version of the cluster virtual NCP servername.	10.10.10.41 server41

Parameter	Action	Sample Value
User Name	Enter the eDirectory user name of a user that is a file system trustee of the remote volume with the Supervisor right.	dstuser
Context	Enter the context of the specified login user.	users.boston.novell
Password	Enter the password of the specified login user.	password

On successful login, the response is:

```
Logged in
```

4 After a successful login, verify that the volume was successfully mounted by navigating to the default mount location for the volume.

The remote NSS volume is mounted by default on the DST server at

```
/var/opt/novell/nclmnt/.Servers/<remote_servername>/<remote_volumename>
```

For example:

```
/var/opt/novell/nclmnt/.Servers/SERVER41/DSTVOL1
```

5 Do one of the following:

- ◆ **Remote NetWare Server:** If the volume contains data, collect the trustee and file system access settings so that you can reset them later from the merged view of the DST shadow volume. Continue with Section C.5, "Creating a Shadow Volume with a Remote Secondary NSS Volume," on page 206.

- ◆ **Remote Linux Server:** If the remote NSS volume is on an OES 1 Linux or OES 2 Linux server, continue with Section C.4, "Copying a Remote Linux NSS Volume's Trustee Database to the Primary NSS Volume," on page 205.

C.4   Copying a Remote Linux NSS Volume's Trustee Database to the Primary NSS Volume

If the remote secondary NSS volume resides on an OES 1 Linux server or an OES 2 Linux server, its trustee information is stored in the `../._NETWARE/.trustee_database.xml` file at the root of the volume. Its trustee information is not available to the primary volume.

To avoid resetting the trustee and rights information, copy the trustee file from the old volume to the new empty volume. Use the local Linux path of the mounted remote NSS volume on the DST server when you copy the file, such as:

```
/var/opt/novell/nclmnt/.Servers/<remote_servername>/<remote_volumename>/._NETWARE/
.trustee_database.xml
```

To copy the trustee file from the remote NSS volume to the primary NSS volume:

1 On the DST server, unmount the primary volume from NCP Server:

1a In a Web browser, open Novell Remote Manager for the DST server, then log in as the root user.

1b Select *Manage NCP Services > Manage Shares* to view a list of active volumes.

1c Select the *Unmount* button next to the volume.

This dismounts the volume from NCP, but it is still mounted by NSS.

2 Log in to the DST server as the `root` user.

3 In a file browser, go to the Linux path for the primary NSS volume, then rename or delete the `/media/nss/`*primary_volumename*`/._NETWARE/.trustee_database.xml` file.

4 Copy the trustee file from the secondary volume location to the primary volume location by entering the following at a terminal console prompt:

```
cp /var/opt/novell/nclmnt/.Servers/<remote_servername>/<remote_volumename>/
._NETWARE/.trustee_database.xml /media/nss/primary_volumename/._NETWARE/
.trustee_database.xml
```

Remember that the remote servername in the secondary path is uppercase.

5 In Novell Remote Manager, select *Manage NCP Services > Manage Shares* to view a list of active volumes.

6 Mount the primary volume for NCP Server by selecting the *Mount* button next to the volume.

7 At the terminal console prompt, enter the following command to synchronize the NSS trustee information that is now on the primary volume with NCP Server:

```
ncpcon nss resync=primary_volumename
```

8 Continue with .

C.5 Creating a Shadow Volume with a Remote Secondary NSS Volume

The following procedure creates a DST shadow volume with two NSS volumes. The primary NSS volume is mounted on the DST server. The secondary volume is a remote NSS volume that is mounted on the DST server via the Novell Client for Linux.

NSS Volumes	Sample Value
Primary NSS volume	VOL1
Secondary path	Use the full Linux path on the DST server to the mount point for the remote NSS volume: `/var/opt/novell/nclmnt/.Servers/SERVER41/DSTVOL1`

1 In a Web browser, open Novell Remote Manager for the DST server, then log in as the `root` user.

2 Select *View File System > Dynamic Storage Technology Options* to view a list of mounted volumes.

3 On the Dynamic Storage Technology page, ensure that the NSS volume that you want to use as the primary volume appears in the *Volume Information* list with a status of *Add Shadow*.

If it is not listed, the NSS volume might be unmounted, or its NCP/NSS bindings might be disabled.

4 Use one of the following methods to go to the Share Information page of the NSS volume that you want to use as the primary storage area.

◆ Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page, then click the *Add Shadow* link next to the volume name of the NSS volume.

For example, click the *Add Shadow* link for VOL1.

 ◆ Select *Manage NCP Services > Manage Shares* to open the Manage Shares page, then click the *Information* (i) icon next to the volume name of the NSS volume.

5 On the volume's Share Information page, scroll down to the *Volume Tasks* area, then click *Add Shadow Volume*.

6 Specify the following information for the secondary storage area for the DST shadow volume, then click *Create* to define the shadow volume.
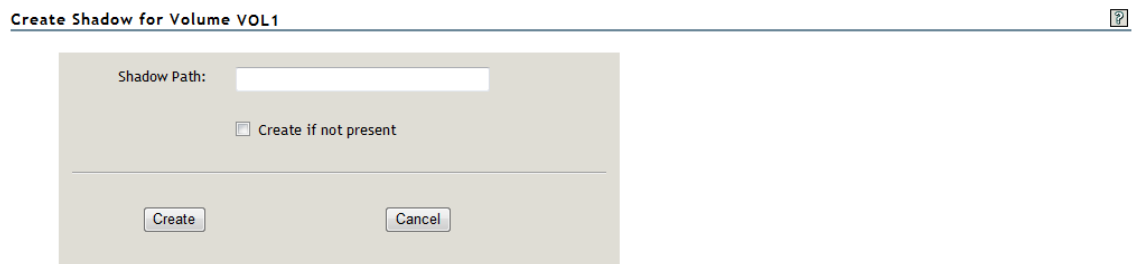
 ◆ **Shadow Path:** Type the full Linux path for the remote NSS volume. The default Linux path where remote volumes are mounted is:

```
/var/opt/novell/nclmnt/.Servers/<remote_servername>/<remote_volumename>
```

For example, type the following in the *Shadow Path* field:

```
/var/opt/novell/nclmnt/.Servers/SERVER41/DSTVOL1
```

 ◆ **Create If Not Present:** For NSS volumes, the volume must already exist. Make sure this option is deselected (not checked) when shadowing NSS volumes.

7 On the volume's Share Information page, ensure that the *File System Shadow Path* information shows the shadow path you specified in Step 3.

You can click the link to verify that the file system is properly mounted and the data on the remote volume is available to DST.

VOL1 Share Information

Information	
Description	**Value**
File system path	/media/nss/VOL1
File system shadow path	/var/opt/novell/nclmnt/.Servers/SERVER41/DSTVOL1
File system type	NSS
NCP volume ID	2
Status	mounted, online, NSS, user quotas, directory quotas, salvageable
Capacity	976.73 MB
Advanced Information	View

Open File Information

Share Management Home

8 Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page, then verify that the *Shadow Status* for the volume is set to *Shadowed* and the *View Log* link is available.

9 Use an NCP client or management tool to configure the file system and trustee rights on the merged view of the DST shadow volume.

10 (Optional) Do one of the following to configure file access for CIFS users:

◆ **Novell CIFS:** Verify that the CIFS share is configured only for the primary NSS volume.

◆ **Novell Samba:** Continue with Chapter 12, "Using ShadowFS to Provide a Merged View for Novell Samba Users," on page 129.

11 Configure and manage policies for the DST shadow volume as described in Chapter 10, "Creating and Managing Policies for Shadow Volumes," on page 101.

C.6 Managing the Remote Secondary Connection

The DST functionality is affected when the Novell Client connection is lost or disconnected.

C.6.1 Novell Client Connection Is Lost

When the Novell Client connection between the DST server and the remote server is lost and an automatic restore of the connection happens, the DST shadow volume relationship automatically resumes. User sessions with remote files might be delayed or interrupted, but the files and folders in the remote volume are automatically made available again.

C.6.2 Novell Client Connection Is Disconnected

Each time the DST server is rebooted or the remote server is rebooted, the Novell Client connection to the remote server is disconnected. This can also happen if you intentionally log out of your Novell Client session with the remote server.

You should not allow users to access the primary volume or run policies until the secondary volume is mounted.

To resume the DST shadow volume relationship:

1 Use the `nwlogin` command on the DST server to reconnect to the remote server as described in

You can do this manually for each remote server, or you can put the `nwlogin` commands in the startup script so that they happen automatically on reboot.

IMPORTANT: It is a security issue to include the password in a script.

The `nwlogin` command syntax is:

```
nwlogin --server <remote_server_IP_address> --tree <tree_name> --user dstusername --context <dstusername_context> --password <dstuser_password>
```

For example:

```
nwlogin -s 10.10.10.41 -t MYCOMPANY_TREE -u dstuser -c users.boston.novell -p dstpassword
```

For more information about the Novell Client command options, see the `nwlogin(1)` man page, or see "Novell Client for Linux Man Pages" in the *Novell Client 2.0 SP3 for Linux Administration Guide*.

C.7 Removing a Shadow Relationship with a Remote NSS Volume

You can use the remote secondary volume as an independent volume again by removing the relationship with the remote secondary volume and disconnecting the Novell Client connection to the remote server. Because none of the file access rights that were set on the merged view of the shadow volume were pushed to the secondary NSS volume, you must set the trustees and file system rights again for the data on the remote volume.

1 Remove the shadow volume relationship between the two volumes.

  1a In Novell Remote Manager for Linux, log in as the `root` user.

  1b Select *Manage NCP Services > Manage Shares* to go to the NCP Shares page.

  1c Locate the primary NSS volume in the *Active Shares* list, then click the *Unmount* button next to the share name.
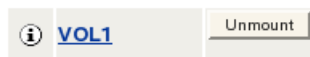
  1d On the Manage Shares page, click the *Information* (i) icon next to the volume name of the NSS volume to access the *Remove Shadow Action Options*.

  1e On the volume's Share Information page under *Volume Tasks > Remove Shadow Action Options*, click *Remove Shadow*.

  After the shadow volume is removed, the page refreshes to report a successful removal.

1f Select *Share Management* to go to the NCP Shares page, locate the volume that was the primary volume in the *Active Shares* list, then click the *Mount* button next to it.

1g Verify that the shadow volume was removed by using one of the following methods:

◆ Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page. The former primary volume now has an *Add Shadow* link next to it instead of a *Shadowed* link.

◆ Select *Manage NCP Services > Manage Shares*, then click the *Information* icon next to the former primary volume's name. The *File System Shadow Path* field displays n/a (not applicable).

2 Use one of the following methods to remove file access to the secondary volume:

◆ **All NSS volumes on all of the remote servers:** On the DST server, log out of the Novell Client sessions for all remote servers.

1. Log in to the DST server as the `root` user, then open a terminal console.

2. At the console prompt, enter

   `nwlogout --tree <tree_name>`

◆ **All NSS volumes on the remote server:** On the DST server, log out of the Novell Client session for a specified remote server.

1. Log in to the DST server as the `root` user, then open a terminal console.

2. At the console prompt, enter

   `nwlogout --server <remote_servername_or_ip_address>`

◆ **Individual NSS volume on the remote server:** Remove the file system access rights on the remote volume for the user name you used to log in to the remote server.

3 For the remote NSS volume, remove any special file system access rights that you gave the user name that you used for the remote login.

4 Set up file access for users on the independent remote NSS volume.

D Technology Preview: Using DST Shadow Volumes with Remote Secondary NSS Volumes and Novell Cluster Services

This section describes how to configure and manage Novell Dynamic Storage Technology (DST) shadow volumes with remote secondary Novell Storage Services (NSS) volumes in a Novell Cluster Services cluster.

IMPORTANT: The remote secondary capability for DST shadow volumes is presented as a technology preview for Novell Open Enterprise Server (OES) 2 SP3 for Linux. It is not recommended for a production environment.

D.1 Planning for Using Shadow Volumes with Remote Secondary NSS Volumes in a Cluster

Before you begin, ensure that you understand the requirements and guidelines in the following sections:

D.2 Requirements for Using Remote NSS Secondary Volumes in DST Shadow Volume Cluster Resources

In addition to the requirements in Section 13.1, "Planning for DST in a Cluster," on page 139, consider the requirements in this section when setting up DST shadow volumes with remote secondary NSS volumes in a Novell Cluster Services cluster environment.

D.2.1 Novell Open Enterprise Server 2 Linux

Each node in the cluster that hosts a DST shadow volume with a remote secondary NSS volume must be running OES 2 SP3 Linux (or later). For simplicity, these nodes are referred to as DST nodes in this section.

D.2.2 Novell Client 2.3 for Linux

Create a Novell Client for Linux mount point for the remote server on each DST node in the cluster that is in the *Preferred Nodes* list of the DST shadow volume resource.

The remote secondary NSS volume should be mounted on a DST node before you online the DST shadow volume resource on that node.

D.2.3 Primary NSS Volume

The primary pool must be cluster-enabled, and its resource runs on DST nodes in the cluster.

D.2.4 Remote NSS Volume

The remote secondary NSS volume can be in a pool that is unshared or shared. It does not matter whether DST is running on the remote server.

If the remote secondary NSS volume is unshared, it can reside on any server in the same Novell eDirectory tree and partition, including on a node in the cluster.

If the secondary volume is shared and is in the same cluster, you can use one of the methods to manage the secondary volume on the same node that are described in Chapter 13, "Configuring DST Shadow Volume Pairs with Novell Cluster Services," on page 139. You can use the remote setup if you want to manage the shared primary and shared secondary volumes on different nodes in the cluster.

D.3 Cluster Setup with Manual Login to the Remote Server

The cluster setup in this section describes how to set up the Novell Client connection to the remote server and define the DST shadow volume for each DST node. The remote volume's mount point is always active on each of the DST nodes. When the primary pool cluster resource is active on a DST

node, DST activates the shadow volume relationship that you defined on that node. When the pool cluster resource is offline or migrated to another server, the DST shadow volume is deactive for that node.

Whenever a DST node is rebooted, the Novell Client connection is broken. You can log in manually to each remote server, or you can put the `nwlogin` commands in the server startup script so that they happen automatically on reboot.

If the remote server is rebooted, you must manually log in again to the remote server from each DST node in the cluster.

To set up this DST cluster solution:

1 In iManager, create a dstuser identity and assign the user name as a trustee with the Supervisor right for the remote NSS volume.

2 If the primary NSS pool cluster resource and volume do not already exist, create a pool cluster resource on the cluster, create an NSS volume on it to use as the primary volume, then configure the cluster resource *Preferred Nodes* list and the load, unload, and monitoring scripts. Ensure that you specify only DST nodes in the *Preferred Nodes* list.

For information, see *Configuring Cluster Resources for Shared NSS Pools and Volumes* in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

3 For each DST node in the cluster, log in to the remote server and set up the shadow volume relationship:

3a Log in to a DST node as the `root` user, then open a terminal console.

3b Cluster migrate the primary pool cluster resource to the DST node by entering

```
cluster migrate resource_name node_name
```

Replace *resource_name* with the name of the primary pool cluster resource. Replace *node_name* with the hostname of the DST node.

3c Use the Novell Client for Linux to log in to the remote server and mount the remote NSS volume. At the console prompt, enter

```
nwlogin --server remote_servername_or_IP_address --tree tree_name
--user dst_username --context username_context --password dst_password
```

For example, enter

```
nwlogin --server 10.10.10.41 --tree MYCOMPANY_TREE
--user dstuser --context users.context --password novell
```

If the server hostname is `server41` and the remote volume is `SHVOL1`, the mount path is:

```
/var/opt/novell/nclmnt/.Servers/SERVER41/SHVOL1
```

3d In a Web browser, open Novell Remote Manager on the DST node, then log in as the `root` user.

You must be logged in as the `root` user in order to have the file system rights necessary to access the Linux path for the mount point of the remote NSS volume.

3e In Novell Remote Manager, select *View File Systems > Dynamic Storage Technology Options*, click *Add Shadow* next to the primary NSS volume, then configure the shadow volume.

- **Primary volume:** The shared NSS volume.
- **Secondary path:** The Linux path of the mount point for the remote secondary NSS volume.

```
/var/opt/novell/nclmnt/.Servers/<servername>/<volumename>
```

The path is case sensitive.

3f Repeat Step 3a to Step 3e for each DST node in the cluster.

4 Use the normal load, unload, and monitoring scripts for managing the primary NSS pool cluster resource.

D.4 Cluster Setup with a Scripted Login to the Remote Server

An alternative to the method used in Section D.3, "Cluster Setup with Manual Login to the Remote Server," on page 212 is to add the `nwlogin` command to the primary pool cluster resource load script and to add the `nwlogout` command to its unload script.

IMPORTANT: It is a security concern to add the user password to the load script because it is stored in clear text.

You configure the shadow volume in the cluster load script so that it defines the NCP volume as the resource loads. The clustered shadow volume is not permanently defined in the /etc/opt/novell/ncpserv.conf files of each node. It is added to the server's /etc/opt/novell/ncpserv.conf file when the pool cluster resource fails over to that node. You use the `ncpcon mount volumename=volID,SHADOWPATH=shadowpath` command in the load script to mount the volume. For information, see Section A.3.4, "Scenario 4: Primary NSS and Shadow Non-NSS (Supported for the Remote Secondary NSS Volume in the Technology Preview)," on page 189.

If the remote server is rebooted, you must manually log in again from the active DST node to the remote server.

To set up this DST cluster solution:

1 In iManager, create a `dstuser` identity and assign the user name as an NSS file system trustee with the Supervisor right for the remote NSS volume.

2 If the primary NSS pool cluster resource and volume do not already exist, create a pool cluster resource on the cluster, create an NSS volume on it to use as the primary volume, then configure the cluster resource *Preferred Nodes* list and the load, unload, and monitoring scripts. Ensure that you specify only DST nodes in the *Preferred Nodes* list.

For information, see *Configuring Cluster Resources for Shared NSS Pools and Volumes* in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

3 Modify the load script for the primary pool cluster resource:

3a In iManager, select *Clusters > Cluster Options*, then browse to select the cluster.

3b In the list of Cluster objects, click the *Name* link for the primary pool cluster resource to open its Properties page, then click the *Scripts* tab.

3c On the *Load Script* page, add the `nwlogin` command and the `ncpcon mount volumename=volID,SHADOWPATH=shadowpath` command to the load script.

```
#Log in to the remote server
exit_on_error /opt/novell/ncl/bin/nwlogin --server 10.10.10.41 --tree
MYCOMPANY_TREE --user dstuser --context users.context --password novell

ncpcon mount volumename=volID,SHADOWPATH=shadowpath
```

Comment out the default mount command:

```
#exit_on_error ncpcon mount VOL1=254
```

The script is not activated until the pool cluster resource is taken offline and then brought online.

The following is a sample load script:

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

#Log in to the remote server
exit_on_error /opt/novell/ncl/bin/nwlogin --server 10.10.10.41 --tree
MYCOMPANY_TREE --user dstuser --context users.context --password novell

sleep 10
exit_on_error nss /poolact=POOL1
#exit_on_error ncpcon mount VOL1=254

exit on error ncpcon mount VOL1=254,SHADOWPATH=/var/opt/novell/nclmnt/
.Servers/SERVER41/SHVOL1

exit_on_error add_secondary_ipaddress 10.10.10.44
exit_on_error ncpcon bind --ncpservername=CLUS1_POOL1_SERVER
--ipaddress=10.10.10.44

#Uncomment this command if Novell CIFS is used
#exit_on_error novcifs --add --
vserver=.cn=CLUS1_POOL1_SERVER.ou=servers.o=novell.t=MYCOMPANY_TREE.
--ip-addr=10.10.10.44

exit 0
```

3d Click *Apply* to save your changes.

4 Modify the unload script for the primary pool cluster resource:

4a On the *Properties* > *Script* page, click *Unload Script*.

4b Add the `nwlogout` command to the unload script.

```
ignore error nwlogout --server remote_servername_or_IP_address
```

The script is not activated until the pool cluster resource is taken offline and then brought online.

The following is a sample unload script:

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs

ignore_error ncpcon unbind --ncpservername=CLUS1_POOL1_SERVER --
ipaddress=10.10.10.44

ignore_error del_secondary_ipaddress 10.10.10.44
ignore_error nss /pooldeact=POOL1

ignore error nwlogout --tree MYCOMPANY_TREE

exit 0
```

4c Click *Apply* to save your changes.

5 Modify the monitoring script for the primary pool cluster resource:

5a On the *Properties* > *Script* page, click *Monitoring Script*.

5b Verify that there is no entry for ncpcon to monitor the remote NSS volume.

The remote secondary volume is mounted as a Linux POSIX volume, and it is not accessible to NCP.

5c Click *OK* to save your changes.

6 Activate the script changes by offlining then onlining the primary pool cluster resource:

    6a Click *Clusters > Cluster Manager*.

    6b Select the check box next to the primary pool cluster resource, then click *Offline*.

    6c Select the check box primary pool cluster resource, then click *Online*.

D.5 Removing the Shadow Volume Relationship in a Cluster Resource with a Remote Secondary

1 Log in to the master node of the cluster as the `root` user, then open a terminal console.

2 If the cluster pool resource for the shadow volume is not running on the master node, cluster migrate it to the master node. At the console prompt, enter

```
cluster migrate resource_name masternode_name
```

3 Offline the cluster pool resource that is managing the shadow volume.

```
cluster offline resource_name
```

This unloads the cluster resource and deactivates the cluster pool and the shadow volume so that the cluster is not controlling them.

4 Manually activate the shared pool and mount the primary volume.

    4a At the console prompt of the master node, enter

        `nssmu`

    4b In the NSSMU menu, select *Pools*, then press Enter.

    4c Select the primary pool, then press F7 to activate it.

    4d Press Esc to return to the NSSMU menu, select *Volumes*, then press Enter.

    4e Select the primary volume, then press F7 to mount it.

    4f Press Esc twice to exit NSSMU.

5 Remove the shadow volume relationship between the two volumes:

    5a In Novell Remote Manager for Linux, log in as the `root` user. to the master node.

    5b Select *Manage NCP Services > Manage Shares* to go to the NCP Shares page.

    5c On the NCP Shares page, locate the primary NSS volume in the *Active Shares* list, then click the *Unmount* button next to the share name.

    5d On the Manage Shares page, click the *Information* (i) icon next to the volume name of the NSS volume to access the *Remove Shadow Action Options*.

5e On the volume's Share Information page under *Volume Tasks > Remove Shadow Action Options*, click *Remove Shadow*.
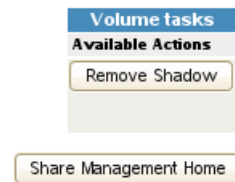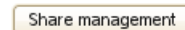
VOL1 Share Information

> **Volume tasks**
> **Available Actions**
>
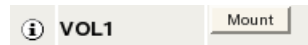> Remove Shadow

Share Management Home

After the shadow volume is removed, the page refreshes to report a successful removal.

Remove Shadow from Volume VOL1

Volume task has completed successfully

Share management

5f Select *Share Management* to go to the NCP Shares page, locate the volume that was the primary volume in the *Active Shares* list, then click the *Mount* button next to it.

ⓘ **VOL1**   Mount

5g Verify that the shadow volume was removed by using one of the following methods:

◆ Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page. The former primary volume now has an *Add Shadow* link next to it instead of a *Shadowed* link.

Volume Information		
Volume Name	**Shadow Status**	
ⓘ VOL1	Add Shadow	Inventory
ⓘ _ADMIN	No Shadow	Inventory
ⓘ SYS	Add Shadow	Inventory

◆ Select *Manage NCP Services > Manage Shares*, then click the *Information* icon next to the former primary volume name.

The *File System Shadow Path* field displays that it is not applicable (n/a).

File system path	/media/nss/VOL1
File system shadow path	n/a

6 In NSSMU, manually deactivate the primary pool and its volume.

This automatically dismounts the shared volume, which allows the cluster resource to be managed by the cluster resource again.

6a At the console prompt of the master node, enter

`nssmu`

6b In the NSSMU menu, select *Pools*, then press Enter.

6c Select the primary pool, then press F7 to deactivate it.

6d Press Esc twice to exit NSSMU.

7 Modify the load script of the cluster pool resource that was managing the clustered shadow volume pair:

7a In iManager, select *Clusters*, then select *Cluster Manager*.

7b Click the *Object* browser, then locate and select the cluster server node to view a list of cluster resources.

7c On the Cluster Manager page, click the name link of the primary cluster resource to view its Cluster Pool Properties page, then click the *Scripts* tab.

7d On the *Scripts > Load Script* page, comment out or remove the following commands:

```
#Log in to the remote server
exit_on_error /opt/novell/ncl/bin/nwlogin --server 10.10.10.41 --tree
MYCOMPANY_TREE --user dstuser --context users.context --password novell

ncpcon mount volumename=volID,SHADOWPATH=shadowpath
```

7e On the *Scripts > Load Script* page, uncomment the mount command for the primary pool's volume that you commented out when you set up the clustered shadow volume. For example:

```
exit_on_error ncpcon mount VOL1=254
```

7f Click *Apply* to save your changes.

The changes do not take effect until the cluster resource is taken offline and brought online.

8 Modify the unload script of the cluster pool resource that was managing the clustered shadow volume pair:

8a On the *Scripts > Load Script* page, click the *Unload Script* link.

8b On the *Scripts > Unload Script* page, comment out or remove the nwlogout command for the remote secondary server:

```
#ignore error nwlogout --server remote_servername_or_IP_address
```

8c Click *Apply* to save your changes.

The changes do not take effect until the cluster resource is taken offline and brought online.

9 Online the cluster pool resource for the primary pool:

9a Select *Clusters*, then select *Cluster Manager* to view the list of cluster resources.

9b Select the check box next to the primary cluster pool resource, then click *Online*.

9c Select the cluster node where you want the resource to load (such as server38), then click *OK*.

10 Verify that the cluster resource is running by going to the *Clusters > Cluster Manager* page.

11 Use one of the following methods to remove file access to the secondary volume:

- **All NSS volumes on all of the remote servers:** On the DST server, log out of the Novell Client sessions for all remote servers.

   1. Log in to the DST server as the root user, then open a terminal console.
   2. At the console prompt, enter

      ```
      nwlogout --tree <tree_name>
      ```

- **All NSS volumes on the remote server:** On the DST server, log out of the Novell Client session for a specified remote server.

   1. Log in to the DST server as the root user, then open a terminal console.

2. At the console prompt, enter

```
nwlogout --server <remote_servername_or_ip_address>
```

   - **Individual NSS volume on the remote server:** Remove the file system access rights on the remote volume for the user name you used to log in to the remote server.

12 For the remote NSS volume, remove any special file system access rights that you gave the user name that you used for the remote login.

13 For the remote NSS volume, set up file access for users.

E Documentation Updates

This section contains information about documentation content changes made to the *OES 2: Dynamic Storage Technology Administration Guide* since the initial release of Novell Open Enterprise Server 2. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

This document was updated on the following dates:

E.1 September 6, 2013

Updates were made to the following section. The changes are explained below.

E.1.1 Planning for DST Shadow Volumes and Policies

Location	Change
Section 5.11, "Using Backup Utilities with DST Shadow Volumes," on page 55	For information about using the NSS /ListXattrNWmetadata option and the security considerations involved, see "ListXattrNWmetadata Option" in the *OES 2 SP3: NSS File System Administration Guide for Linux*.
	Backup utilities might also work against the ShadowFS merged view. However, because the ShadowFS merged view is a Linux mount point and is not seen by the backup software as an NSS volume, the file system rights and attributes are not preserved. It is not recommended or supported to back up NSS files from this Linux mount point.

E.2 June 25, 2013

Updates were made to the following section. The changes are explained below.

◆ Section E.2.1, "Configuring DST Shadow Volume Pairs with Novell Cluster Services," on page 222

E.2.1 Configuring DST Shadow Volume Pairs with Novell Cluster Services

Location	Change
Chapter 13, "Configuring DST Shadow Volume Pairs with Novell Cluster Services," on page 139	Sections and steps to manually set the EXCLUDE_VOLUME line in the /etc/opt/novell/ncp2nss.conf file were removed.
Section 13.2.4, "NCP2NSS Bindings for the Secondary Volume," on page 143	When you bring the resource online on a node for the first time, an EXCLUDE_VOLUME line is automatically added to the /etc/opt/novell/ncp2nss.conf file as well as the temporary exclusion table in cache on that node.

E.3 May 2013 Scheduled Maintenance

Updates were made the following sections. The change is explained below.

◆ Section E.3.1, "Planning for DST Shadow Volumes and Policies," on page 223
◆ Section E.3.2, "What's New or Changed for DST," on page 223

E.3.1 Planning for DST Shadow Volumes and Policies

Location	Change
"Using Backup Utilities with DST Shadow Volumes" on page 55	If you back up the NSS volume by using the NSS Extended Attributes (XAttr) settings to preserve the NetWare metadata (netware.metadata) for file system rights and attributes, this information can be restored only directly to an NSS volume.
	Backup utilities might also work against the ShadowFS merged view. However, because the ShadowFS merged view is a Linux mount point and is not seen by the backup software as an NSS volume, it is not recommended or supported to back up NSS files from this Linux mount point.

E.3.2 What's New or Changed for DST

Location	Change
"What's New (May 2013 Patches)" on page 25	This section is new.

E.4 April 2013 Scheduled Maintenance

Updates were made the following section. The change is explained below.

E.4.1 What's New

Location	Change
"What's New (April 2013 Patches)" on page 25	This section is new.

E.5 January 2013 Scheduled Maintenance

Updates were made to the following sections. The changes are explained below.

E.5.1 Configuring DST Shadow Volumes with Novell Cluster Services

This section has been updated for clarity.

Location	Change
"Using the Clusters Plug-in for iManager 2.7.5 or Later" on page 146	This section is new.

E.5.2 What's New or Changed for DST

Location	Change
"What's New (January 2013 Patches)" on page 26	This section is new.

E.6 August 2012 Scheduled Maintenance

Updates were made to the following sections. The changes are explained below.

- Section E.6.1, "Creating and Managing Policies for Shadow Volumes," on page 224
- Section E.6.2, "What's New or Changed for DST," on page 224

E.6.1 Creating and Managing Policies for Shadow Volumes

Location	Change
"Subdirectory Restrictions" on page 105	A preceding forward slash (/) is required for subdirectory path entries. Specify the path relative to the root of the volume.

E.6.2 What's New or Changed for DST

Location	Change
"What's New (July 2012 Patches)" on page 26	This section is new.

E.7 June 30, 2012

Updates were made to the following sections. The changes are explained below.

- Section E.7.1, "Commands and Utilities for Dynamic Storage Technology," on page 225
- Section E.7.2, "Configuring DST Shadow Volumes with Novell Cluster Services," on page 225

E.7.1 Commands and Utilities for Dynamic Storage Technology

Location	Change
"create shadow_volume <primary_volumename> <shadow_path> / ID=<volume_id>" on page 184	Use this command only for non-clustered shadow volumes. The /ClusterResource option is deprecated. For cluster shadow volumes, see Section A.3, "DST Commands for NCPCON for Use with Novell Cluster Services for Linux Clusters," on page 188.
"remove shadow_volume [/l] [/i] [/f] <primary_volumename>" on page 185	Use this command only for non-clustered shadow volumes. Added definitions for the /i and /f options.

E.7.2 Configuring DST Shadow Volumes with Novell Cluster Services

Location	Change
"Merged View Access with NCP" on page 140	This section is new.
"Merged View Access with Novell CIFS" on page 141	The CIFS status command is added to the monitor script for the primary pool cluster resource. You can modify this to use the CIFS monitor command.

E.8 May 2012 Scheduled Maintenance

Updates were made to the following sections. The changes are explained below.

E.8.1 Installing and Configuring ShadowFS for Novell Samba Users

Location	Change
"Enabling or Disabling ShadowFS" on page 135	Updated to reflect the renamed *Load ShadowFS* option.

E.8.2 What's New or Changed for DST

Location	Change
"What's New (May 2012 Patches)" on page 27	This section is new.

E.9   April 12, 2012

The document format was updated to reflect newly revised corporate standards.

Updates were made to the following section. The changes are explained below.

◆ Section E.9.1, "Creating and Managing Policies for Shadow Volumes," on page 226

E.9.1   Creating and Managing Policies for Shadow Volumes

Location	Change
"Search Pattern" on page 106	You can specify file names with spaces in them.

E.10   July 21, 2011

Updates were made to the following section. The changes are explained below.

◆ Section E.10.1, "Configuring DST Shadow Volumes with Novell Cluster Services," on page 226
◆ Section E.10.2, "Creating and Managing DST Volumes for NSS Volumes," on page 227
◆ Section E.10.3, "Creating and Managing Policies for Shadow Volumes," on page 227

E.10.1   Configuring DST Shadow Volumes with Novell Cluster Services

Location	Change
"Configuring the DST Pool Cluster Resource with Two Cluster-Enabled Pools" on page 147	Information was added to clarify the load and unload script setup.
"Configuring the DST Pool Cluster Resource with a Cluster-Enabled Pool and a Shared Pool" on page 156	

E.10.2 Creating and Managing DST Volumes for NSS Volumes

Location	Change
"Removing the Shadow Relationship for a Non-Clustered DST Shadow Volume" on page 96	A non-functioning option on the Remove Shadow page has been removed.
"Removing the Shadow Relationship for a Clustered DST Volume Pair" on page 168	
"Removing a Shadow Relationship with a Remote NSS Volume" on page 209	
"Removing the Shadow Volume Relationship in a Cluster Resource with a Remote Secondary" on page 216	

E.10.3 Creating and Managing Policies for Shadow Volumes

Location	Change
"Viewing Information about the Files Moved During a Policy Run" on page 112	This section is new.

E.11 June 2011

Updates were made to the following sections. The changes are explained below.

E.11.1 Configuring DST Global Policies

Location	Change
"Shift Modified Shadow Files" on page 67	If you disable the Shift Modified Shadow Files parameter, it is still possible for modified files to reappear on the primary location. See this section for details.

E.11.2 Troubleshooting

Location	Change
"Files that initially reside only on the secondary volume can end up as directories on the primary volume" on page 178	This section is new.

E.12 April 2011

Updates were made to the following section. The changes are explained below.

- Section E.12.1, "Commands and Utilities for DST," on page 228

E.12.1 Commands and Utilities for DST

Location	Change
Section A.2, "DST Commands for NCPCON," on page 184	The SHIFT command works only at the command line, and not in ncpcon interactive mode.Enter the command as the root user at a terminal console prompt.

E.13 January 31, 2010

Updates were made to the following sections. The changes are explained below.

- Section E.13.1, "Configuring DST Shadow Volumes with Novell Cluster Services for Linux," on page 228

E.13.1 Configuring DST Shadow Volumes with Novell Cluster Services for Linux

Location	Change
Section 13.2.9, "Additional Volumes in the Primary Pool," on page 145	This section is new.

E.14 December 2010 (OES 2 SP3)

The guide was revised for clarity. In addition, updates were made to the following sections. The changes are explained below.

E.14.1 Configuring DST Shadow Volumes with Novell Cluster Services for Linux

Location	Change
"Merged View Access with Novell CIFS" on page 141	This section is new.
Section 13.5, "Configuring the DST Pool Cluster Resource with Two Cluster-Enabled Pools," on page 147	This section was modified to add information about Novell CIFS.
Section 13.6, "Configuring the DST Pool Cluster Resource with a Cluster-Enabled Pool and a Shared Pool," on page 156	This section was modified to add information about Novell CIFS.

E.14.2 Installing and Configuring Dynamic Storage Technology

Location	Change
Section 3.1.5, "Novell CIFS," on page 32	This section is new.

E.14.3 Managing DST Shadow Volumes for NSS Volumes

Location	Change
Chapter C, "Technology Preview: Creating and Managing DST Shadow Volumes with Remote Secondary NSS Volumes," on page 199	This section is new.
Chapter D, "Technology Preview: Using DST Shadow Volumes with Remote Secondary NSS Volumes and Novell Cluster Services," on page 211	This section is new.

E.14.4 Managing Policies for Shadow Volumes

Location	Change
Section 10.1.12, "Stop," on page 108	This section is new.
Section 10.7, "Stopping a Running Policy," on page 113	This section is new.
Section 10.8, "Deleting a Shadow Volume Policy," on page 114	The *Delete* option now prompts you to confirm the deletion.

E.14.5 Technology Preview: Creating and Managing DST Shadow Volumes with Remote Secondary NSS Volumes

This section is new.

E.14.6 Technology Preview: Using DST Shadow Volumes with Remote Secondary NSS Volumes and Novell Cluster Services

This section is new.

E.14.7 What's New or Changed for DST

Location	Change
Section 2.6, "What's New for OES 2 SP3," on page 27	This section is new.

E.15 June 16, 2010

Updates were made to the following sections. The changes are explained below.

- Section E.15.1, "Configuring DST Shadow Volumes with Novell Cluster Services for Linux," on page 231
- Section E.15.2, "Installing and Configuring Dynamic Storage Technology," on page 231
- Section E.15.3, "Managing Shadow Volumes for NSS Volumes," on page 231
- Section E.15.4, "Troubleshooting Dynamic Storage Technology," on page 232

E.15.1 Configuring DST Shadow Volumes with Novell Cluster Services for Linux

Location	Change
Section 13.2, "Planning for DST Shadow Volume Pairs and Policies in a Cluster," on page 142	This section was revised for clarity.
Section 13.5.3, "Adding Commands for the Secondary Clustered Pool and Volume to the Primary Pool Cluster Resource," on page 151	This section is new.

E.15.2 Installing and Configuring Dynamic Storage Technology

Location	Change
Section 3.2.2, "Installing on an Existing OES 2 Linux Server," on page 36	This section was revised for clarity.

E.15.3 Managing Shadow Volumes for NSS Volumes

Location	Change
Step 8 in Section 9.5, "Copying a Trustee Database to the Primary NSS Volume," on page 87	The command should be: `ncpcon nss resync=`*`primary_volumename`*
Section 9.11.2, "Planning Your Restore Solution," on page 93	Added information about restoring data where the backup was made with Extended Attributes (XAttr).

E.15.4 Troubleshooting Dynamic Storage Technology

Location	Change
Section 14.3, "Users cannot see some files and directories," on page 178	Added information about NCP Server performance issues that can also result in some files appearing to be missing. See TID 7004888.

E.16 February 19, 2010

Updates were made to the following sections. The changes are explained below.

- Section E.16.1, "Commands and Utilities for Dynamic Storage Technology," on page 232
- Section E.16.2, "Configuring DST Shadow Volumes with Novell Cluster Services for Linux," on page 232

E.16.1 Commands and Utilities for Dynamic Storage Technology

Location	Change
Section A.2, "DST Commands for NCPCON," on page 184	When quotation marks are used in a command (such as surrounding a file name), you must escape each quotation mark character (") with a backslash (\), such as \" when using the command at the command line or in a script. Added examples of using quotation marks in the interactive, command line, and scripting modes.

E.16.2 Configuring DST Shadow Volumes with Novell Cluster Services for Linux

Location	Change
Section 13.2.6, "Load Order in the Load Script," on page 144	**IMPORTANT:** If wait times are added to the load script or unload script, ensure that you increase the script timeout settings accordingly. Otherwise, the script might time out while you are waiting for the action.
Section 13.4, "Preparing the Nodes to Support DST in a Cluster Environment," on page 146	**IMPORTANT:** The Shadow File System uses FUSE (File Systems in Userspace) to create a local mount point that presents a merged file system view of a shadow volume for SMB/CIFS users. If your SMB/CIFS users do not need to access a volume that is shadowed, or if there are no SMB/CIFS users for the volume, then it is not necessary to load FUSE or to set up FUSE in the load and unload scripts.
Section 13.5.3, "Adding Commands for the Secondary Clustered Pool and Volume to the Primary Pool Cluster Resource," on page 151	The procedure was modified for clarity and accuracy.

Location	Change
Section 13.7.1, "Sample Load Script for a DST Shadow Volume," on page 167	The load script was modified for clarity and accuracy.
Section 13.7.2, "Sample Unload Script," on page 167	The unload script was modified for clarity and accuracy.

E.17 November 9, 2009 (OES 2 SP2)

This guide was updated to the Novell documentation standards for OES 2 SP2.

E.17.1 Commands and Utilities for Dynamic Storage Technology

Location	Change
Section A.2, "DST Commands for NCPCON," on page 184	Corrected the following example for the `ncpcon shadow` command to add the time option: `shadow VOL1 operation=ms time=m range=j` Moves all files on the primary storage area that have not been modified in more than two years from the primary storage area to the secondary storage area for the shadow volume `VOL1`.

E.17.2 Managing Policies for Shadow Volumes

Location	Change
Section 10.1.10, "Subdirectory Restrictions," on page 105	Modified the example in Table 9-3 to show the paths as `project_abc/videos` and `project_abc/contracts` so that they are relative to the root of the DST volume. Beginning in OES 2 SP2, you can specify multiple paths to be either included or excluded when the policy runs.
"Search Pattern" on page 106	Beginning in OES 2 SP2, you can specify multiple extensions in the search pattern. Separate multiple entries with a comma and no spaces.

E.17.3 What's New or Changed for DST

Location	Change
Section 2.7, "What's New for OES 2 SP2," on page 28	This section is new.

E.18 March 3, 2009

Updates were made to the following sections. The changes are explained below.

- Section E.18.1, "Configuring DST Shadow Volumes with Novell Cluster Services for Linux," on page 234

E.18.1 Configuring DST Shadow Volumes with Novell Cluster Services for Linux

Location	Change
Section 13.5.3, "Adding Commands for the Secondary Clustered Pool and Volume to the Primary Pool Cluster Resource," on page 151	If you are loading other items like Samba, rsync, and so on, and you are relying on the ShadowFS volume to provide the merged file tree view, you might need to add additional wait time for the ShadowFS file system to mount.
Section 13.5.3, "Adding Commands for the Secondary Clustered Pool and Volume to the Primary Pool Cluster Resource," on page 151	If you are using `ShadowFS` to provide a merged file tree view to Samba users, you must unmount the FUSE-mounted file systems that are displayed in the `/media/ShadowFS/VOLUME` directory.

E.19 February 13, 2009

Updates were made to the following sections. The changes are explained below.

- Section E.19.1, "Configuring DST Shadow Volumes with Novell Cluster Services for Linux," on page 235
- Section E.19.2, "Installing and Configuring Dynamic Storage Technology," on page 235
- Section E.19.3, "Managing DST Shadow Volumes for NSS Volumes," on page 235

E.19.1 Configuring DST Shadow Volumes with Novell Cluster Services for Linux

Location	Change

Section 13.5.3, "Adding Commands for the Secondary Clustered Pool and Volume to the Primary Pool Cluster Resource," on page 151	If you are using ShadowFS to provide the merged file tree view for SMB/CIFS users, you must allow time in the load script after mounting the shadow volume to allow ShadowFS to become active before continuing. Add a `sleep 10` command after mount command.
	
	For example:
	
	`exit_on_error ncpcon mount VOL1=254,shadowvolume=ARCVOL1`
	`sleep 10`

Section 13.9, "Removing the Shadow Relationship for a Clustered DST Volume Pair," on page 168	**IMPORTANT:** In the OES 2 SP1 release for DST, if you disable the *Check to leave existing files on the shadow volume* option, the shadow volume is not removed and an error occurs. DST does not remove the shadow relationship until you enable the option to keep data where it is.

E.19.2 Installing and Configuring Dynamic Storage Technology

Location	Change
Section 7.2, "Restarting the Novell eDirectory (ndsd) Daemon," on page 63	**IMPORTANT:** Restarting or stopping ndsd automatically disconnects all user connections and does not warn users before the connection is broken. Users can reconnect to the server after the service starts.

E.19.3 Managing DST Shadow Volumes for NSS Volumes

Location	Change
Section 9.12, "Removing the Shadow Relationship for a Non-Clustered DST Shadow Volume," on page 96	**IMPORTANT:** In the OES 2 SP1 release for DST, if you disable the *Check to leave existing files on the shadow volume* option, the shadow volume is not removed and an error occurs. DST does not remove the shadow relationship until you enable the option to keep data where it is.

E.20 January 13, 2009

Updates were made to the following sections. The changes are explained below.

E.20.1 Management Tools for Dynamic Storage Technology

Location	Change
Section 6.1.4, "Quick Reference for NCP Server Options," on page 60	Clarified that the mount or unmount options apply to the primary volume of the DST shadow volume pair.

E.20.2 Managing DST Shadow Volumes for NSS Volumes

Location	Change
Section 9.5, "Copying a Trustee Database to the Primary NSS Volume," on page 87	In Step 5 on page 87, you must rename or delete the `/media/nss/primary_volumename/._NETWARE/.trustee_database.xml file` on the primary volume before you can copy the `.trustee_database.xml` file from the secondary volume to that location.

E.21 December 2008 (OES 2 SP1)

Updates were made to the following sections. The changes are explained below.

- Section E.21.1, "Configuring DST Shadow Volumes with Novell Cluster Services for Linux," on page 236
- Section E.21.2, "Installing and Configuring Dynamic Storage Technology," on page 237
- Section E.21.3, "Installing and Configuring Shadow File System (ShadowFS) for SMB/CIFS Users," on page 237
- Section E.21.4, "Managing DST Shadow Volumes for NSS Volumes," on page 237
- Section E.21.5, "Planning Your Dynamic Storage Technology Solution," on page 237
- Section E.21.6, "Using DST to Migrate Data on Demand from NetWare to OES 2 Linux," on page 238

E.21.1 Configuring DST Shadow Volumes with Novell Cluster Services for Linux

Location	Change
Section 13.9, "Removing the Shadow Relationship for a Clustered DST Volume Pair," on page 168	This section is new.

E.21.2 Installing and Configuring Dynamic Storage Technology

Location	Change
"Broadcasting Conflict Messages to NCP Users" on page 72	The broadcast message capability is called Send Message in the Novell Client. In OES 2 SP1, the Send Message feature is available in the Novell Client 4.91 SP4 for Windows XP/2003, the Novell Client 1.0 SP1 for Vista, and the Novell Client 2.0 for Linux.

E.21.3 Installing and Configuring Shadow File System (ShadowFS) for SMB/CIFS Users

Location	Change
Section 12.4, "Installing ShadowFS and FUSE," on page 131	**IMPORTANT:** Make sure you run only a single instance of ShadowFS at a time. Avoid entering the command multiple times.
Section 12.11, "Starting and Stopping ShadowFS Manually," on page 136	Added information on how to stop ShadowFS.

E.21.4 Managing DST Shadow Volumes for NSS Volumes

Location	Change
Section 9.8, "Viewing the Name and Path Information for a Shadow Volume," on page 89	This section is new.

E.21.5 Planning Your Dynamic Storage Technology Solution

Location	Change
Section 5.1.1, "Storage Devices," on page 41	Revised for clarity.
Section 5.1.2, "iSCSI Block Storage Devices," on page 42	Added information about supported configurations.
Section 5.1.3, "Remote Secondary Volumes (Technology Preview)," on page 43	This section is new.
Section 5.1.4, "File Systems," on page 43	**IMPORTANT:** Mixing file systems for the primary and secondary areas in a given DST shadow volume pair is not supported.

Location	Change
Section 5.5, "Using NSS File System Trustees, Rights, and Attributes on DST Shadow Volumes," on page 51	This section is new.
Section 5.7, "Using NSS Quotas on DST Shadow Volumes," on page 52	This section is new.

E.21.6 Using DST to Migrate Data on Demand from NetWare to OES 2 Linux

Information in this chapter was revised and moved to Section 5.1.2, "iSCSI Block Storage Devices," on page 42.

E.22 May 30, 2008

Updates were made to the following section. The changes are explained below.

E.22.1 Managing Policies for Shadow Volumes

Location	Change
Section 10.1.10, "Subdirectory Restrictions," on page 105	Specify the path relative to the root of the DST volume, and not to the root of the server. For example, enter subdir1/subdir2.

E.23 May 5, 2008

Updates were made to the following section. The changes are explained below.

E.23.1 Commands and Utilities for Dynamic Storage Technology

Location	Change
Section A.1.2, "Command Line Mode," on page 184	You must escape quote characters when using ncpcon to issue commands at the console command prompt.

E.23.2 Installing and Configuring Dynamic Storage Technology

Location	Change
Section 3.1.6, "Novell Samba with ShadowFS, FUSE, and LUM," on page 32	Linux User Management is installed by default. Only SMB/CIFS users must be Linux-enabled with Linux User Management.

E.23.3 Installing and Configuring Shadow File System (ShadowFS) for SMB/ CIFS Users

Location	Change
Section 12.3, "Preparing Your System for Using ShadowFS," on page 130	For information about configuring SSH for a user, see "SSH Services on OES 2" in the *OES 2 SP3: Planning and Implementation Guide*.
Section 12.5, "Setting Rights to ShadowFS Shares," on page 132	For information about configuring SSH for a user, see "SSH Services on OES 2" in the *OES 2 SP3: Planning and Implementation Guide*.

E.24 January 7, 2008

Updates were made to the following section. The changes are explained below.

◆ Section E.24.1, "Managing DST Shadow Volumes for NSS Volumes," on page 239

E.24.1 Managing DST Shadow Volumes for NSS Volumes

Location	Change
Section 9.4.3, "Enabling or Disabling NCP/NSS Bindings by Editing the /etc/opt/novell/ncp2nss.conf File," on page 86	When the NCP/NSS bindings parameter is disabled for a volume, NCP Server adds an EXCLUDE_VOLUME entry to the /etc/opt/novell/ ncp2nss.conf file.

E.25 December 7, 2007

Updates were made to the following sections. The changes are explained below.

◆ Section E.25.1, "Planning Your Dynamic Storage Technology Solution," on page 240

◆ Section E.25.2, "Using DST to Migrate Data on Demand from NetWare to OES 2 Linux," on page 240

E.25.1 Planning Your Dynamic Storage Technology Solution

Location	Change
Section 5.1.2, "iSCSI Block Storage Devices," on page 42	References were added for information about Linux iSCSI target devices.

E.25.2 Using DST to Migrate Data on Demand from NetWare to OES 2 Linux

Location	Change
Chapter 12, "Using Secondary Volumes on iSCSI Block Storage Devices," on page 145	You can follow a similar procedure for NSS volumes on any iSCSI target device that is compatible with the Linux iSCSI initiator running on the OES 2 Linux server.

E.26 November 16, 2007

Updates were made to the following section. The changes are explained below.

- Section E.26.1, "Installing and Configuring Shadow File System (ShadowFS) for SMB/CIFS Users," on page 240

E.26.1 Installing and Configuring Shadow File System (ShadowFS) for SMB/CIFS Users

The following change was made to this section:

Location	Change
Section 12.5, "Setting Rights to ShadowFS Shares," on page 132	To test the POSIX rights setup, you need a user who is Linux-enabled with LUM, has SSH permissions for the server, and who has eDirectory rights to the location.