

Novell iSCSI for NetWare®

2SP1

www.novell.com

ADMINISTRATION GUIDE

October 2008



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 \(http://www.novell.com/info/exports/\)](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 © 2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

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

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

Novell Trademarks

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

Third-Party Materials

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

This Novell product includes code licensed from Intel Corporation as described in the following notice.

Copyright © 2000 Intel Corporation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Intel Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Contents

| | |
|------------------------------------------------------------------------------------------|-----------|
| About This Guide | 7 |
| 1 Overview | 9 |
| 1.1 Product Features | 10 |
| 1.2 Product Benefits | 11 |
| 1.3 iSCSI SAN Configurations | 12 |
| 1.4 What's Next | 14 |
| 2 Installation, Configuration, and Management | 15 |
| 2.1 iSCSI Initiator Requirements | 15 |
| 2.2 iSCSI Target Requirements | 15 |
| 2.2.1 NetWare Server | 15 |
| 2.2.2 Storage Router | 15 |
| 2.3 Installing iSCSI Initiator and Target Software | 15 |
| 2.4 Configuring iSCSI Targets | 16 |
| 2.4.1 Creating iSCSI Partitions | 16 |
| 2.4.2 Loading iSCSI Target Software | 17 |
| 2.4.3 Creating NSS Partitions, Pools, and Volumes | 17 |
| 2.4.4 Configuring Access Control to iSCSI Targets | 18 |
| 2.5 Configuring iSCSI Initiators | 19 |
| 2.5.1 Loading iSCSI Initiator Software and Connecting to an iSCSI Target | 19 |
| 2.5.2 Enabling and Configuring iSCSI Initiator Security | 21 |
| 2.6 Managing iSCSI | 22 |
| 2.6.1 Creating an iSCSI Session | 22 |
| 2.6.2 Ending an iSCSI Session | 22 |
| 2.6.3 Viewing and Editing Initiator Properties | 22 |
| 2.6.4 Viewing Target Properties | 24 |
| 2.6.5 Viewing Target Status | 24 |
| 2.6.6 Viewing Initiator Status | 25 |
| 2.6.7 Modifying Access Control to iSCSI Targets | 25 |
| 2.7 Accessing iSCSI Targets on NetWare Servers from Linux Initiators | 27 |
| 2.7.1 Configuring LDAP Access Control for Linux Initiators | 27 |
| 2.7.2 Ensuring the Cisco iSCSI Package Is Installed | 27 |
| 2.7.3 Editing the iSCSI Configuration File | 28 |
| 2.7.4 Connecting to the iSCSI Target | 28 |
| 3 Troubleshooting iSCSI services | 29 |
| 3.1 Unable to manage/configure Target Access control services from Novell Remote Manager | 29 |
| A Documentation Updates | 31 |
| A.1 March 20, 2008 | 31 |
| A.2 April 28, 2008 | 31 |

About This Guide

This guide describes how to install and configure Novell® NetWare® iSCSI. The guide is intended for network administrators and is divided into the following sections:

- ♦ Chapter 1, “Overview,” on page 9
- ♦ Chapter 2, “Installation, Configuration, and Management,” on page 15

IMPORTANT: OES NetWare and NetWare 6.5 share the same code base and are the same in every way. Installing the OES NetWare product or associated support pack is the same as installing the simultaneously released NetWare 6.5 product or associated support pack.

Audience

This guide is intended for network administrators.

Feedback

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

Documentation Updates

For the most recent version of the *iSCSI Installation and Configuration Guide*, see the [OES 2 Documentation Web site \(http://www.novell.com/documentation/oes2/stor_iscsi_nw/index.html?page=/documentation/oes2/stor_iscsi_nw/data/bookinfo.html#bookinfo\)](http://www.novell.com/documentation/oes2/stor_iscsi_nw/index.html?page=/documentation/oes2/stor_iscsi_nw/data/bookinfo.html#bookinfo).

Documentation Conventions

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

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

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX* or Linux*, should use forward slashes as required by your software.

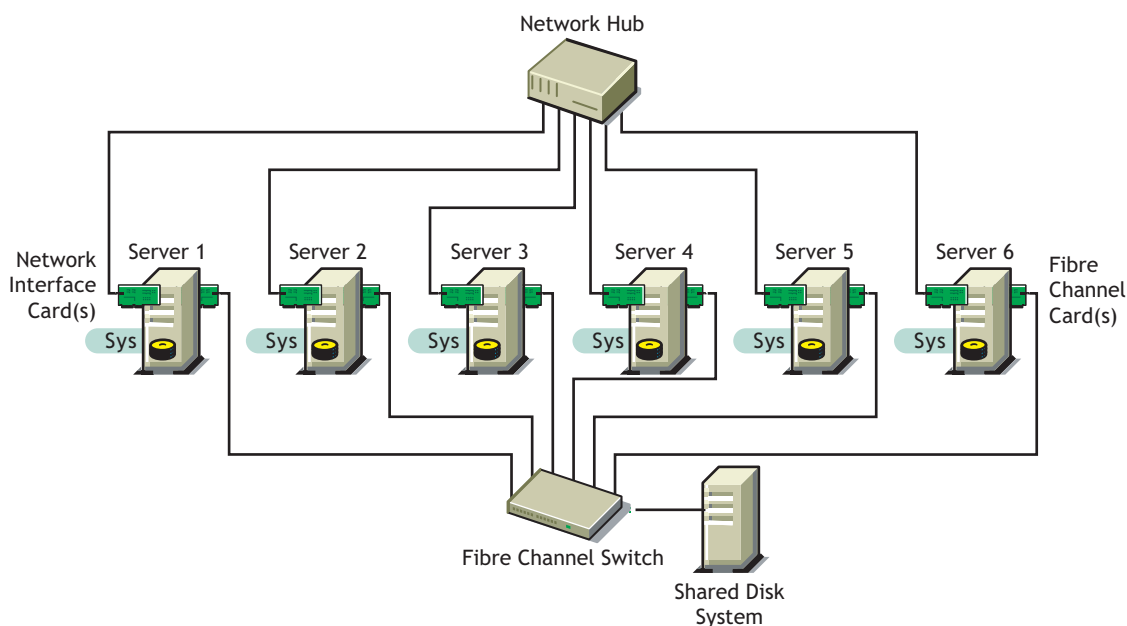
Overview

1

iSCSI is an emerging standard for SCSI block storage protocols networked over high-speed TCP/IP networks. iSCSI lets you create a low-cost Storage Area Network (SAN) using commodity high-speed Ethernet hardware. iSCSI provides significant cost savings when compared to the costs required to create a fibre channel SAN.

Currently, Novell® SANs consist of storage devices purchased from third-party storage vendors. Most SANs are constructed using fibre channel devices and storage arrays. A fibre channel host bus adapter is installed into each NetWare® server and connects each server to a fibre channel switch and external shared storage arrays. The SAN consolidates storage resources for servers running NetWare. RAID sets or individual disk drives located inside centralized storage arrays are exclusively assigned to individual servers in order to emulate direct-attached disks dedicated for each server, or they are assigned to and shared by multiple servers if running cluster software like Novell Cluster Services™. The following figure shows how a typical fibre channel SAN configuration might look.

Figure 1-1 Typical Fibre Channel SAN Configuration



The configuration illustrated above creates two separate networks and corresponding management domains. One is the fibre channel SAN dedicated to storage. The other is the traditional local area network that carries file, messaging, Web, LDAP, and other standard client/server protocol packets that clients of NetWare servers use to interact with Novell services.

NetWare iSCSI allows a SAN to be built using the same hardware and management domain that is used in a traditional LAN. An iSCSI SAN can use the same infrastructure as the LAN or it can have its own dedicated infrastructure.

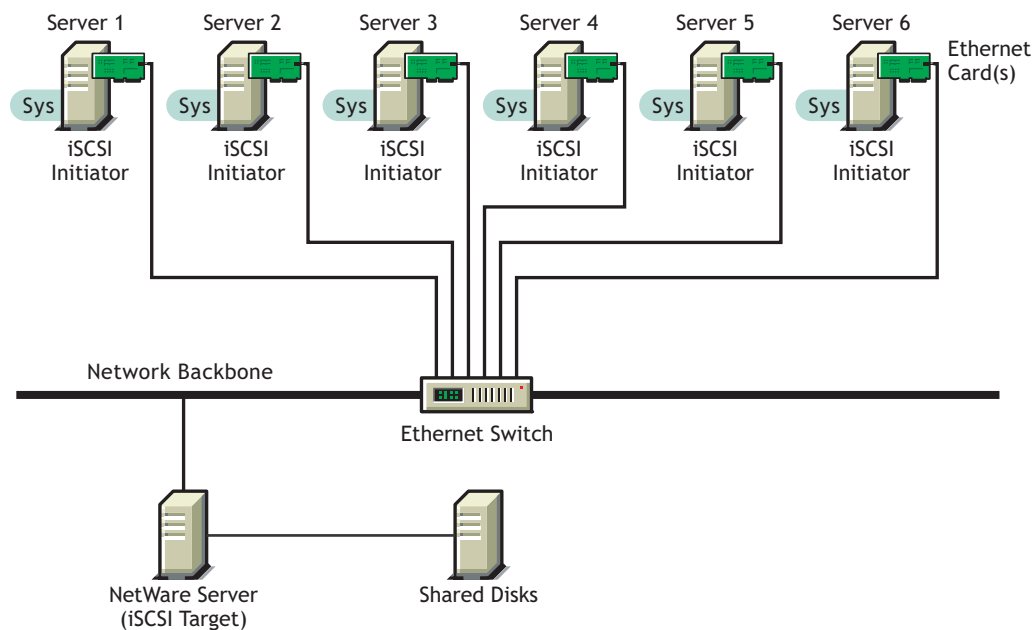
NetWare iSCSI consists of software that you add to your existing NetWare servers. It lets you use existing hardware on your NetWare network to create a SAN and a NetWare cluster.

NetWare iSCSI software is divided into two parts:

- ♦ **Initiator software** is installed and configured on servers in the SAN that will be used to access shared storage. Initiators can be cluster servers. Initiators use the iSCSI protocol to communicate with an iSCSI storage server or target over a TCP/IP network.
- ♦ **Target software** is installed on a NetWare server and provides access to shared disks through the iSCSI protocol. iSCSI target software enables the server where it is installed to function as a disk controller for the shared disk system.

The following figure shows how a typical iSCSI SAN configuration might look.

Figure 1-2 Typical iSCSI SAN Configuration



iSCSI storage routers perform the same function as an iSCSI target server. If you are using an iSCSI storage router, NetWare iSCSI target software is not needed.

1.1 Product Features

NetWare iSCSI includes several important features to help you create and manage a low-cost NetWare SAN:

- ♦ Support for standard TCP/IP networks using commodity Ethernet hardware.
- ♦ LDAP and directory-enabled NetWare iSCSI functions for enhanced disk access control.
- ♦ Single point of administration through the browser-based NetWare Remote Manager. This lets you remotely manage your iSCSI SAN.
- ♦ Support for Challenge Handshake Authentication Protocol (CHAP) authentication for initiator identity verification.
- ♦ Support for the iSCSI draft specification (Ratified Standard Draft 20).
- ♦ Interoperability with industry standard iSCSI storage servers or targets, including Cisco*, Network Appliance, and Adaptec*.

- ♦ Easy installation and configuration, especially compared to the complexity involved in installing and configuring a fibre channel SAN.

1.2 Product Benefits

Fibre channel hardware is expensive and complex to manage. NetWare iSCSI lets you consolidate storage and improve the management of your storage infrastructure on the well known TCP/IP infrastructure. It is a lower cost, more flexible alternative to fibre channel. With NetWare iSCSI, you can easily add storage and repartition existing storage between systems and logical groupings. If one user volume is growing too rapidly, storage from another area can be allocated to it.

Some of the benefits of implementing iSCSI include

- ♦ Low-cost hardware requirements
- ♦ Longer distance storage connectivity
- ♦ Easy-to-manage SAN solution
- ♦ Scalability and flexibility
- ♦ Reduced SAN management training requirements
- ♦ Increased flexibility in storage management and growth
- ♦ Ability to create a SAN from existing direct-attached storage servers

The benefits NetWare iSCSI provides can be better understood through the following scenario:

John is responsible for the network at the marketing ad agency he works at. For five years, a 70 GB hard disk in a server with an attached tape backup unit has met the needs of the small firm of 10 account reps and support staff. Then one of the account reps decided to create a proposal using digital video for a client, and the rest of the staff decided to do the same. One month later, all of the 70 GB was used up. John purchased 136 GB of additional disk space and directly attached it to his server. He had to bring the server down to plug in the new adapter card, hook up the storage, and configure the additional adapter and storage. Two months later, he noticed that he again needed additional storage. He purchased another 364 GB, and had to configure it and get it added into the system. System backups had started taking longer than a weekend, so he added another tape drive for backup. A few months later, he determined that another 1.3 TB was needed, and this would need to be on a SAN with LAN Free backup in order to manage the large amount of data. John started looking for an easy solution with lower costs, because the firm did not have the financial resources to purchase a 1.3 TB SAN. He is now stuck between a rock and a hard place.

John needs a cost-effective mass storage solution that can be easily managed. This includes data protection (backup or archival) that doesn't require John to learn a lot of new skills.

John expects to be able to add storage to his network without going through complex tasks to configure and install the storage, and he cannot succumb to down time. Adding storage should also automatically deal with his data protection problems.

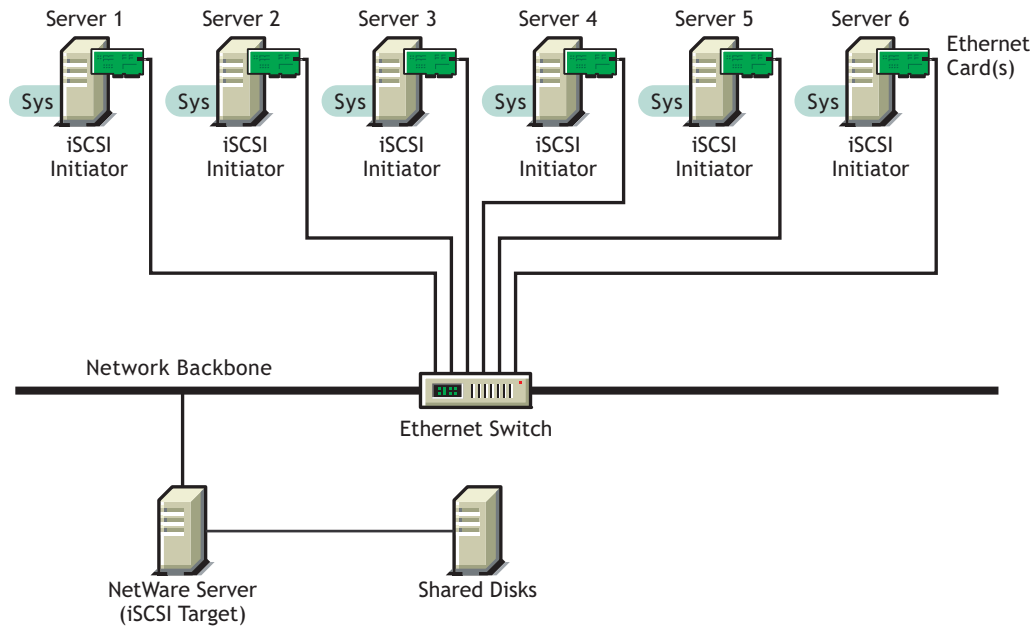
With NetWare iSCSI, John's problem is solved. His SAN infrastructure investment is no more than Gigabit Ethernet. He is already trained on 100 MB Ethernet for his LAN topology, so the required training for the hardware infrastructure is not needed. For iSCSI, the training is minimal. With Novell's LDAP-enabled iSCSI solution, management is simplified. The greatest cost is for the 1.3 TB disk array, which is much less expensive than a fibre channel SAN solution. Coupled with Novell's snapshot technology included in NetWare 6.5, he has an inexpensive solution for managing his rapidly growing data needs.

1.3 iSCSI SAN Configurations

iSCSI provides a great deal of flexibility and a number of different configuration options.

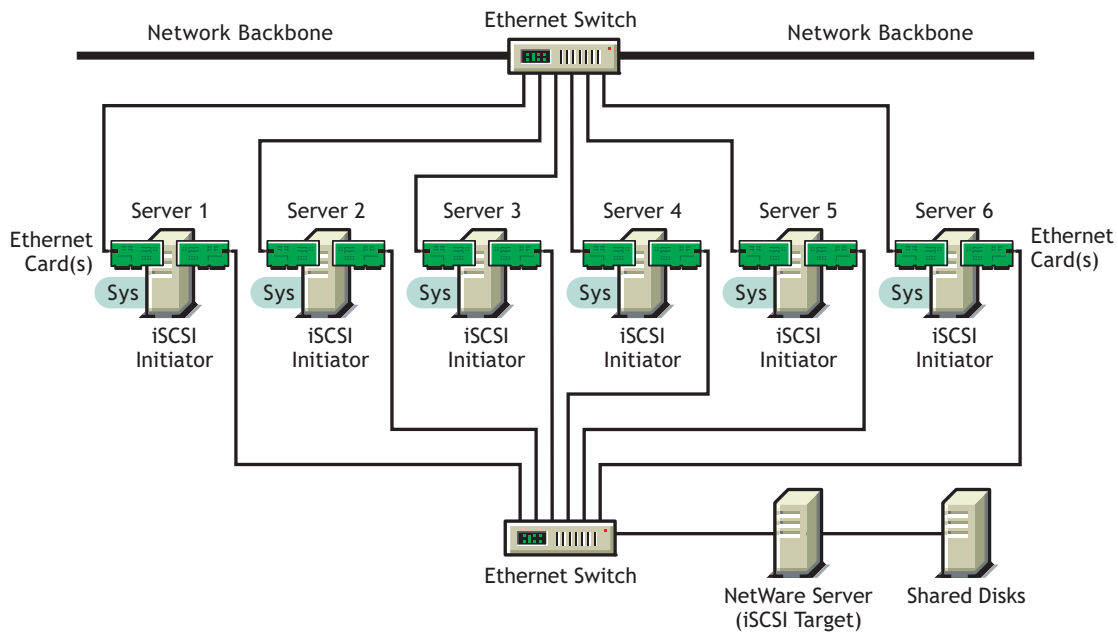
Three common iSCSI configurations are illustrated below, along with the advantages and disadvantages of each.

Figure 1-3 *Non-Dedicated Ethernet Configuration*



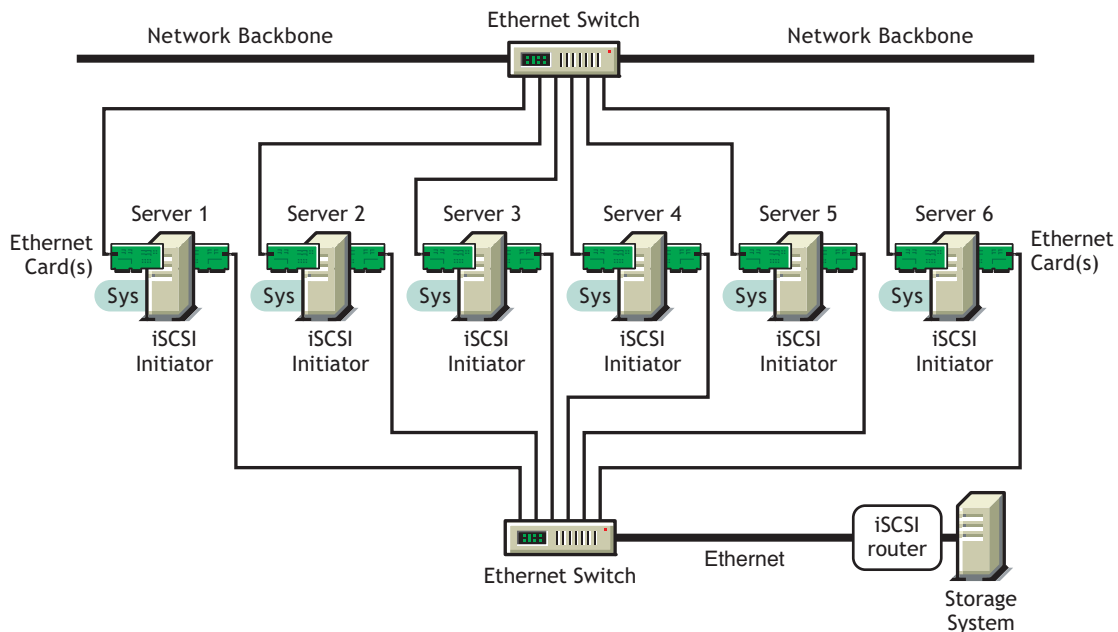
The nondedicated Ethernet configuration illustrated above is the least expensive iSCSI configuration option because you can leverage existing Ethernet hardware to create a low-cost SAN. Nondedicated Ethernet does not provide the same level of performance as dedicated Ethernet or iSCSI router configurations because disk requests and LAN traffic use the same network hardware.

Figure 1-4 *Dedicated Ethernet Configuration*



The dedicated Ethernet configuration illustrated above is more expensive than non-dedicated Ethernet, but provides better performance because separate Ethernet hardware is required for the SAN. Disk requests and LAN traffic each have their own dedicated Ethernet hardware.

Figure 1-5 *iSCSI Storage Router Configuration*



The iSCSI storage router configuration illustrated above is the most expensive iSCSI configuration option, but it provides the best performance. The iSCSI router configuration utilizes standard Ethernet hardware. Servers are connected via Ethernet connections to the iSCSI router, which is part of the shared storage system.

1.4 What's Next

To install and configure NetWare iSCSI, continue with [Chapter 2, “Installation, Configuration, and Management,”](#) on page 15.

Installation, Configuration, and Management

2

This section contains information that will help you install, configure, and manage iSCSI.

2.1 iSCSI Initiator Requirements

- ☐ NetWare® 6.5 software installed on all servers that will run iSCSI initiator software.
- ☐ The following software module upgraded on all NetWare servers that will function as iSCSI initiators:

Updated WINSOCK software, which is included with the OES Support Pack 2 update (NetWare 6.5 Support Pack 5): See [TID # 2974185 \(http://support.novell.com/docs/Readmes/InfoDocument/2974185.html\)](http://support.novell.com/docs/Readmes/InfoDocument/2974185.html) to download this software.

2.2 iSCSI Target Requirements

iSCSI targets can be NetWare 6.5 servers running iSCSI target software or storage routers (which are available from Cisco and other vendors).

2.2.1 NetWare Server

- ☐ NetWare 6.5 software installed on each server that will run iSCSI target software
- ☐ Direct-attached disk storage on the NetWare servers that will function as iSCSI targets
- ☐ The following software module upgraded on all NetWare servers that will function as iSCSI targets:

Updated WINSOCK software, which is included with the OES Support Pack 2 update (NetWare 6.5 Support Pack 5): See [TID # 2974185 \(http://support.novell.com/docs/Readmes/InfoDocument/2974185.html\)](http://support.novell.com/docs/Readmes/InfoDocument/2974185.html) to download this software.

2.2.2 Storage Router

- ☐ iSCSI target device that supports the iSCSI Internet Draft Specification 20
- ☐ Disk system connected to the iSCSI target device and configured according to the device manufacturer's instructions

2.3 Installing iSCSI Initiator and Target Software

NetWare iSCSI initiator and target software is automatically copied to the appropriate directories on your NetWare server during the NetWare 6.5 installation. No additional installation is required.

IMPORTANT: Do not run iSCSI initiator and target software simultaneously on the same server.

IMPORTANT: If you intend to install Novell® Cluster Services™ software on an iSCSI initiator server, in most cases you should do so *after* installing and configuring iSCSI initiator software and *before* creating NSS partitions on the disks on the shared disk system.

An exception to this might be if you are switching from fibre channel hardware to iSCSI.

2.4 Configuring iSCSI Targets

For information on configuring iSCSI targets that use iSCSI storage routers, refer to your iSCSI storage router documentation.

To configure an iSCSI target on a NetWare server, you must create an iSCSI partition, load iSCSI target software, configure access control to the target, and then create pools and volumes on the target from an iSCSI initiator.

In order to configure an iSCSI target using NetWare Remote Manager, NetWare Remote Manager must be configured and working properly on a secure port. See [Accessing Novell Remote Manager for Netware in the OES 2: Novell remote Manager for NetWare Administration Guide](http://www.novell.com/documentation/oes2/mgmt_remotemgr_nw/index.html?page=/documentation/oes2/mgmt_remotemgr_nw/data/a7hjvxo.html#a7hjvxo) (http://www.novell.com/documentation/oes2/mgmt_remotemgr_nw/index.html?page=/documentation/oes2/mgmt_remotemgr_nw/data/a7hjvxo.html#a7hjvxo) for more information

NOTE: iSCSI initiators cannot connect to NetWare servers functioning as iSCSI targets unless access control is configured.

2.4.1 Creating iSCSI Partitions

If you are using a NetWare server for an iSCSI target device, you can use either the NSSMU utility or NetWare Remote Manager to create iSCSI partitions.

Using NSSMU

- 1 Start the NSSMU utility by entering `nssmu` at the target server console.
- 2 Select Partitions from the Main menu.
- 3 Press Insert and select the device where you want to create the partition.
- 4 Select iSCSI as the partition type.
- 5 Specify the partition size, then select Create to create the partition.

Using NetWare Remote Manager

- 1 In the left column of the NetWare Remote Manager page under the Manage Server section, click Partition Disks.

A screen appears displaying a list of devices that are currently accessible to servers in the cluster. For each device, the list displays the partitions, NSS pools, volumes, and free space on that device.
- 2 Find the device where you want to create the iSCSI partition (on the iSCSI target), then click Create.
- 3 Select Novell iSCSI as the partition type, then click Create a New Partition.
- 4 Specify the desired partition size, then click Create to create the iSCSI partition.

2.4.2 Loading iSCSI Target Software

To load iSCSI Target software, you should set up your NetWare 6.5 server to load the Target software automatically. This can be done during the NetWare 6.5 server installation by choosing either the iSCSI SAN Storage Server option as part of a Pattern Installation, or the iSCSI Target component in the Customized NetWare Server installation. Choosing either installation option will automatically configure iSCSI target software on the server and cause the software to load automatically when the server starts.

Choosing either iSCSI installation option causes the following to happen automatically:

1. TON.NCF is added to the autoexec.ncf file of the server.

TON.NCF is used to start iSCSI target software on the server with access control enabled.

2. TINIT.NCF runs iscsitar.nlm with the -l, -p, and -s parameters.

NOTE: The command line switches referenced above are used with iscsitar.nlm, not TINIT.NCF. Because the above process happens automatically, there is no need to manually run TINIT.NCF.

- ♦ -l is the fully distinguished LDAP name for admin.
- ♦ -p is the admin password
- ♦ -s is the fully distinguished LDAP name for the iSCSI target server.

The admin name, target server name and the admin password are recorded during the NetWare 6.5 installation. They are then encrypted and saved in the sys:\etc\iscsi.lss file.

If you already have a NetWare 6.5 server that is not an iSCSI target installed and configured, you can make that server an iSCSI target by choosing the iSCSI Target component as part of a post-installation. For more information on NetWare 6.5 installation options and post-installation procedures, see the [OES 2 Netware Installation and Upgrade Guide \(http://www.novell.com/documentation/oes2/inst_oes_nw/index.html?page=/documentation/oes2/inst_oes_nw/data/front.html#front\)](http://www.novell.com/documentation/oes2/inst_oes_nw/index.html?page=/documentation/oes2/inst_oes_nw/data/front.html#front) for more information.

iSCSI target software can be unloaded by entering `toff` at the target server console.

iSCSI target software can be manually reloaded by entering `ton` at the target server console.

2.4.3 Creating NSS Partitions, Pools, and Volumes

On an iSCSI initiator with target session running, initialize and partition the iSCSI partition on the target using NSSMU or NetWare Remote Manager.

After configuring an iSCSI initiator and creating an iSCSI target session, create pools and volumes on the iSCSI target from the initiator server using NSSMU or NetWare Remote Manager. See [Section 2.5, “Configuring iSCSI Initiators,” on page 19](#) for information on configuring iSCSI initiators and creating iSCSI target sessions.

The iSCSI partition acts similar to a disk device (LUN). Servers running iSCSI initiator software see the iSCSI partition as a LUN. For this reason, it is still necessary to create an NSS partition on the iSCSI partition. The process for creating and configuring NSS partitions, pools, and volumes is the same for both iSCSI and fibre channel SANs. See the [OES 2 Novell Cluster Services 1.8.3 for NetWare Administration Guide \(http://www.novell.com/documentation/oes2/inst_oes_nw/index.html?page=/documentation/oes2/inst_oes_nw/data/front.html#front\)](http://www.novell.com/documentation/oes2/inst_oes_nw/index.html?page=/documentation/oes2/inst_oes_nw/data/front.html#front) for more information.

2.4.4 Configuring Access Control to iSCSI Targets

If your iSCSI target service is running on a NetWare server, you can control or limit access to targets through LDAP access control. LDAP access control is enabled by default, and uses Novell eDirectory™ to provide the ability to control the initiators that can access your iSCSI targets. iSCSI initiators will not be able to connect to NetWare servers functioning as iSCSI targets until you configure access control for each initiator.

Controlling initiator access to your iSCSI targets is necessary to prevent data corruption. Data corruption can occur if two initiators attempt to access the same target device at the same time in an uncoordinated way. Novell Cluster Services software provides the necessary coordination for multi-initiator access. Multiple initiators accessing the same target device can occur if any of the following conditions applies:

- ♦ Your iSCSI target server is accessible from multiple servers that do not have cluster software installed or running.
- ♦ Your iSCSI target is accessible from multiple servers that have cluster software installed and running, but the servers are in separate or different clusters.
- ♦ Your iSCSI target is accessible from multiple servers running different operating systems (NetWare, Linux*, etc.).

Because LDAP access control is enabled by default when iSCSI target software is installed and loaded, you just need to make the initiators that will access the iSCSI target, trustees of the Target object. Making iSCSI initiators trustees of an iSCSI target object is also necessary to properly secure iSCSI targets.

- 1** If your iSCSI target is in the same eDirectory tree as the iSCSI initiators that will access it, make each initiator server that you want to access the target a trustee of the Target object.

You don't need to assign specific access rights, you just need to make each Initiator object a trustee of the Target object.

When iSCSI target software is first started on a server, an iSCSI target object for each iSCSI partition is automatically created in the same eDirectory context as the target server.

- 2** (Conditional) If your iSCSI target is not in the same eDirectory tree as the iSCSI initiators that will access it, create initiator objects, and make them trustees of the Target object.

- 2a** In the eDirectory tree where the iSCSI target object resides, create a separate Initiator object to represent each iSCSI initiator that you want to access the iSCSI target.

Use the same name for the Initiator object as the initiator server it represents.

If a question mark (?) appears next to the Initiator objects that you create, it indicates that a snap-in is not present. This does not adversely affect the trustee assignments.

- 2b** Make each Initiator object a trustee of the Target object.

Do not change any of the defaults while completing this step.

- 2c** At the server console of an iSCSI initiator server, enter `iscsi list` and record the initiator's Internet Qualified Name (IQN).

- 2d** Change the initiator server's IQN to correspond to the applicable Initiator object you just created in the target server's eDirectory tree by entering `iscsi set InitiatorName=baseIQN:initiator_objectdn` at the initiator server console.

For example, if after entering `iscsi list` at the server console, the server's current IQN and distinguished name (dn) displays as

InitiatorName=iqn.1984-08.com.novell:.SERV1.acme.ACMETREE.

and the distinguished name of the initiator object you created in the eDirectory tree where the iSCSI target resides is

SERV1.sales.SALESTREE

then you would enter the following at the iSCSI initiator server console:

```
iscsi set InitiatorName=iqn.1984-  
08.com.novell:.SERV1.sales.SALESTREE.
```

NOTE: As is illustrated in the above example, the eDirectory tree name is required when specifying the distinguished name of the iSCSI Initiator object.

NOTE: Do not use underscore characters when specifying the initiator server's IQN, the eDirectory tree, or the distinguished name of the initiator object. Underscore characters are not RFC compliant.

LDAP access control ensures that only the initiators that are trustees of the Target object are able to access that target. Without LDAP access control, any initiator that could connect to a target could access the storage devices on that target.

2.5 Configuring iSCSI Initiators

NetWare iSCSI initiator software can be configured either at the server console using server console commands or remotely using NetWare Remote Manager. In order to configure an iSCSI initiator using NetWare Remote Manager, NetWare Remote Manager must be configured and working properly on a secure port. See [Accessing Novell Remote Manager for Netware in the OES 2: Novell remote Manager for NetWare Administration Guide \(http://www.novell.com/documentation/oes2/mgmt_remotemgr_nw/index.html?page=/documentation/oes2/mgmt_remotemgr_nw/data/a7hjvxo.html#a7hjvxo\)](http://www.novell.com/documentation/oes2/mgmt_remotemgr_nw/index.html?page=/documentation/oes2/mgmt_remotemgr_nw/data/a7hjvxo.html#a7hjvxo) for more information

2.5.1 Loading iSCSI Initiator Software and Connecting to an iSCSI Target

Using Server Console Commands

For each server that you want to function as an iSCSI initiator, do the following:

- 1 Enter `ion` at the server console to load iSCSI initiator software. Wait for about 10 secs for the initiator to startup.

You can also enter `ioff` at the server console to unload iSCSI initiator software. .

- 2 Enter `iscsinit connect a.b.c.d target_name` at the server console.

Replace *a.b.c.d* with the IP address of the iSCSI target device that is connected to the shared storage system.

If the iSCSI target device is an iSCSI storage router, then this is the IP address of the storage router. If the iSCSI target device is a NetWare server, then this is the IP address of the NetWare server.

Replace *target_name* with the iSCSI target name that is displayed after running the `iscsinit discover a.b.c.d` command. The iSCSI target name is case sensitive. You can leave the target name out to cause the initiator to connect to all available targets. Wait for about 10 secs such that the devices are mounted before issuing any command to mount the pools or cluster resources that reside on those devices.

- 3 (Optional) To use CHAP authentication when connecting to an iSCSI target, use the `/CHAP` command line option with the `iscsinit connect` command.

For example, if you have configured a locally stored CHAP secret and you want CHAP to use it, you would enter `iscsinit/chap connect a.b.c.d` at the command line.

If you want to use a user-supplied CHAP secret, you would enter `iscsinit/chap="sys:\system\chap.txt connect a.b.c.d` at the command line.

The `chap.txt` file must be created prior to running the command and must contain the following lines:

```
OutgoingUsername=initiator name or agreed upon name
```

```
OutgoingPassword=shared secret text
```

You can configure and enable CHAP using NetWare Remote Manager. For more information on configuring and enabling CHAP, see [“Enabling and Configuring iSCSI Initiator Security” on page 21](#).

If you want iSCSI initiator software to load automatically when servers start, you can add the commands in the above steps to the `autoexec.ncf` file of each initiator server.

Using NetWare Remote Manager

For each server that you want to function as an iSCSI initiator:

- 1 Enter `ion` at the server to load iSCSI initiator software.

You can do this either at the server console or remotely by using NetWare Remote Manager to access the server console.

- 2 On the NetWare Remote Manager main page, click the iSCSI Services link at the bottom of the left column.

- 3 Click Add Target and type the IP address of the iSCSI target device that is connected to the shared storage system.

If the iSCSI target device is an iSCSI storage router, then this is the IP address of the storage router. If the iSCSI target device is a NetWare server, then this is the IP address of the NetWare server.

Each target device can have multiple targets.

If you want a list of possible target names for a given IP address, click Browse and type the IP address of the target device.

- 4 Click Next, select the target name you want to establish a session with, then click Next.

2.5.2 Enabling and Configuring iSCSI Initiator Security

Configuring iSCSI initiator security consists of configuring the initiator-to-target authentication method. Challenge Handshake Authentication Protocol (CHAP) authentication is the method currently supported for initiator identity verification. CHAP protects against attacks and provides secure access between the iSCSI initiator and the target. If CHAP is not enabled, someone could potentially use the identity of a valid initiator to gain unauthorized access to iSCSI target devices. CHAP authentication is not enabled by default.

If your iSCSI target has CHAP enabled, you must enable CHAP on the initiators that will access that target, or target access will be denied. CHAP authentication is not currently supported on NetWare servers configured as iSCSI targets.

To enable and configure CHAP authentication using NetWare Remote Manager:

- 1 On the NetWare Remote Manager main screen, click the iSCSI Services link at the bottom of the left column.

- 2 Click the Security link.

This brings up a page that lets you choose the initiator-to-target authentication method.

- 3 Choose CHAP as the authentication method, then click Apply.

If you choose CHAP, you must create a CHAP secret that will be used to ensure secure authentication between this initiator and the target.

- 4 Click Create to bring up a page that lets you configure the CHAP secret.

If you have already configured a locally stored CHAP secret, the Update, Delete, and Change To buttons appear to let you modify or delete your existing secret, or change it to a user supplied secret. If you have already chosen the user supplied secret option, a Change To button appears to let you change to a locally stored secret.

- 5 Choose whether you want the CHAP secret to be locally stored or user supplied.

A locally stored secret is encrypted and stored on the initiator server. The same locally stored secret is used each time a session is started between this initiator and the target. Selecting the Locally Stored Secret option brings up a page that lets you specify the CHAP username and secret.

If you choose a user supplied CHAP secret, you will be prompted to create the CHAP secret each time you start a session between this initiator and the target. With this option, the CHAP secret is not stored on the initiator server, and it is not encrypted.

- 6 (Conditional) If you chose to create a locally stored CHAP secret, view and if necessary edit the CHAP username and create a CHAP secret.

The Initiator CHAP Username field is automatically filled in. It is the Internet Qualified Name (IQN) of this initiator. This field should not be changed unless you change the IQN of this initiator or you want to create or modify a CHAP locally stored secret for another initiator.

The Initiator CHAP Secret can include any ASCII characters and should be at least 16 characters long. The secret is encrypted and stored locally on the initiator.

- 7 Repeat the above steps to enable and configure CHAP authentication for each initiator server.

2.6 Managing iSCSI

NetWare iSCSI software includes management features that let you create or end iSCSI initiator/target sessions, view or edit initiator properties, monitor iSCSI status and connection information, and modify or disable iSCSI Target access control.

2.6.1 Creating an iSCSI Session

To create an iSCSI initiator/target session, follow the instructions in [Section 2.5, “Configuring iSCSI Initiators,”](#) on page 19.

2.6.2 Ending an iSCSI Session

You can end an iSCSI target session at the initiator server console or by using NetWare Remote Manager.

To end an iSCSI target session at the initiator server console, enter `iscsinit disconnect a.b.c.d`

Replace *a.b.c.d* with the IP address of the iSCSI target device.

Using the `iscsinit disconnect` command will disconnect or end all iSCSI target sessions for the specified IP address. If you want to end an iSCSI target session for a specific target, use NetWare Remote Manager.

If you have NetWare 6.5 Support Pack 3 (SP 3) or later installed, you can specify the target name to disconnect from a specific target. In this case, you would enter `iscsinit disconnect a.b.c.d target_name`.

Replace *target_name* with the iSCSI target name that is displayed after running the `iscsinit discover a.b.c.d` command. The iSCSI target name is case sensitive. With NetWare 6.5 SP 3, you can also leave the target name out to cause the initiator to disconnect from all available targets at the specified IP address.

To end an iSCSI target session using NetWare Remote Manager:

- 1 On the NetWare Remote Manager main page, click the iSCSI Services link at the bottom of the left column.
- 2 Click End Session.
- 3 Check the check box next to each target you want to disconnect from this initiator, then click Next to disconnect them.

The same procedure for ending a session using NetWare Remote Manager can also be used from the target.

2.6.3 Viewing and Editing Initiator Properties

You can view iSCSI initiator properties at the initiator server console or by using NetWare Remote Manager. To change iSCSI initiator and driver properties, you must use NetWare Remote Manager.

To view iSCSI initiator properties at the initiator server console, enter `iscsinit info`.

To view or change iSCSI initiator properties using NetWare Remote Manager:

- 1 On the NetWare Remote Manager main page, click the iSCSI Services link at the bottom of the left column.
- 2 Click the Properties link to bring up a page that lets you view or change initiator and driver properties.
- 3 View or change the desired properties, then click Finish to save changes.

Current initiator and driver properties include the following:

- ♦ Authentication Method
- ♦ Frontpage Display Controls
- ♦ Connection Path Recovery Controls
- ♦ Number of LUN Probes per Target
- ♦ Display Driver Statistics
- ♦ Performance and Trend Graphs
- ♦ Reports

Authentication Method

The default authentication method is None. This property cannot be changed or deselected for this release.

Frontpage Display Controls

The Frontpage Display Controls check boxes determine what information is displayed on the iSCSI initiator main page. Checking a check box causes that information to be displayed. For example, if you check the Network Address check box, the IP address of the target device will be displayed in the Storage Sessions section of the iSCSI initiator main page.

Connection Path Recovery Controls

The Connection path recovery controls are tolerance and timeout configuration settings for communication between initiators and targets. You can enable or disable Connection path recovery controls. These controls are configured to default settings, and should not be changed except under the direction of Novell Technical Support.

Number of LUN Probes per Target

The number of LUN probes per target is the number of targets you want the initiator to communicate with on the target device.

NOTE: If the iSCSI target is a NetWare server, only one LUN per target is supported. Adjusting the number of LUN probes per target only applies to third-party iscsi targets (Cisco, NetApp, etc.).

Display Driver Statistics

Checking the Display Driver (HAM) Statistics check box causes operational statistics to be displayed on the iSCSI initiator main page. There will also be link on the main page to an iSCSI Device Driver Requests graph.

Performance and Trend Graphs

If you check the Performance and Trend Graphs check box, there will be links to informative graphs for Data Transfer Rate and Trend Distribution on the iSCSI initiator main page.

Reports

If you check the Reports check box, there will be buttons to view or e-mail the iSCSI report on the iSCSI initiator main page. The iSCSI report contains statistics for iSCSI files and functions.

2.6.4 Viewing Target Properties

You can view iSCSI target properties by using NetWare Remote Manager.

- 1 On the NetWare Remote Manager main screen, click the iSCSI Services link at the bottom of the left column.
- 2 Click the Properties link to bring up a page that lets you choose which target properties you want displayed on the iSCSI target main page.

Current driver properties include the following:

- ♦ Frontpage Display Controls
- ♦ Performance and Trend Graphs
- ♦ Reports

Frontpage Display Controls

The Frontpage Display Controls check boxes determine what information is displayed on the iSCSI target main page. Checking a check box causes that information to be displayed. For example, if you check the Initiator Network Address check box, the IP address of initiators with active sessions will be displayed in the Storage Sessions section of the iSCSI target main page.

Performance and Trend Graphs

If you check the Performance and Trend Graphs check box, there will be links to informative graphs for Data Transfer Rate and Trend Distribution on the iSCSI target main page.

Reports

If you check the Reports check box, there will be buttons to view or e-mail the iSCSI report on the iSCSI target main page. The iSCSI report contains statistics for iSCSI files and functions.

2.6.5 Viewing Target Status

You can view general iSCSI target status information and active session information at the target server console or by using NetWare Remote Manager.

To view iSCSI target status and active session information at the target server console, enter `iscsitar sessions`.

To view iSCSI target status and active session information using NetWare Remote Manager:

- 1 After logging in to an initiator with an active iSCSI session using NetWare Remote Manager, click the iSCSI Services link at the bottom of the left column to bring up the iSCSI initiator main page.
- 2 Click the Status button to bring up a page that displays general target status information.
If there are no active iSCSI target session, no Status buttons or storage sessions are displayed.
- 3 On the page that appears after clicking the Status button, click a connection number to get more detailed information on the status of that connection.

2.6.6 Viewing Initiator Status

You can view general iSCSI initiator status information and active session information at the initiator server console or by using NetWare Remote Manager.

To view iSCSI target status and active session information at the initiator server console, enter `iscsinit status`.

To view iSCSI target status and active session information using NetWare Remote Manager:

- 1 After logging in to a target with an active iSCSI session using NetWare Remote Manager, click the iSCSI Services link at the bottom of the left column to bring up the iSCSI target main page.
- 2 Click the Status button to bring up a page that displays general initiator status information.
If there are no active iSCSI sessions, no Status buttons are displayed.

2.6.7 Modifying Access Control to iSCSI Targets

You can modify, disable, or remove iSCSI target access control after it has been configured. If you disabled or removed access control, you can also re-enable it or add it again.

Modifying iSCSI Target Access Control

The only modification you can currently make to iSCSI target access control after it has been configured, other than disabling or removing it, is to change the iSCSI administrator password.

This password is encrypted and stored in a secret store. The iSCSI target server administrator password by default is set to be the same as the eDirectory administrator password. Changing this password does not automatically change the eDirectory administrator password. Likewise, changing the eDirectory administrator password does not automatically change this password. Both passwords must currently be managed separately.

You can change the LDAP DN that the iSCSI target server administrator uses to match passwords with from the eDirectory administrator default to another user object by removing and readding iSCSI target access control. If you change the LDAP DN, that user object must have administrative rights to the iSCSI objects. See [“Disabling or Removing iSCSI Target Access Control” on page 26](#) for more information.

The iSCSI target server administrator password must be the same as the specified eDirectory user (default is eDirectory administrator) with administrative rights to the iSCSI objects. If they are different, iSCSI partitions on the target server will not be accessible to initiators. If the password

changes for the eDirectory user with administrative rights to the iSCSI objects, you must use this option to change the iSCSI target administrator password to match.

To change the iSCSI administrator password:

- 1 Log in to the iSCSI target using NetWare Remote Manager and click the iSCSI Services link at the bottom of the left column to bring up the iSCSI target main page.
- 2 Click the LDAP link and enter the old password and the new one.

Disabling or Removing iSCSI Target Access Control

You can disable or completely remove iSCSI access control capability on the iSCSI target. If you disable or remove iSCSI target access control, any initiator on the same network will be able to connect to the iSCSI target.

To disable or remove iSCSI target access control:

- 1 Log in to the iSCSI target using NetWare Remote Manager and click the iSCSI Services link at the bottom of the left column to bring up the iSCSI target main page.
- 2 Click the LDAP link, then click the radio button to either disable LDAP configuration or remove LDAP configuration.

Removing LDAP configuration deletes the secret store where the iSCSI administrator password is encrypted and stored.

- 3 After clicking the Next button, unload and reload iSCSI target server software to cause the changes to take effect.

You can do this by entering TOFF at the target server console to unload iSCSI target software and then entering TON at the target server console to load iSCSI target software.

LDAP access control can be enabled or added by clicking LDAP on the main iSCSI target page and entering the necessary information in the fields provided.

Adding or Re-enabling iSCSI Target Access Control

If you have disabled or removed iSCSI target access control, you can easily re-enable it or add it again using NetWare Remote Manager. If you removed iSCSI target access control, adding it again re-creates the secret store that was deleted when you removed access control.

To re-enable or add iSCSI target access control:

- 1 Log in to the iSCSI target using NetWare Remote Manager and click the iSCSI Services link at the bottom of the left column to bring up the iSCSI target main page.
- 2 Click the LDAP link, then ensure that the Service DN and Login DN fields are correct.

Service DN is the LDAP distinguished name of the server running iSCSI target software. The LDAP distinguished name of the iSCSI target server is automatically added to the field.

Login DN is the LDAP distinguished name of the eDirectory administrator account. You can leave the default or enter the distinguished name of another eDirectory user with administrative rights to the iSCSI objects.

- 3 Enter the administrator password for the Login DN and confirm the password is correct by adding it again.
- 4 After clicking the Next button, unload and reload iSCSI target server software to cause the changes to take effect.

You can do this by entering TOFF at the target server console to unload iSCSI target software and then entering TON at the target server console to load iSCSI target software.

2.7 Accessing iSCSI Targets on NetWare Servers from Linux Initiators

You can configure access to a NetWare server functioning as an iSCSI target from Linux initiators. To do this, you must first configure your NetWare server to be an iSCSI target as explained in [Section 2.4, “Configuring iSCSI Targets,” on page 16](#). Linux partition types (ext2, ext3, reiser) instead of NSS partitions can be created on the iSCSI target LUN.

This section covers the following information to help you configure access to NetWare iSCSI targets from Linux initiators:

- [Section 2.7.1, “Configuring LDAP Access Control for Linux Initiators,” on page 27](#)
- [Section 2.7.2, “Ensuring the Cisco iSCSI Package Is Installed,” on page 27](#)
- [Section 2.7.3, “Editing the iSCSI Configuration File,” on page 28](#)
- [Section 2.7.4, “Connecting to the iSCSI Target,” on page 28](#)

2.7.1 Configuring LDAP Access Control for Linux Initiators

The information in this section assumes you have LDAP access control to your iSCSI target enabled. If you have disabled LDAP access control to your iSCSI target, skip to [Section 2.7.2, “Ensuring the Cisco iSCSI Package Is Installed,” on page 27](#).

To configure LDAP access control from a Linux initiator to your iSCSI target:

- 1 Create an iSCSI Initiator object in LDAP for each Linux server you want to function as an iSCSI initiator.
- 2 Edit the `/etc/initiatorname.iscsi` file and add the LDAP distinguished name of the iSCSI Initiator objects you created above.

For example, in the `/etc/initiatorname.iscsi` file, find the line that appears similar to
`InitiatorName=iqn.1987-05.com.cisco:01.988fe4ed1d87`

In the line above, remove the text after the colon (:) and replace it with the distinguished name of an iSCSI Initiator object. The line should now appear similar to the following example:

`InitiatorName=iqn.1987-05.com.cisco:cn=LinuxInitiator,o=Novell`

where *LinuxInitiator* is the name of the iSCSI Initiator object you created above.

- 3 Make the iSCSI Initiator objects you created above trustees of the iSCSI Target object.

See [“Configuring Access Control to iSCSI Targets” on page 18](#) for more information on enabling, disabling, and configuring iSCSI target access control.

2.7.2 Ensuring the Cisco iSCSI Package Is Installed

The Cisco iSCSI package is included with SLES9. To see if the package is installed, search for the `iscsi.conf` file in the `/etc` directory. If the `iscsi.conf` is not present, install the package using Linux console commands or YaST.

Continue with [Section 2.7.3, “Editing the iSCSI Configuration File,” on page 28](#).

2.7.3 Editing the iSCSI Configuration File

After installing the Cisco iSCSI package, you must edit the iSCSI configuration file (`iscsi.conf`) to add the necessary information. The `iscsi.conf` configuration file contains instructions on the kinds of configuration information that can be added to the file.

- 1 Find and record the Internet Qualified Name (iqn) of the iSCSI target by entering `iscsitar targets` at the server console of the iSCSI target server.

- 2 Edit the `/etc/iscsi.conf` file and add the following lines:

```
DiscoveryAddress=ipaddress
```

```
TargetName=internet_qualified_name
```

Replace *ipaddress* with the IP address of the iSCSI target server.

Replace *internet_qualified_name* with the iqn you recorded in [Step 1](#).

The new lines should appear similar to the following example:

```
DiscoveryAddress=151.152.153.10
```

```
TargetName=iqn.1984-08.com.novell:80804566-51e6-d811-b869-  
0007e913505a
```

2.7.4 Connecting to the iSCSI Target

To cause the Linux initiator server to connect to the NetWare iSCSI target server, enter `/etc/init.d/iscsi start` at the Linux console.

A message should appear indicating that the server has discovered new hardware. To verify that the Linux initiator has connected to the target, enter `iscsi-ls` at the initiator server console.

If you are connecting to an iSCSI target that already has NSS partitions and pools created on it, you may not be able to access those NSS partitions and pools until you either reboot the Linux initiator server or run the `evms_activate` command at the Linux server console. This is required for each Linux initiator server that will access the iSCSI target.

Troubleshooting iSCSI services

3

This section discusses potential issues and workarounds for Novell® iSCSI services on OES 2 NetWare.

- ♦ [Section 3.1, “Unable to manage/configure Target Access control services from Novell Remote Manager,” on page 29](#)

3.1 Unable to manage/configure Target Access control services from Novell Remote Manager

Cause: In a server, if the initiator and target software are loaded together and at any point of time if the initiator software is unloaded using `ioff`, then you will lose the iscsi management plugin ‘Storage Services’ from the NRM. Hence you may not be able to manage/configure the Target Access control services from NRM. .

Action: To get the pluggin ‘Storage Services’ back, reload target software typing ‘TON’.

Documentation Updates

A

- ♦ [Section A.1, “March 20, 2008,” on page 31](#)
- ♦ [Section A.2, “April 28, 2008,” on page 31](#)

A.1 March 20, 2008

- ♦ Updated the preface with a section for Audience and Feedback.
- ♦ Updated the guide with common edits and structure.
- ♦ Updated the book to the December 11, 2007 template.

A.2 April 28, 2008

- ♦ Updated the book to the April 24, 2008 template.