

SpinServer® 4100

Quick Start Guide

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <http://www.netapp.com>

Part number 210-00736
February 2005

Copyright and trademark information

Copyright information

Copyright © 1994–2005 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

Portions © 1998–2001 The OpenSSL Project. All rights reserved.

No part of this book covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Portions of this product are derived from the Berkeley Net2 release and the 4.4-Lite-2 release, which are copyrighted and publicly distributed by The Regents of the University of California.

Copyright © 1980–1995 The Regents of the University of California. All rights reserved.

Portions of this product are derived from NetBSD, which is copyrighted by Carnegie Mellon University.

Copyright © 1994, 1995 Carnegie Mellon University. All rights reserved. Author Chris G. Demetriou.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that both the copyright notice and its permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS “AS IS” CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Software derived from copyrighted material of The Regents of the University of California and Carnegie Mellon University is subject to the following license and disclaimer:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notices, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS 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 THE REGENTS 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.

Portions of the software were created by Netscape Communications Corp.

The contents of those portions are subject to the Netscape Public License Version 1.0 (the "License"); you may not use those portions except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/NPL/>.

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released March 31, 1998.

The Initial Developer of the Original Code is Netscape Communications Corp. Portions created by Netscape are Copyright © 1998 Netscape Communications Corp. All rights reserved.

This software contains materials from third parties licensed to Network Appliance Inc. which is sublicensed, and not sold, and title to such material is not passed to the end user. All rights reserved by the licensors. You shall not sublicense or permit timesharing, rental, facility management or service bureau usage of the Software.

Portions developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999 The Apache Software Foundation.

Portions Copyright © 1995–1998, Jean-loup Gailly and Mark Adler

Portions Copyright © 2001, Sitraka Inc.

Portions Copyright © 2001, iAnywhere Solutions

Portions Copyright © 2001, i-net software GmbH

Portions of this product are derived from version 2.4.11 of the libxml2 library, which is copyrighted by the World Wide Web Consortium.

Network Appliance modified the libxml2 software on December 6, 2001, to enable it to compile cleanly on Windows, Solaris, and Linux. The changes have been sent to the maintainers of libxml2. The unmodified libxml2 software can be downloaded from <http://www.xmlsoft.org/>.

Copyright © 1994–2002 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>

Software derived from copyrighted material of the World Wide Web Consortium is subject to the following license and disclaimer:

Permission to use, copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications, that you make:

1. The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.
2. Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, a short notice of the following form (hypertext is preferred, text is permitted) should be used within the body of any redistributed or derivative code: "Copyright © [Sdate-of-software]"

World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved.
<http://www.w3.org/Consortium/Legal/>.

3. Notice of any changes or modifications to the W3C files, including the date changes were made.

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

Software derived from copyrighted material of Network Appliance, Inc. is subject to the following license and disclaimer:

Network Appliance reserves the right to change any products described herein at any time, and without notice. Network Appliance assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Network Appliance. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Network Appliance.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the Network Appliance design, the bolt design, NetApp—the Network Appliance Company, FAServer, NearStore, NetCache, and WAFL are registered trademarks of Network Appliance, Inc. in the United States and other countries. Network Appliance is a registered trademark of Network Appliance, Inc. in Monaco and a trademark of Network Appliance, Inc. in the United States and Canada. SnapCopy is a registered trademark of Network Appliance, Inc. in the European Union and a trademark of Network Appliance, Inc. in the United States. DataFabric, FilerView, SecureShare, SnapManager, SnapMirror, SnapMover, SnapRestore, and SyncMirror are registered trademarks of Network Appliance, Inc. in the United States. Data ONTAP and Snapshot are trademarks of Network Appliance, Inc. in the United States and other countries. ApplianceWatch, BareMetal, Center-to-Edge, ContentDirector, FlexClone, FlexVol, FPolicy, gFiler, MultiStore, RAID-DP, SecureAdmin, Serving Data by Design, Smart SAN, SnapCache, SnapDrive, SnapLock, SnapVault, vFiler, and Web Filer are trademarks of Network Appliance, Inc. in the United States. Spinnaker Networks, the Spinnaker Networks logo, SpinAccess, SpinCluster, SpinFS, SpinHA, SpinMove, SpinServer, and SpinStor are registered trademarks of Spinnaker Networks, LLC in the United States, other countries, or both. SpinAV, SpinManager, SpinMirror, and SpinShot are trademarks of Spinnaker Networks, LLC in the United States, other countries, or both.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the United States and/or other countries.

Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries.

RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

Network Appliance is a licensee of the CompactFlash and CF Logo trademarks.

Network Appliance NetCache is certified RealSystem compatible.

Table of Contents

	Preface	.ix
Chapter 1	Introduction	1
Chapter 2	Obtaining Configuration Information	3
	SpinServer Configuration Information	4
	NFS Client Configuration Information	5
	CIFS Client Configuration Information	6
Chapter 3	Attaching System Cables and Power Cords	7
	Attaching system cables	8
	Connecting server and storage cabinets	10
	Attaching power cords	13
Chapter 4	Initializing the System.	15
	Turning on system components.	16
	Installing SpinFS	17
Chapter 5	Configuring the System	21

Preface

- About this guide

This guide describes tasks that are required to get a SpinServer® system up and running quickly.
- Audience

This guide is for system administrators who are familiar with operating systems that run on the SpinServer’s clients, such as UNIX®, Windows 95™, Windows NT®, Windows® 2000, and Windows 2003. It assumes that you know how to use a Web browser.
- Terminology

This guide uses the term “SpinServer system” to mean all components that are packaged and configured with the SpinServer product, including SpinServer 4100 servers, uninterruptible power supplies (UPSs), FAS270c RAID enclosures, DS14mk2 FC JBOD enclosures, and Fibre Channel switches.
- Command conventions

You can enter commands on the system console or from any client that can obtain access to the SpinServer by using a Secure Shell (SSH) session.
- Formatting conventions

The following table lists different character formats used in this guide to set off special information.

Formatting convention	Type of information
<i>Italic type</i>	◆ Words or characters that require special attention. ◆ Placeholders for information you must supply. For example, if the guide requires you to enter the <code>fctest adaptername</code> command, you enter the characters “fctest” followed by the actual name of the adapter. ◆ Book titles in cross-references.
Monospaced font	◆ Command and daemon names. ◆ Information displayed on the system console or other computer monitors. ◆ The contents of files.

Formatting convention	Type of information
Bold monospaced font	Words or characters you type. What you type is always shown in lowercase letters, unless your program is case-sensitive and uppercase letters are necessary for it to work properly.

Keyboard conventions

This guide uses capitalization and some abbreviations to refer to the keys on the keyboard. The keys on your keyboard might not be labeled exactly as they are in this guide.

What is in this guide...	What it means...
hyphen (-)	Used to separate individual keys. For example, Ctrl-D means holding down the Ctrl key while pressing the D key.
<i>Enter</i>	Used to refer to the key that generates a carriage return; the key is named Return on some keyboards.
<i>type</i>	Used to mean pressing one or more keys on the keyboard.
<i>enter</i>	Used to mean pressing one or more keys and then pressing the Enter key.

Special messages

This guide contains special messages that are described as follows:

Note

A note contains important information that helps you install or operate the system efficiently.

Caution

A caution contains instructions that you must follow to avoid damage to the equipment, a system crash, or loss of data.

System components

The SpinServer system comes with the following components preinstalled in equipment cabinets:

- ◆ Two SpinServer chassis to create a cluster, with additional SpinServers added in pairs
- ◆ For each SpinServer, two, three, or four FAS270c RAID disk enclosures, for a minimum of four RAID enclosures per SpinServer system
- ◆ For each FAS270c RAID enclosure, zero, one, or two DS14mk2 FC JBOD disk enclosures
- ◆ One UPS per SpinServer
- ◆ Two eight- or sixteen-port Brocade® SilkWorm® Fibre Channel switches

As shipped from the factory, the SpinServer system is in a minimum of two cabinets: the *server cabinet*, which contains SpinServers and their corresponding UPSs, and one or more *storage cabinets*, which contain FAS270c RAID enclosures, DS14mk2 FC JBOD enclosures, and Fibre Channel switches.

When working with SpinServer system equipment, follow all safety warnings and precautions as described in the *SpinServer 4100 Installation Guide*, *FAS270/270c Hardware and Service Guide*, *Fibre Channel DiskShelf14 Hardware Guide*, and *42U Cabinet Guide*.

Ethernet requirements

The SpinServer system requires Ethernet switches providing five ports for each SpinServer, two ports for each RAID enclosure, and one port for each switch. For instance, a SpinServer system consisting of two SpinServers, four FAS270c RAID enclosures, and two Ethernet switches requires 20 ports. Ethernet switches are not provided or preconfigured with the SpinServer system. See the *SpinServer 4100 Installation Guide* for a list of supported switches. At minimum, three subnets are required, one for each of the following purposes:

- ◆ A physically secure, dedicated network to connect to the two cluster ports on each SpinServer
- ◆ A physically secure network to connect to the management port on each SpinServer and to two management ports on each FAS270c RAID enclosure (one management port for each RAID controller)
- ◆ A general corporate network to connect to the two network ports on each SpinServer for access to client data

SpinServer documentation

For additional information on the tasks listed in this guide, see the following documentation:

- ◆ *SpinFS 2.5 Administration Guide*
- ◆ *SpinFS 2.5 Administration Reference*
- ◆ *SpinServer 4100 Installation Guide*
- ◆ *SpinFS Release Notes*
- ◆ Data ONTAP™ 6.5.2 documentation set
- ◆ *FAS270/270c Hardware and Service Guide*
- ◆ *Fibre Channel DiskShelf14 Hardware Guide*
- ◆ *42U System Cabinet Guide*

SpinServer and SpinFS® documentation can be accessed from the SpinManager™ GUI or from the software CD-ROM. To access the documentation from the CD-ROM, open the *root_directory*/SpinDocs/index.html file in a web browser, where *root_directory* is the root directory of the CD-ROM.

Data ONTAP, FAS270c, DS14mk2 FC, and cabinet documentation is available from the NetApp® on the Web (NOW) site (now.netapp.com).

All SpinServer and related documentation is available from the NOW site.

Purpose

Before installing SpinServer software, you must obtain configuration information from your network administrator. Use the following tables to gather the information that is needed during the configuration process.

SpinServer Configuration Information

The following information is needed for each of the SpinServers in your cluster.

Note_____

The SpinServer ID cannot be changed after you have entered it during the initial software installation process.

SpinServer ID	
Management IP address (if not using DHCP)	
Management netmask (if not using DHCP)	
Management default gateway IP address (if not using DHCP)	
Management primary name server (if not using DHCP)	
Server IP address 1	
Server netmask 1	
Server IP address 2 (optional)	
Server netmask 2 (optional)	
Cluster IP address 1	
Cluster IP address 2 (optional)	
Cluster netmask	
Cluster broadcast	

NFS Client Configuration Information

If your SpinServer system is deployed in an environment with NIS, you can configure the domain on the SpinServer with the following information to take advantage of NIS.

NIS domain name	
NIS server	

CIFS Client Configuration Information

The following information is needed to enable the CIFS protocol on your SpinServer system.

CIFS domain name or ID	
CIFS domain's WINS server IP address	
CIFS domain's primary domain controller (PDC) name	
CIFS domain's PDC IP address	
CIFS domain's backup domain controller (BDC) name	
CIFS domain's BDC IP address	
Virtual server name or ID	
Visible domain names or IDs	
NetBIOS name	
Node type	
Share name or ID	
Share's directory path	

Purpose

The cables needed for connecting SpinServer system components to one another and to the subnets are described in this chapter. Proper system connectivity is needed for successful software installation and component configuration. This chapter also describes the required power connections.

Attaching system cables

Preconfigured connections

The following connections are preconfigured at the factory:

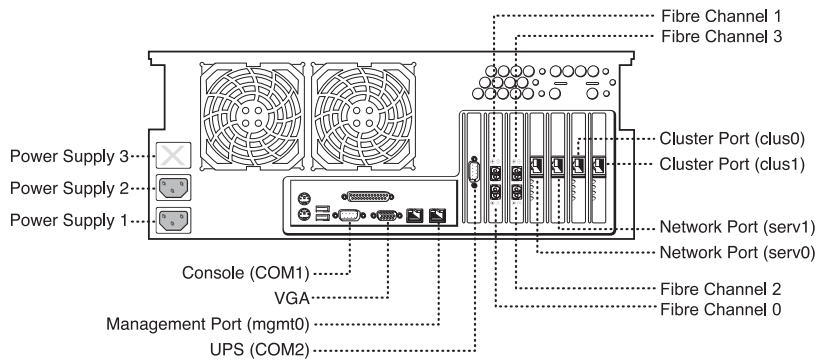
- ◆ UPS—The SpinServer COM2 port is connected to the APC UPS Computer Interface Port.
- ◆ RAID enclosures—Each FAS270c RAID enclosure is connected to a Fibre Channel switch with optical Fibre Channel cables.
- ◆ JBOD enclosures—Each DS14mk2 FC JBOD enclosure is connected to a FAS270c RAID enclosure with copper Fibre Channel cables.

Required connections

Make the following connections to SpinServer system components:

- ◆ Console—Connect the SpinServer console port (COM1) to a console, configured for ANSI-9600-8N1, by null modem cable.
- ◆ Management, client, and cluster subnets—Connect these ports by Ethernet cables to the appropriate Ethernet switches. See the following illustration of the management, client, and cluster ports.
- ◆ Tape devices—To attach a tape device to the SpinServer system, connect an unused Fibre Channel port on the SpinServer to a Fibre Channel bridge with a Fibre Channel cable. Attach the tape device to the Fibre Channel bridge with a Fibre Channel cable. If the tape device is a Fibre Channel library, a bridge is not required. A tape library can also be attached to a Fibre Channel switch.
- ◆ Server cabinet and storage cabinets—Fibre Channel connections must be made between the server cabinet and storage cabinet or cabinets, as described in “[Connecting server and storage cabinets](#)” on page 10.

SpinServer ports and connections are shown in the following illustration.



Connecting server and storage cabinets

Preconfigured Fibre Channel connections

The RAID and JBOD enclosures and Fibre Channel switches within each storage cabinet are connected at the factory.

Required Fibre Channel connections

You need to connect the SpinServers in the server cabinet to the Fibre Channel switches in the corresponding storage cabinet. The SpinServers and their corresponding Fibre Channel switches are marked with matching colored label. For instance, in a system that includes four SpinServers and two storage cabinets, the lower two SpinServers and the switches in the corresponding storage cabinet might be marked with blue labels, and the upper two SpinServers and the switches in the other storage cabinet might be marked with red labels. Use optical Fibre Channel cables to connect the SpinServers and the Fibre Channel switches that have matching colored labels.

Make the following connections to complete the Fibre Channel cabling for the SpinServer system. See the previous illustration for the location of the SpinServer’s Fibre Channel ports.

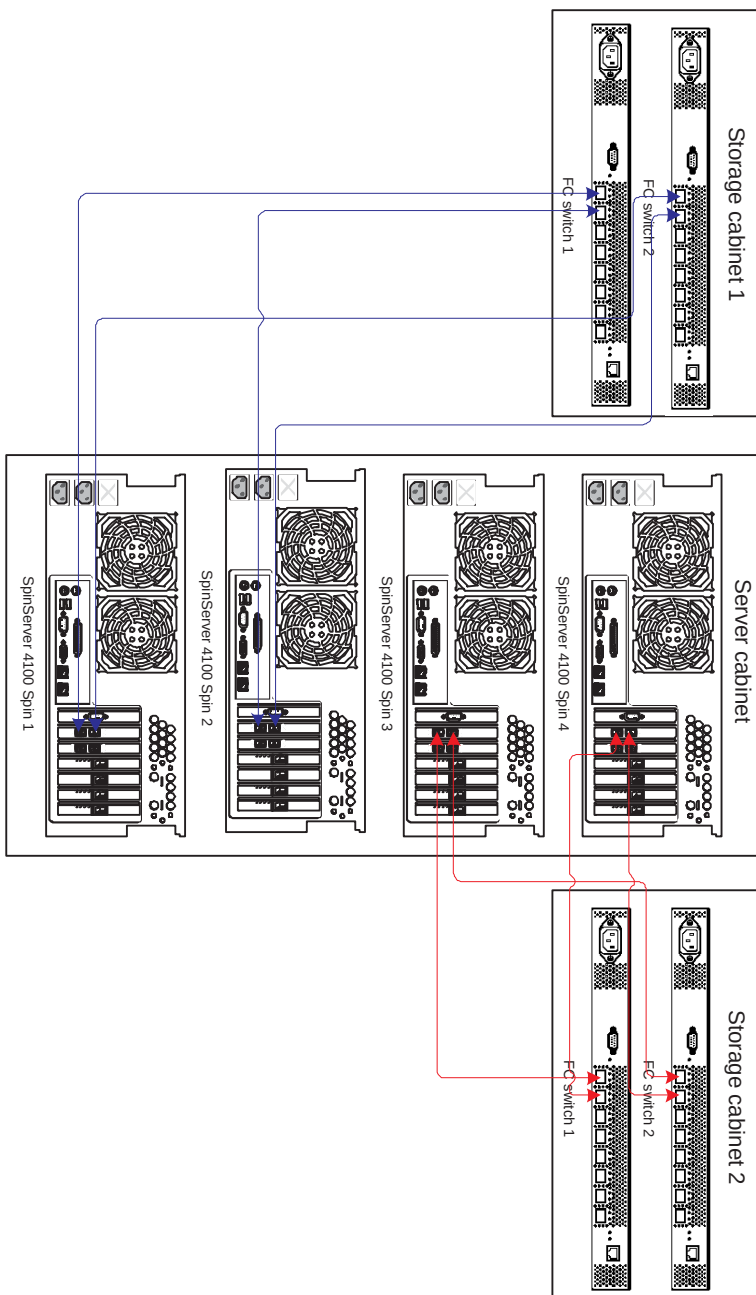
		SpinServer 4100 Spin 1 (lowermost)		SpinServer 4100 Spin 2 (second lowest)	
Storage cabinet 1		FC 0	FC 1	FC 0	FC 1
FC switch 1 (lower)	Port 0	X			
	Port 1			X	
FC switch 2 (upper)	Port 0		X		
	Port 1				X

If the SpinServer system includes a server cabinet with four SpinServers and a second storage cabinet, make the following additional connections.

		SpinServer 4100 Spin 3 (third lowest)		SpinServer 4100 Spin 4 (uppermost)	
Storage cabinet 2		FC 0	FC 1	FC 0	FC 1
FC switch 1 (lower)	Port 0	X			
	Port 1			X	
FC switch 2 (upper)	Port 0		X		
	Port 1				X

If the SpinServer system includes additional server and storage cabinets, connect the SpinServers in each server cabinet to the Fibre Channel switches in the corresponding storage cabinet or cabinets in the same manner.

The following figure shows the Fibre Channel connections that need to be made between the SpinServers in the server cabinet and the Fibre Channel switches in the storage cabinet or cabinets. The figure shows SilkWorm 3200 switches.



Attaching power cords

Power connections

The power connections for the SpinServers and the RAID and JBOD enclosures must provide power redundancy for these system components, as follows:

- ◆ RAID and JBOD power connections—For each RAID and JBOD enclosure, connect the two power cords to AC power outlets on different circuits.
- ◆ SpinServer power connections—Each SpinServer has its own UPS. Connect each SpinServer to the AC power outlet on its UPS.

Note

Connect only the SpinServer to the UPS. Do not connect any other equipment to the UPS.

Caution

The SpinServer power cord must be connected to the same UPS that is connected to the SpinServer's COM2 port. Incorrect connections can result in the loss of data.

Connecting the UPS battery cables

Connect the internal battery cables for the UPS as described in the *APC Smart-UPS User Manual*. The UPS cannot function until its battery cables are connected.

Purpose

This section describes initializing the SpinServer system. You must initialize the system before configuring it for client data access.

Overview of initialization

Initialization involves the following general steps:

1. Turning on system components
2. Installing SpinFS on the SpinServers
3. Optionally, resetting the administrative and root password on each SpinServer

Turning on system components

Turn on the SpinServer system components in the following order:

1. UPS
2. DS14mk2 FC JBOD enclosures
3. FAS270c RAID enclosures
4. SpinServer

Note

During the power-up sequence for the SpinServer, place the SpinFS software installation CD-ROM into the CD-ROM drive. From the console, you can monitor the SpinServer startup sequence as it progresses.

Installing SpinFS

Purpose

This section describes the initial installation of the SpinFS software on the SpinServer.

Caution

You specify the SpinServer ID when you initially install SpinFS. The SpinServer ID can be an IP address (for instance, 10.1.1.14) or a name (for the examples used in this document, Server1). The name or ID of the SpinServer is propagated from the initial installation of the software into the SpinManager management framework. To prevent confusion and potential loss or misplacement of data, the SpinServer IDs you choose must be orderly and easily recognizable by all system administrators who maintain the SpinServer system. Any naming system can be chosen for your SpinServer system, *but the IDs for the SpinServers must be unique within a cluster*. After the ID for a SpinServer has been set, you cannot modify the server name, server ID, or host name. To do so invalidates the failover port designations for the SpinServer and can result in the loss of data.

Note

To assure that all system components work together properly, one cluster port must be configured even if only a single SpinServer is being configured as a cluster. Even if you intend to use only one of the cluster ports, NetApp strongly recommends that you configure both cluster ports during the initial installation of SpinFS.

Installing the software

Perform the following steps to install SpinFS.

Note

If you are configuring the SpinServer's management port with a static IP address, you must enter all IP addresses manually, and you need to have them available before you begin the installation process. This is the information that you entered into the table in "[SpinServer Configuration Information](#)" on page 4.

Step	Action
1	If the SpinServer is on, turn it off by pressing and holding the power button until the LEDs on the front panel power supply turn red. This takes about five seconds.
2	When the SpinServer is off, press and release the power button one time to turn it on again and to begin the SpinServer startup sequence. Place the SpinFS CD-ROM into the CD-ROM drive. Monitor the initialization process from the serial console. Note _____ Ensure that the CD-ROM is in place before the SpinServer searches for its boot drives. Result: The Welcome screen displays the End User License Agreement.
3	Page through the screens of the End User License Agreement by following the instructions at the bottom of each screen. For example, to read the second End User License Agreement screen, press Ctrl-F 2.
4	After the final End User License Agreement screen, the following message is displayed: Installing the Spinnaker software constitutes acceptance of the End User License Agreement and will cause all data on the local disk drives to be destroyed. Please enter install to begin the install process. Enter install to continue the installation process. Result: On-screen messages indicate that the system is formatting file systems, installing software packages, and completing other procedures for configuring the system.

Step	Action
5	When the SpinServer restarts and ejects the CD-ROM, remove the CD-ROM from the drive. Caution_____ The SpinFS CD-ROM must be removed from the drive before installation proceeds. If the SpinServer loses power and the CD-ROM is in the drive, the SpinServer installation process can restart when power to the SpinServer is restored. If the installation of the software is restarted and completed, all data that is stored on the SpinServer is lost.
6	Enter the clock settings. Select the settings for your region and tab to OK. Press the space bar. Note_____ The default setting for the hardware clock is Greenwich Mean Time (GMT). Do not change this setting.
7	The installation process prompts you for the name or ID of the SpinServer. Type the SpinServer ID into the Hostname field, tab to OK, and press the space bar.
8	Configure the SpinServer's management port. If the management port is to be configured with DHCP, tab to OK and press the space bar. If you are manually entering the network configuration information, complete the fields with the configuration information provided by your network administrator. When finished, tab to OK and press the space bar.
9	At the end of the installation process, the SpinServer displays the login: prompt. At the prompt, enter admin. At the Password: prompt, type admin.

Note_____

After the initialization process, the SpinServer shows local disk activity for several minutes as it mirrors its SCSI drives. This is normal behavior and does not interfere with the configuration or operation of the SpinServer system.

Changing the administrative password

After the initial installation of SpinFS on the SpinServer, you can change the administrative password by performing the following steps.

Step	Action
1	Use secure shell (SSH) to log in as root with the password admin .
2	Enter the following command to enter a new password for the admin account: <code>passwd admin</code>
3	Enter the new password a second time to confirm the password.

Changing the root password

After the initial installation of SpinFS on the SpinServer, you can change the root password by performing the following steps.

Step	Action
1	Use secure shell (SSH) to log in as root with the password admin .
2	Enter the following command to enter a new password for the root account: <code>passwd root</code>
3	Enter the new password a second time to confirm the password.

Purpose

This section provides an example configuration for the SpinServer system. This example is for a mixed NFS and CIFS environment. The example uses the SpinManager GUI for each configuration task. See the *SpinFS 2.5 Administration Guide* for more information about SpinManager and these procedures. Check the current version of the *SpinFS Release Notes* for any revisions to these procedures.

Note

The IP addresses, names, and IDs that are used in this section are examples that are given for each configuration task. The IP addresses, names, and IDs for your system are different; see the information you collected in “[SpinServer Configuration Information](#)” on page 4. The parameters for different tasks can also differ, depending on your site’s requirements.

Logging in to the GUI

Log in to the GUI by opening a Web browser and entering the URL of one SpinServer. At the Login ID: prompt, enter **admin**. At the Password: prompt, enter **admin** or the password that you set in “[Changing the administrative password](#)” on page 20.

Creating a new cluster

Every SpinServer is part of a cluster, and although the cluster can contain only a single SpinServer, every SpinServer must be entered into a cluster before any other system management task is performed. To create a new cluster with the first SpinServer, select SpinServers and run Create Cluster. Enter the following information to complete the task:

- ◆ Cluster name: **Cluster1**
- ◆ Primary IP address: **192.168.66.1**
- ◆ Primary netmask: **255.255.0.0**
- ◆ Primary broadcast: **192.168.255.255**
- ◆ Primary MTU: **9000**
- ◆ Secondary IP address (optional): **192.168.66.2**
- ◆ Secondary netmask (optional): **255.255.0.0**
- ◆ Secondary broadcast (optional): **192.168.255.255**
- ◆ Secondary MTU (optional): **9000**

Caution

The Create Cluster command must not be used for any purpose other than to create a new cluster. If you mistakenly run the command in an attempt to add a SpinServer to an existing cluster, you must reinstall SpinFS on the SpinServer or completely delete all configuration data to undo the operation. Before you reinstall SpinFS or delete any configuration information, contact Network Appliance Technical Support.

Adding the second SpinServer to the cluster

To add the second SpinServer to the cluster, select SpinServers, run Join Cluster, and enter the following information:

- ◆ IP address of existing node in cluster: 192.168.66.1
- ◆ Primary IP address: 192.168.66.3
- ◆ Primary netmask: 255.255.0.0
- ◆ Primary broadcast: 192.168.255.255
- ◆ Primary MTU: 9000
- ◆ Secondary IP address (optional): 192.168.66.4
- ◆ Secondary netmask (optional): 255.255.0.0
- ◆ Secondary broadcast (optional): 192.168.255.255
- ◆ Secondary MTU (optional): 9000

Verifying LUNs

Logical unit numbers (LUNs) are preconfigured on the FAS270c RAID enclosures and DS14mk2 FC JBOD enclosures. When you configure a SpinServer system, the LUNs on the FAS270c enclosures must be visible to the SpinServers as storage units. To verify that the LUNs are visible as storage units, select Storage Pools > Storage Units. If storage units (LUNs) are not listed, force the discovery of the LUNs by selecting System > Hardware > Fibre Channel, then selecting each channel and running LIP Reset. Alternatively, restart the SpinServer by selecting SpinServers and running Reboot SpinServer.

If the LUNs are not visible after you have issued LIP resets and restarted the SpinServer, select System > Hardware > Fibre Channel and verify that the listed Fibre Channel port names match the initiator group (igroup) definitions displayed by the `fcpl show initiator` command on the FAS270c RAID enclosures. See the *Data ONTAP Block Access Management Guide for FCP* for more information.

Note

The FAS270c RAID enclosures are preconfigured to use RAID level 4. If you want to use RAID Double Parity (DP), you must delete the preconfigured volumes and LUNs and create new volumes and LUNs. See the *Data ONTAP Block Access Management Guide for FCP* and *Data ONTAP Storage Management Guide* for information.

Creating a storage pool

A single storage unit represents a single external RAID set or a single LUN that has been created on a storage device. A storage pool is a logical grouping of one or more storage units.

To create a storage pool, select Storage Pools > Storage Pools and run New with the following information:

- ◆ Device ID (storage pool name): **sp1**
- ◆ Layout: **stripe**
- ◆ Free space alarm threshold (%): **5**
- ◆ Storage units: **su1**
- ◆ Home server: **Server1**

Note

Depending on the number of physical disks that are included in the storage units that are being used, this command can take several minutes to complete.

NetApp recommends that you create storage pools from sequentially numbered LUNs to optimize performance. For example, consider a system with two SpinServers and 24 LUNs, numbered 0 through 23. If you create one storage pool on each SpinServer, assign the LUNs as follows:

- ◆ Storage pool A (SpinServer 1): LUNs 0 through 11
- ◆ Storage pool B (SpinServer 2): LUNs 12 through 23

If you create two storage pools on each SpinServer, assign the LUNs as follows:

- ◆ Storage pool A (SpinServer 1): LUNs 0 through 5
- ◆ Storage pool B (SpinServer 1): LUNs 6 through 11
- ◆ Storage pool C (SpinServer 2): LUNs 12 through 17
- ◆ Storage pool D (SpinServer 2): LUNs 18 through 23

Specifying a NIS domain

NIS domains are used to support NFS clients. To specify a NIS domain, select SpinAccess > NFS > NIS Domains and run New with the following information:

- ◆ NIS domain name: **acmebricks.com**
- ◆ Domain servers: **10.2.2.1, 10.3.3.1**

Defining a CIFS domain

CIFS domains are used to support CIFS clients. Windows NT 4.0, Windows 2000, and Windows 2003 CIFS domains are supported. Add any domains that CIFS users need to access the SpinServer. To create a CIFS domain, select SpinAccess > CIFS > Domains and run New with the following information:

- ◆ Domain name: **ENG**
- ◆ WINS server: **10.1.1.116**
- ◆ Primary domain controller (PDC) name: **STORM**
- ◆ PDC IP address: **10.1.1.116**
- ◆ Kerberos configuration name: **None**
- ◆ Backup domain controller (BDC) 1 name (optional): **RAIN**
- ◆ BDC 1 IP address (optional): **10.1.1.118**
- ◆ BDC 2 name (optional):
- ◆ BDC 2 IP address: (optional)
- ◆ BDC 3 name (optional):
- ◆ BDC 3 IP address (optional):
- ◆ BDC 4 name (optional):
- ◆ BDC 4 IP address (optional):

Note

To configure a CIFS domain at this point, it is assumed that the PDC's IP address is on the same subnet as the SpinServer's management port (mgmt0). If the PDC's subnet is the same as the subnet connected to the SpinServer's network ports (serv0 and serv1), then a virtual server and a bound virtual interface must first be configured for the subnet. See "[Creating a virtual server](#)" and "[Creating a virtual interface](#)" for details.

Creating a virtual server

A virtual server represents a distinct file-system name space with distinct network access and provides the same flexibility and control as a dedicated server. To create a virtual server and set an NFS user and group identity as the owner of its root directory, select Virtual Servers > Servers and run New with the following information:

- ◆ Virtual server name: **vs1**
- ◆ Storage pool for root virtual file system (VFS): **sp1**
- ◆ Enable SpinAuth: **false**
- ◆ Enable floating superusers: **false**
- ◆ Minimum authentication level: **none**
- ◆ Export ruleset name: **default_ruleset**
- ◆ Virus scan for RW VFS: **false**
- ◆ Virus scan for RO VFS: **false**

Creating a virtual interface

A virtual server provides access to a set of virtual file systems (VFSs) through a set of virtual interfaces. To create a virtual interface, select Interfaces > Configuration and run New with the following information:

- ◆ SpinServer ID: **Server1**
- ◆ Virtual interface name: **if1**
- ◆ Physical port for interface binding: **serv0**
- ◆ IP address assigned to the virtual interface: **10.1.1.140**
- ◆ Netmask assigned to the virtual interface: **255.255.255.0**

Binding the virtual interface to the virtual server

Each virtual interface must be bound to a virtual server to enable access to the virtual server's VFSs. To bind the virtual interface to the virtual server, select Virtual Servers > Servers, select the virtual server, and run Bind Network Interface with the following information:

- ◆ SpinServer ID: **Server1**
- ◆ Network interface: **if1**

Associating a NIS domain with a virtual server

To associate a NIS domain with a virtual server to enable NFS client access, select SpinAccess > NFS > Servers and run New with the following information:

- ◆ Virtual server: **vs1**
- ◆ NIS domain name: **acmebricks.com**
- ◆ Kerberos realms: **None**

Creating a CIFS server

Prior to configuring the virtual server for CIFS client access, create a valid computer account for the SpinServer in the CIFS domain. Include all trusted domains in the visible domain list. Use one of the following methods to create the SpinServer's account:

- ◆ For Windows NT 4.0, use Server Manager.
- ◆ For Windows 2000 and later, open the Active Directory, select NEW > Computer, add the SpinServer, and select the "Allow pre-Windows 2000 computers to use this account" check box.

To create a shared CIFS server for CIFS client access, select SpinAccess > CIFS > Servers and run New with the following information:

- ◆ Virtual server: **vs1**
- ◆ NetBIOS name: **NB0**
- ◆ Domain name: **ENG**
- ◆ Visible domains: **MARKETING, ENG**
- ◆ Node type: **M**
- ◆ Kerberos enabled: **no**
- ◆ Kerberos privileged user (optional):
- ◆ Kerberos privileged password (optional):

Enabling two-node high availability

A high-availability (HA) configuration ensures that data remains available in the event of a SpinServer failure. To enable high availability, select Cluster > Configuration and run Enable 2-node HA Mode.

Creating a virtual file system

A virtual file system (VFS) is the primary unit of storage management for a SpinServer system. To create a VFS, select File Storage > Virtual File Systems and run New with the following information:

- ◆ VFS name: **vfs1**
- ◆ Virtual server: **vs1**
- ◆ Mount type: **context**
- ◆ Mount path: **/vfs1**
- ◆ Minimum quota (MB): **5000**
- ◆ Maximum quota (MB): **10000**
- ◆ Free space alarm threshold (%): **10**
- ◆ Storage pool: **sp1**
- ◆ User type of root FID: **NFS**

- ◆ Domain of root FID: **acmebricks.com**
- ◆ User of root FID: **user1**
- ◆ Group of root FID: **group1**
- ◆ Export ruleset name: **default_ruleset**
- ◆ Virus scan for RW: **false**
- ◆ Virus scan for RO: **false**
- ◆ Show SpinShot directory: **true**
- ◆ Restricted ACL: **false**

Note

The User type of root FID field has four options: SPIN, NFS, CIFS, and NFS-Kerberos. Use the SPIN user type if an NFS or CIFS domain is not configured or available. If you create an NFS- or CIFS-enabled virtual server or VFS, a NIS or CIFS domain must already be configured on the SpinServer. The CIFS user type is used only for CIFS or mixed-protocol (NFS and CIFS) environments. The NFS-Kerberos user type assigns the ownership of the VFS to the user that is mapped to the Kerberos principal name specified by the value of the User of root FID field. The NFS user type is used in this example.

Creating a CIFS share

A CIFS share is required for users to share data by using the CIFS protocol. To create a CIFS share, select SpinAccess > CIFS > Shares and run New with the following information:

- ◆ Virtual server: **vs1**
- ◆ Share name: **share1**
- ◆ Path: **/vfs1**
- ◆ Share properties: **oplocks**
- ◆ Directory mode bits (optional):
- ◆ File mode bits (optional):
- ◆ Remark (optional):

Setting up a CIFS-to-NFS mapping

CIFS-to-NFS mappings are required to enable users to access data by using both the NFS and CIFS protocols. To set up a CIFS-to-NFS mapping, select SpinAccess > CIFS-NFS Mapping and run New with the following information:

- ◆ Virtual server: **vs1**
- ◆ Mapping type: **USER**
- ◆ CIFS pattern: **ENG\\(.+)**

- ◆ CIFS pattern replacement: \1
- ◆ NFS pattern: (.+)
- ◆ NFS pattern replacement: **ENG**\\1

Note

For information about regular expressions, see your UNIX system administration documentation, the online UNIX documentation for `sed` or `regex`, or *Mastering Regular Expressions*, published by O'Reilly and Associates.

**Performing
additional
configuration tasks**

Additional configuration tasks can include the following:

- ◆ Adding default routes to virtual interfaces and virtual servers
- ◆ Setting up SpinShots™ and mirrors of VFSs
- ◆ Setting up security with Kerberos authentication, export rule sets, and pluggable authentication modules (PAM)
- ◆ Setting up the SpinServer system to notify you of critical events via e-mail
- ◆ Configuring backup and restoration products

For information on performing these and other tasks, see the *SpinFS 2.5 Administration Guide*.