

Data ONTAP™ Software 5.3

First-Time Configuration

Using the Setup Command

Network Appliance, Inc.
2770 San Tomas Expressway
Santa Clara, CA 95051, USA
Tel: +1 408 367-3000
Fax: +1 408 367-3151
Support tel: (888) 4-NETAPP
Support: <http://www.netapp.com/support/form.html>
Information email: info@netapp.com
Web: <http://now.netapp.com>
Part number 210-02343
March, 1999

Copyright and trademark information

Copyright information

Copyright © 1999 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

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.

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 and purchase of this product do 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

Network Appliance, NetCache, Data ONTAP, SmartSAN, SnapCopy, SnapMirror, SnapRestore, Snapshot, WAFL, Web Filer, FilerView, BareMetal, and SecureShare are trademarks of Network Appliance, Inc. FAServer, NetApp, and the Network Appliance logo are registered trademarks of Network Appliance, Inc.

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

Communications regulation information

Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the users will be required to correct the interference at their own expense.

Cables

To maintain compliance with applicable emission standards, use cables shielded with metallic RFI/EMI connector hoods on this device.

Canada notice

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of the Canadian Department of Communications.

Avis Canadien

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

BZT Hinweis

Hiermit wird bescheinigt, daß dieses Gerät in Übereinstimmung mit den Bestimmungen der BAPT-AmtsblVfg 243/1991 funktentstört ist. Der vorschriftsmäßige Betrieb mancher Geräte (z.B. Meßsender) kann allerdings gewissen Einschränkungen unterliegen. Beachten Sie deshalb die Hinweise in der Bedienungsanleitung.

Dem Bundesamt für Zulassungen in der Telekommunikation wurde das Inverkehrbringen dieses Gerätes angezeigt und die Berechtigung zur Überprüfung der Serie auf die Einhaltung der Bestimmungen eingeräumt.

Safety warnings

Failure to follow the directions contained in the following statements could result in bodily harm or loss of life.

- ◆ To reduce the risk of personal injury from hot surfaces, allow the internal components time to cool before touching or installing options.
- ◆ To reduce the risk of personal injury or damage to the equipment, ensure that the equipment is properly supported or braced when installing options.
- ◆ This equipment is designed for connection to a grounded outlet. The grounding type plug is an important safety feature. To avoid the risk of electrical shock or damage to the equipment, do not disable this feature.
- ◆ This equipment is furnished with one or more lithium batteries. There is a danger of explosion and risk of personal injury if the battery is incorrectly replaced or mistreated. Do not attempt to recharge the battery, disassemble it, or dispose of it in a fire.

Electrical safety considerations

High leakage current cautions

CAUTION:

HIGH LEAKAGE CURRENT
EARTH CONNECTION ESSENTIAL
BEFORE CONNECTING SUPPLY

WARNUNG:

HOHER ABLEITSTROM
Vor inbetriebnahme
Erdungsverbindung herstellen

ATTENTION:

COURANT DE FUITE ÉLEVÉ
Raccordement à la terre indispensable
avant le raccordement au réseau

Disconnecting power cautions

CAUTION:

UNIT IS PROVIDED WITH TWO POWER CORDS. TO DISCONNECT ALL
POWER FROM THE UNIT, REMOVE BOTH POWER CORDS.

WARNUNG:

DAS GERÄT IST MIT ZWEI NETZKABELN AUSGERÜSTET. ZUR
SICHEREN TRENNUNG DES GERÄTES VOM NETZ. MÜSSEN BEIDE
NETZKABEL GEZOGEN WERDEN.

ATTENTION:

CET APPAREIL COMPORTE PLUS D'UN CORDON D'ALIMENTATION.
AFIN DE PRÉVENIR LES CHOCS ÉLECTRIQUES. DÉBRANCHER LES
DEUX CORDONS D'ALIMENTATION AVANT D'EFFECTUER LE
DÉPANNAGE.

Table of Contents

Chapter 1	Welcome	1
	About this guide	1
Chapter 2	Configuration Instructions	3
	Overview	3
	Using DHCP with an F700 series filer	7
	Configuring the filer(s)	8
	Verifying network connections	10
Chapter 3	Configuring HTTP on the Filer	11
	HTTP configuration information	11
Chapter 4	Setting Up Password and Group Files	13
	Password and group information	13
Chapter 5	Configuring Access to CIFS Shares	19
	Assigning access rights	19
Chapter 6	Configuring Clients to Access the Filer	23
	NFS and CIFS client configuration	23
	Configuring NFS clients	24
	Configuring CIFS clients	27
Chapter 7	Installing SecureShare	29
	About SecureShare	29
	Installing SecureShare Access	30
	Installing SecureShare Account Migrator	31

Chapter 8	Cluster Configuration Check.	33
	Checking the cluster filer configuration	33
Chapter 9	About the Filer Software	35
	Filer software description.	35
Chapter 10	Using FilerView	37
	Administering from a Web-based tool	37
Appendix A	Time zones	41
	Time zone selection.	41
Appendix B	Worksheets.	47
	Introduction.	47
	Worksheet 1: Host name and interfaces	49
	Worksheet 2: Administration host	59
	Worksheet 3: Time zone	61
	Worksheet 4: DNS and NIS information.	63
	Worksheet 5: Password.	65
	Worksheet 6: Disks	67
	Worksheet 7: CIFS information	69
Appendix C	Preparing for CIFS Configuration.	73
	CIFS information needed.	73
	Deciding on a domain or workgroup configuration	74
	Choosing between PC-style or UNIX-style permissions.	77
	Adding the filer to a Windows NT domain.	79
Appendix D	Installing the Hardware.	81
	Prerequisites	81

Setting up your cluster 82

Cabling a cluster in a system cabinet 84

Configuring your cluster for an equipment rack 86

Cabling a cluster in an equipment rack 96

Cabling a minimum cluster configuration in an equipment rack 98

Cabling a maximum cluster configuration in an equipment rack 104

About this guide

How to use this guide

Welcome to *First-Time Configuration Using the Setup Command*.

Use this guide to get your new NetApp® filers configured and operating from the console using the **setup** command.

Is this the right guide for you?

If you are installing new filers, this is the correct guide for you. If you are not installing new filers, use the following table to decide which guide to read.

If you are...	Read...
Configuring a new NetApp filer using the Web-based Setup Wizard	<i>First-Time Configuration Using the Setup Wizard</i>
Upgrading an existing filer to the Data ONTAP 5.3 software	<i>Software and Firmware Upgrade Guide</i>
Converting existing NetApp F630 or F700 series filers into a cluster	<i>Cluster Conversion Guide</i>

Audience

This guide is for system administrators who are familiar with networking concepts, such as host names, Internet Protocol (IP) addresses, Network File System (NFS) exports, and Common Internet File System (CIFS) shares. If you are not familiar with these concepts, you might need assistance to complete the initial filer configuration.

Cluster filer configuration

When you configure filers in a clustered environment, parameters, configuration files, all licenses, and network interfaces must match. In this way, when one filer takes over the failed filer, it appears the same as the failed filer. Keep the following items in mind during the filer configuration; these items should match on both filers to create a successful cluster:

- ◆ **options** command parameters
- ◆ Licenses, such as CIFS, Cluster, HTTP, and NFS

Licenses must match on both filers; you must purchase a separate license for each filer.

- ◆ The following configuration files must have identical contents:
 - ❖ */etc/resolv.conf*
 - ❖ */etc/httpd.mimetypes*
 - ❖ */etc/dgateways*
 - ❖ */etc/nsswitch.conf*

Overview

The configuration process

The following table describes the process for configuring a new filer (or new clustered filers) for the first time. Shaded cells in the table indicate procedures that are optional depending on the filer options that you purchased.

Stage	What you do	Details
1	Set up DHCP.	If you purchased an F700 series filer (or clustered filers) and you want to use the Dynamic Host Configuration Protocol (DHCP) to configure the filer's onboard interface (e0), follow the instructions in "Using DHCP with an F700 series filer" on page 7. Using DHCP to assign an IP address to an F700 series filer enables you to use a Telnet client to complete the first-time configuration, rather than having to attach a serial console to the filer to complete the configuration.
2	Cable filers in a cluster.	If you purchased filers as a cluster, the filers and disk shelves need to be cabled together according to the instructions in Appendix D, "Installing the Hardware," on page 81 .

Stage	What you do	Details
3	Complete the worksheets.	The worksheets in Appendix B, “ Worksheets ,” on page 47 describe all the information that you are asked to enter to configure your filers.
4	Add the filer to a Windows NT domain.	If you purchased a license for the CIFS protocol for your filer and you plan to add the filer to a Windows NT domain, follow the instructions in “ Adding the filer to a Windows NT domain ” on page 79.
5	Configure the filer.	Configure your filer according to the instructions in “ Configuring the filer ” on page 8.
6	Verify the filer’s network connections.	Verify that the filer is communicating on the network by following the instructions in “ Verifying network connections ” on page 10.
7	Configure HTTP service.	If you purchased a license for the HTTP protocol for your filer, configure the HTTP options as described in Chapter 3, “ Configuring HTTP on the Filer ,” on page 11.
8	Set up password and group files.	If you purchased a license for the CIFS protocol for your filer and you are not using a Windows NT domain controller to authenticate users, configure password and group files according to the instructions in Chapter 4, “ Setting Up Password and Group Files ,” on page 13.

Stage	What you do	Details
9	Configure CIFS shares.	If you purchased a license for the CIFS protocol for your filer, configure CIFS shares so that users can access directories on the filer.
10	Configure clients to access the filer.	You must configure clients according to the instructions in Chapter 6, “ Configuring Clients to Access the Filer ,” on page 23 so that they can access information on the filer.
11	Install the SecureShare™ program on CIFS clients.	If you purchased a license for the CIFS protocol for your filer, you can install the SecureShare program on Windows client machines according to the instructions in Chapter 7, “ Installing SecureShare ,” on page 29. This enables users to view and modify the UNIX permissions and attributes on files stored on the filer.
12	Check the configuration of clustered filers.	If you configured clustered filers, check the cluster configuration information according to the instructions in Chapter 8, “ Cluster Configuration Check ,” on page 33.
13	Learn about the Data ONTAP software.	Read Chapter 9, “ About the Filer Software ,” on page 35.

Stage	What you do	Details
14	Learn about FilerView	Read Chapter 10, “ Using FilerView ,” on page 37 to learn how to administer your filer using the FilerView Web-based administration tool.

Using DHCP with an F700 series filer

Description

Follow this procedure to use DHCP to assign a static IP address to the onboard interface (*e0*) on an F700 series filer during first-time configuration. This procedure enables you to use a Telnet client to access the filer and complete the first-time configuration, rather than having to attach a hard-wired console to the filer. When you use DHCP to assign an IP address to the onboard interface, the filer

- ◆ Obtains the address from the DHCP server when the filer is turned on
- ◆ Configures the onboard interface with the IP address
- ◆ Becomes accessible to a Telnet client or the Setup Wizard

Prerequisites

To use this procedure, you must have a DHCP server and an F700 series filer on the same network segment.

Steps

Complete these steps to use DHCP to assign an IP address to the onboard interface.

Step	Action
1	Locate the MAC address for the onboard interface by looking for a label on the back of the left side of the filer’s PCB carrier, if necessary.
2	Configure the DHCP server to return a static IP address for the interface based on the MAC address for the onboard interface. Caution— The DHCP server must return a static IP address for the interface. If the server returns a dynamic IP address, the filer displays an error message and continues to use the IP address permanently—which can result in an IP address conflict if the DHCP server assigns the IP address dynamically to other clients from time to time.

Configuring the filer

Description

This procedure describes how to configure your filer whether or not you use DHCP. Complete this procedure after you install your new filer. After you configure your filer, it is visible on your network and available for access by users from their client computers.

Note

If you are installing clustered filers, you must complete this procedure for each filer in the cluster.

Prerequisites

Before you start this procedure, you must

- ◆ Install the filer hardware and the serial console according to the instructions in your hardware guide if you are not using DHCP
- ◆ Complete steps 1 through 3 of the “[The configuration process](#)” on page 3

Steps

Complete these steps to configure a filer.

Step	Action
1	Turn on the filer’s power switch to begin the configuration process. The first time the filer boots ◆ If you followed the steps in “Using DHCP with an F700 Series filer,” the filer obtains an IP address for the e0 interface. ◆ It runs the <code>setup</code> command. Note If your filer is not in the F700 series, or if you decided not to use DHCP to configure the F700 series filer’s onboard interface, you must attach a serial console to the filer so that you can interact with the <code>setup</code> command.

Step	Action
2	Enter the information from the worksheets in Appendix B, “Worksheets,” on page 47. The setup program prompts you to enter the configuration information from the worksheets in the order that the worksheets are numbered.

Results

After you finish configuring the filer, it is on-line. The following directories exist on the filer:

/vol/vol0
/vol/vol0/home

Note

/vol is not a directory—it is a special virtual root path under which the filer mounts its volumes. You cannot mount */vol* to view all the volumes on the filer; you must mount each filer volume separately.

If you purchased a license for the NFS protocol, */vol/vol0* is exported to the administration host for root access; */vol0/home* is exported to the administration host for root access and to all clients for general access.

If you purchased a license for the CIFS protocol, */vol/vol0* is shared as C\$; only the system administrator with the root password has read and write access to the C\$ share. The */vol/vol0/home* directory is shared as HOME without access granted to anyone.

Verifying network connections

Use the ping command

After you configure the filer, you use the `ping` command from a client attached to the network to verify that the filer can communicate with other computers on the network.

Procedure

Complete these steps to verify filer communication.

Step	Action
1	At a client attached to the network, enter the following command: <code>ping hostname-interface</code> Replace the variable <i>hostname</i> with the host name that you assigned to the filer when you ran <code>setup</code>; replace the variable <i>interface</i> with one of the interface names that the filer assigned when you ran <code>setup</code>.
2	Repeat the test once for each interface that is installed in the filer.

Examples

The following examples test the network connections for a filer that has the host name *toaster* with two interfaces named *e0* and *f0* installed:

`ping toaster-e0`

`ping toaster-f0`

How to troubleshoot problems

If an interface does not respond to a `ping` command, make sure that

- ◆ The interface is securely attached to the network.
- ◆ The media type is set up correctly if the interface is using a multi-port Ethernet card with different port speeds.
- ◆ The routers function properly with correct routing information if the `ping` command is issued from a network not directly attached to the interface.

HTTP configuration information

About this chapter

This chapter contains instructions for configuring the filer to provide HTTP service. If you purchased a license for the HTTP protocol, follow the instructions in this chapter to configure HTTP service; otherwise, continue with [Chapter 4, “Setting Up Password and Group Files.”](#)

Prerequisites

Before configuring the filer to provide HTTP service, you must decide which directory path that the filer uses as the home directory for files to be accessed by HTTP clients.

The path name for the directory uses the following format:

/vol/volume_name/directory_name

For example, to use the */home/html_files* directory path on the *vol0* volume, you use the following path:

/vol/vol0/home/html_files

Procedure

Complete these steps to configure HTTP service.

Step	Action
1	At the filer console, enter the following command to enable the HTTP daemon: options httpd.enable on

Step	Action
2	Use the following command syntax to specify the root of the path that HTTP requests can use: <pre>options httpd.rootdir <i>pathname</i></pre> For example, if you want HTTP clients to gain access to files or subdirectories under <i>/vol0/home/html_files</i>, enter <pre>options httpd.rootdir /vol/vol0/home/html_files</pre> When Web browsers request files using HTTP, the filer delivers the files using the root directory. For example, if a browser requests the URL <i>http://toaster/demo/index.htm</i>, the filer sends the file <i>/vol0/home/html_files/demo/index.htm</i>.

Results

The filer is configured to respond to requests from Web browsers.

Password and group information

About this chapter

This chapter describes how to set up the *passwd* and *group* files on the filer so that the filer can authenticate users.

Who should use this chapter

You should use the information in this chapter if your filer is licensed for the CIFS protocol and does not use a Windows NT domain controller to authenticate users.

If your filer does use a Windows NT domain controller, skip this chapter and continue with [Chapter 5](#), “[Configuring Access to CIFS Shares](#).”

Location of the passwd and group files

The `setup` program created default *passwd* and *group* files in the `/etc` directory of the filer default volume.

How the filer uses the passwd and group files

The filer uses *passwd* and *group* files for the following purposes:

- ◆ To authenticate users for CIFS or (PC)NFS access and to translate user and group names in the `/etc/quotas` file to UIDs and GIDs

If the filer uses a Windows NT domain controller to authenticate CIFS users, the domain controller verifies the user's login name and password, and the filer verifies that the user has an entry in the *passwd* file.

If the filer uses the *passwd* file to authenticate NFS or CIFS users, the filer uses the encrypted password in the *passwd* file to verify the user's login name and password.

- ◆ To determine CIFS guest access

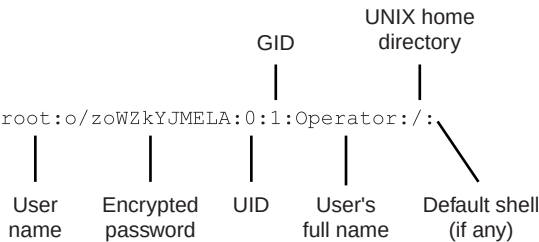
For additional information about guest access, see “Enabling guest access” in Chapter 7 of the *System Administrator's Guide*.

- ◆ To determine users' rights to access files

For information about how the filer uses the files to determine access rights in an environment with both NFS and CIFS users, refer to “Choosing the method for deciding access rights” in Chapter 7 of the *System Administrator's Guide*.

Default entry in the passwd file

The following illustration shows the default entry in the *passwd* file.

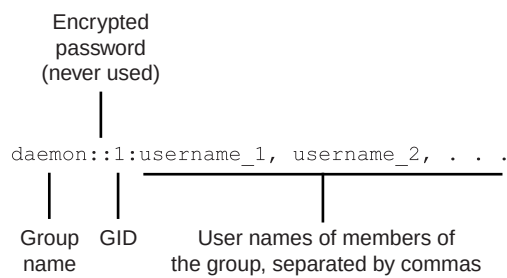


The following table describes the fields in an entry.

Field	Description
User name	Contains a user name for the user.
Encrypted password	Contains a password for the user. The filer disregards this field if NIS or a Windows NT domain controller is used to authenticate user names and passwords.
UID	Contains a unique integer that is the UID.
GID	Contains a unique integer that is the user's primary GID.
User's full name	Contains the user's full name. The filer ignores this field.
UNIX home directory	Contains the path of the user's home directory. The filer ignores this field.
Default shell	Contains the path of the user's default shell. The filer ignores this field.

Default entry in the group file

The following illustration shows the default entry in the *group* file.



The following table describes the fields in an entry.

Field	Description
Group name	Contains a unique group name.
Encrypted password	Contains a password. This field is never used, but should not be left blank if security is important.
GID	Contains a unique integer that is the GID.
User names	Contains a comma-separated list of user names that belong to the group.

Accessing the files from Windows NT and Windows 95 workstations

Complete the following steps to access the files from a Windows NT or Windows 95 workstation.

Step	Action
1	Map a drive to the root of the default filer volume using the following Universal Naming Convention (UNC) path; replace <i>filename</i> with the name of your filer: \\<i>filename</i>\C\$ If Windows displays a dialog box asking for a user name and a password ◆ Use Administrator as the user name. ◆ If you set up the filer to use a Windows NT domain controller to authenticate users, use the domain's administrator password. If you set up the filer to use the <i>passwd</i> file to authenticate users, use the administrator password that you entered when you ran setup.
2	Change to the <i>/etc</i> directory.

Accessing the files from UNIX/NFS clients

Complete the following steps to access the files from a UNIX/NFS client.

Step	Action
1	Mount the root of the default filer volume to the client's file system using the following path; replace <i>filename</i> with the name of your filer: <i>filename</i> : /vol/vol0
2	Change to the <i>/etc</i> directory.

Adding entries to the passwd file

The procedure you use to add entries to the */etc/passwd* file depends on whether you are using the */etc/passwd* file or either a Windows NT domain controller or NIS to authenticate users.

If you are using the */etc/passwd* file to authenticate users, follow the instructions in the next section, [“Adding entries to the passwd file with passwords.”](#)

If you are using either a Windows NT domain controller or NIS to authenticate users, follow the instructions in [“Adding entries to the passwd file without passwords”](#) on [page 17](#).

Adding entries to the passwd file with passwords

In this procedure, you add entries to a *passwd* file on a UNIX host using a text editor, then transfer the file to the filer. You add entries to the *passwd* file on a UNIX host because each entry in the file requires an encrypted password and the filer does not have a command for creating passwords. The format for entries in the *passwd* file is as follows:

```
username:password:uid:gid:full name:/:default shell
```

Complete the steps in the following table to add entries to a *passwd* file.

Step	Action
1	Log in to a UNIX host as the root user.
2	Change to the <i>/etc</i> directory.
3	Make a copy of the existing <i>passwd</i> file under a new name, such as <i>passwd.old</i> .
4	Open the existing <i>passwd</i> file in a text editor.

Step	Action
5	Add an entry for each user who needs access to files. Leave the password and default shell fields empty. You set passwords in Step 8. The filer does not use the default shell field.
6	If you did not purchase a license for the NFS protocol, delete any entries from the <i>passwd</i> file that are for non-CIFS users.
7	Save the file and exit the editor.
8	Set a password for each user by entering the following command: passwd <i>username</i> The passwd program prompts you to enter the new password twice.
9	Copy the <i>passwd</i> file from the UNIX host to the <i>/etc</i> directory on the filer.
10	Delete the <i>passwd</i> file from the UNIX host and rename the saved file to <i>passwd</i> .
11	Continue with “ Adding entries to the group file ” on page 18

Adding entries to the *passwd* file without passwords

In this procedure, you edit the *passwd* file from a Windows NT or Windows 95 workstation or a UNIX/NFS client using a text editor. The format for entries in the *passwd* file is as follows:

```
username:password:gid:uid:full name:default shell
```

Complete the steps in the following table to add entries to the *passwd* file.

Step	Action
1	Use a text editor to open the <i>/etc/passwd</i> file.
2	Add an entry for each user who needs to access files. Leave the password and default shell fields empty. The filer does not use them when users are authenticated by a Windows NT domain controller or NIS.
3	Save the file and exit the text editor.

Step	Action
4	Continue with “ Adding entries to the group file ” on page 18 .

Adding entries to the group file

In this procedure, you edit the *group* file from either a Windows NT or Windows 95 workstation or a UNIX/NFS client using a text editor. The format for entries in the *group* file is as follows:

```
groupname::gid:username, . . . , username
```

This procedure assumes that you already connected to the root filer volume using the instructions in one of the following sections:

- ◆ “[Accessing the files from Windows NT and Windows 95 workstations](#)” on page 15
- ◆ “[Accessing the files from UNIX/NFS clients](#)” on page 16

Complete the steps in the following table to edit the group file.

Step	Action
1	Use a text editor to open the <i>/etc/group</i> file.
2	Add entries to the file for each group.
3	Save the file and exit the text editor.

Results

The *passwd* and *group* files on the filer now contain entries for users and groups. The filer can verify users’ rights to access the filer.

Assigning access rights

About this chapter

This chapter describes how to assign users and groups access rights to CIFS shares (directories) using the `cifs` command; see the *System Administrator's Guide* for instructions about using Windows NT Server Manager to assign access rights. If you did not purchase a license for the CIFS protocol, continue with [Chapter 6, “Configuring Clients to Access the Filer.”](#)

Scope of shares access

The rights you assign to a share apply to the entire share; for example, if you assign a user rights to a share named HOME, the user gains rights to the directory specified by the HOME share and to all subdirectories under the directory. When you assign rights, they are recorded in the share ACL.

Introducing the `cifs` command

You use a specific form of the `cifs` command to grant users and groups access to CIFS shares. The command syntax is as follows:

```
cifs access share [-g] {user|group} rights
```

The command parameters are described in the following table.

Parameter	Description
<code>access</code>	Specifies that an access entry is to be created.
<code>share</code>	Specifies the name of the share.
<code>-g</code>	Specifies that the <code>user group</code> name is a group.
<code>user group</code>	Specifies the name of the user or group for which access to the share is granted.

Parameter	Description
rights	Specifies which rights the user or group have to the share. Rights are specified by three characters, <i>rwX</i>, which stand for read, write, and execute. A dash (-) in any position denies the user the right specified by the character it replaces. Examples: <i>rwX</i> grants read, write, and execute rights. <i>r--</i> grants only the right to read files. <i>rw-</i> grants only the rights to read and write files. <i>r-X</i> grants only the rights to read and execute files. Note— The <code>cifs access</code> command allows spaces for separating the rights.

Examples of the `cifs` command

The following table shows three example access entries created with the `cifs` command.

Description	Command example
Assign members of the group “marketing” read and execute rights to the HOME share.	<code>cifs access HOME -g marketing r-x</code>
Assign members of the group “engineering” read, write, and execute rights to the HOME share.	<code>cifs access HOME -g engineering rwX</code>
Deny the user “cyoung” all rights to the HOME share.	<code>cifs access HOME cyoung ---</code>

Entering commands

You can enter filer commands

- ◆ From the console attached to the filer.

- ◆ From the administration host that you specified during `setup`, using the `rsh` command. For example:
`rsh toaster cifs access HOME toto rw-`
- ◆ From a `telnet` session to the filer.

Complete the following steps to establish access to shares.

Step	Action
1	Select a method for entering filer commands.
2	Enter the <code>cifs</code> command once for each group or user to which you need to grant access to a share.
3	Repeat the process of granting access for each share.

NFS and CIFS client configuration

About this chapter

This chapter describes how to configure NFS and CIFS clients to access directories and files on the filer.

What to do next

Use the information in the following table to decide what to do next.

If ...	Read...
You purchased a license for the NFS protocol.	“Configuring NFS clients” on page 24
You purchased a license for the CIFS protocol.	“Configuring CIFS clients” on page 27

Configuring NFS clients

About this section

If you purchased a license for the NFS protocol, follow the instructions in this section to prepare NFS clients to mount file systems from the filer; otherwise, continue with “[Configuring CIFS clients](#)” on [page 27](#).

About host names and interface names

When you ran `setup`, the filer generated a host name for each interface by appending the number of the interface to the filer host name.

For example, the interface name for the first interface on a filer named `toaster` might be `toaster-e0`; the second interface might be `toaster-e1`.

If you use DNS or NIS for name resolution

If you use DNS or NIS for name resolution, add an entry in your DNS or NIS databases for each of the filer interfaces.

The following example shows how the entries might look for a filer with four interfaces:

192.16.3.1.145	toaster-e0	toaster
192.16.4.1.155	toaster-e1	
192.16.5.1.165	toaster-f0	
192.16.6.1.175	toaster-a5	

In the first line of the preceding example, the filer host name itself is used as an alias for the first network interface.

If you use `/etc/hosts` files for name resolution

If you use `/etc/hosts` files for name resolution, add an entry in each host’s `/etc/hosts` file for each of the filer interfaces.

The following example shows how the entries might look for a filer with four interfaces:

192.16.3.1.145	toaster-e0	toaster
192.16.4.1.155	toaster-e1	
192.16.5.1.165	toaster-f0	
192.16.6.1.175	toaster-a5	

In the first line of the preceding example, the filer host name itself is used as an alias for the first network interface.

- Exporting filer directories

You must export the filer’s file systems before clients can mount them.

Use an editor from an NFS or a CIFS client to edit the `/etc/exports` file to export filer directories.
- Mounting file systems on clients

For clients to mount file systems from the filer, you must create entries for the directories exported from the filer in each client’s `/etc/fstab` or `/etc/vfstab` file.

After you edit the clients’ `/etc/fstab` or `/etc/vfstab` file, the clients mount the file systems automatically when they boot.

Procedure

Complete the following steps to prepare clients to mount the filer’s file systems.

Note

The `/vol/vol0/home` directory is used as a sample filer directory in this procedure. You should use a path that exists on the filer.

Step	Action
1	Create a directory on the client to act as a mount point. For example, <code>/n/toaster/home</code> .
2	To mount the filer’s <code>/vol/vol0/home</code> directory to <code>/n/toaster/home</code>, add the following line to the client’s <code>/etc/fstab</code> or <code>/etc/vfstab</code> file: <code>toaster-e0:/vol/vol0/home /n/toaster/home nfs rw 0 0</code> In the preceding example, the client is on the same network as the filer <code>e0</code> Ethernet interface. If the client is on the same network as the <code>e1</code> Ethernet interface, use the following line instead: <code>toaster-e1:/vol/vol0/home /n/toaster/home nfs rw 0 0</code> The file system is mounted when the client reboots.
3	To mount the <code>/vol/vol0/home</code> directory without a client reboot, enter the following command at the client: <code>mount toaster-e1:/vol/vol0/home /n/toaster/home</code>

Results

After the `/vol/vol0/home` directory on the filer is mounted, the user on the client system can create, modify, or remove files in `/n/toaster/home`.

What to do next

Use the following table to decide what to do next.

If...	Read...
You purchased a license for the CIFS protocol.	“Configuring CIFS clients” on page 27 .
You did not purchase a license for the CIFS protocol.	Chapter 9 , “About the Filer Software.”

Configuring CIFS clients

About this section

If you purchased a license for the CIFS protocol, follow the instructions in this section to configure CIFS clients to access information on the filer.

Filer is visible to CIFS clients after setup finishes

After **setup** finishes, the filer becomes visible to CIFS clients by automatically registering with the master browser on its local network.

If cross-subnet browsing is configured correctly, the filer is now visible to all CIFS clients. For more information about cross-subnet browsing, refer to Microsoft networking documentation.

CIFS client connection methods

The following table describes the various methods by which CIFS clients can connect to the filer. For more information about commands and windows mentioned in the table, refer to the operating system manual for your computer.

Method	Client operating system	Command or window	Description
1	Windows 95, Windows NT 4.0	Map Network Drive window (from Network Explorer)	Connect to the filer as a network drive.
2	Windows 95, Windows NT 4.0	Network Neighborhood	Click the filer icon in the Network Neighborhood window.
3	Windows NT 3.51, Windows for Workgroups	Connect Network Drive window (from the File Manager)	Connect to the filer as a network drive.
4	Any operating system that supports the DOS command-line interface and supports the net use command	net use command	Map a share to a drive letter on the command line. For example: <code>net use f: \\toaster\home</code>

Steps

Complete the following steps to inform users about how to access the filer.

Step	Action
1	From the preceding table, determine the connection methods that are correct for your CIFS clients.
2	If your CIFS clients can use methods 1, 3, and 4 to connect to the filer, inform your users of the filer's UNC path. The UNC path consists of a computer name and a share name in the following format: <i>\\computer_name\share_name</i> Example: If the filer is named toaster and the directory that contains users' directories is shared with the name "home," the UNC path is <i>\\toaster\home</i>.
3	If your CIFS clients can use method 2 to connect to the filer, inform your users of the filer name so that they can locate the filer in Network Neighborhood.

Results

After you provide users with information about how to access the filer, they can connect to the filer, view directories, and read and write files.

About SecureShare

Features in SecureShare

For multiprotocol environments, Data ONTAP provides two SecureShare features:

- ◆ SecureShare Access, which makes it easy for Windows users to change UNIX file permissions on the filer.
SecureShare Access appears as a tab in the Properties dialog box of a set of files you select if at least one of the files is a UNIX file. To use SecureShare Access, follow the instructions in “Changing UNIX permissions from Windows” in Chapter 7 of the *System Administrator’s Guide*.
- ◆ SecureShare Account Migrator (formerly the `cvtusers` tool), which makes it easy to convert users and groups from a Windows NT domain into the format necessary to populate the `/etc/passwd` and `/etc/group` files on your filer. It enables you to perform the following tasks:
 - ❖ Create the commands necessary to build CIFS shares for each user and apply appropriate rights to these shares.
 - ❖ Synchronize a Windows NT domain with `/etc` files, so you can keep your `/etc` files current by running the program daily.

You can run SecureShare Account Migrator only from Windows NT, and only if you have administrative access to the filer.

Installing SecureShare Access

Steps

Complete the following steps to install SecureShare Access from the CD-ROM.

Step	Action
1	Make sure that the Data ONTAP CD-ROM is in the CD-ROM drive.
2	Click the CD-ROM drive icon.
3	Click UTILS.
4	Click SSACCESS.
5	Click SSACCESS.EXE.
6	Follow the prompts in the SecureShare Access installer program.

Installing SecureShare Account Migrator

Procedure

Complete the following steps to install SecureShare Account Migrator from the CD-ROM.

Step	Action
1	Make sure that the Data ONTAP CD-ROM is in the CD-ROM drive.
2	Click the CD-ROM drive icon.
3	Click UTILS.
4	Click SSAM.
5	Open the README file.
6	Click CVTUSERS.EXE.
7	Follow the prompts in the SecureShare Account Migrator installer program.

Checking the cluster filer configuration

Matching filer configurations

When configuring filers as partners in a clustered environment, parameters, configuration files, licenses, and network interfaces must match. In this way, when a partner filer takes over for the failed filer, it appears the same as the failed filer.

After you have configured both filers, use the following tables to ensure that both filers match in their configuration.

Parameter matching

Compare the output of the `options` command for both filers in the cluster to ensure that each option has the same value in both filers.

options command options that must match	
cifs.show_snapshot	dns.domainname
dns.enable	http.admin.enable
httpd.timeout	httpd.timewait.enable
vol.copy.throttle	ip.path_mtu_discovery.enable
nfs.per_client_stats.enable	nfs.v2.df.2gb.lim
nfs.v3.enable	nis.domainname
nis.enable	pcnfsd.enable
raid.reconstruct_speed	raid.timeout
wafl.maxdirsize	wafl.root_only_chown
cf.timed.enable	
Other parameters that must match	
Parameter	Command
ARP table	arp
date	date, rdate
NDMP on or off	ndmpd {on off}

NFS enabled	nfs {enable disable}
route table published	route
routed enabled	routed {on off}
time zone	timezone <i>name</i>

Configuration file matching

The following files must have identical contents:

- ◆ */etc/resolv.conf*
- ◆ */etc/httpd.mimetypes*
- ◆ */etc/dgateways*
- ◆ */etc/nsswitch.conf*

License matching

Licenses must match on both filers. For each feature you want, you must purchase a separate license for each filer. Fill in the license codes for your filers in the following table.

Feature	Filer 1 license code	File 2 license code
CIFS		
Cluster		
HTTP		
NFS		

Filer software description

About this chapter

This chapter describes the software that shipped with the filer.

The filer was shipped with a CD-ROM and system boot diskettes. Because system software has been installed at the factory, you don't need the CD-ROM or system boot diskettes to install or configure a new filer.

Store the filer software in a safe place so that you can use it to recover from any unlikely software problems in the future.

CD-ROM and diskette contents

The following list describes the CD-ROM and system boot diskettes:

Data ONTAP CD-ROM	This CD-ROM contains the system software and documentation. If you need to reinstall the system software for any reason, you need this CD-ROM; call Network Appliance Technical Support for instructions before reinstalling system software on the filer. The Data ONTAP CD-ROM contains the system files and system boot software in two formats so that it can be read by both UNIX and PC workstations. For full information about the contents of the CD-ROM, read the file named <i>index.htm</i> on the CD-ROM.
System boot diskettes	If the filer fails to boot from hard disk, or if you forget your password, you must boot the filer from the system boot diskettes.
Custom MIB	Use this Management Information Base (MIB) with SNMP to get detailed information about filer operation. For further information, see the <i>System Administrator's Guide</i> .

Software updates

Network Appliance regularly makes software updates available to customers who purchase software support agreements.

You can find information about the latest software updates at the Network Appliance NOW Web site at <http://now.netapp.com>.

Administering your filer from a Web-based tool

About this chapter

This chapter introduces FilerView, the Network Appliance™-based administration tool for Data ONTAP.

FilerView enables you to perform most administration tasks from any client on your network that has a compatible Web browser. FilerView uses Java applets to perform tasks that otherwise require you to enter commands at the filer console or edit configuration files.

You can use FilerView even if you did not purchase a license for the HTTP protocol.

If you prefer to manage the filer by using a command-line interface and editing configuration files, refer to the *System Administrator's Guide* for complete instructions.

Prerequisites

You need Netscape Navigator 4 or later or Microsoft Internet Explorer 4 or later to access FilerView. FilerView has not been tested with other Web browsers.

Accessing FilerView

To access FilerView, point your browser to the filer home page (http://hostname/na_admin), substituting the filer name for *hostname*:

Example: If your host's name is toaster, enter the following URL:

http://toaster/na_admin

When your browser connects to the filer, you see the filer home page, as shown.



The initial page contains the choices shown in the following table.

Choice	Description
Manual Pages	Links to UNIX-style man pages for the Data ONTAP console commands.
FilerView	Displays the FilerView program in a separate window.
Filer At-A-Glance	Displays a tool that monitors the performance of the filer.

Choice	Description
Initiate a support call	Directs the Web browser to a form on the Network Appliance technical support Web site. You can use the form to report problems.

FilerView interface

The following illustration shows the FilerView interface.



Using the interface

The FilerView interface consists of two frames: a left frame and a right frame.

Left frame: The left frame contains an expandable list of categories:

- ◆ The Real-time Displays category contains choices that launch separate tools that monitor filer performance.
- ◆ The other categories represent management functions.

To view the real-time displays or the functions in a category, double-click Real-time Displays or a category name. To select a real-time display or a function, double-click the display or function name.

Note

The first time you select a function, FilerView prompts you to enter the filer's administration password. After you enter the correct password, FilerView does not prompt you for the password again.

Right frame: The right frame contains a logo initially.

As you select functions from the left frame, the right frame changes to display forms that provide information about the filer configuration and enable you to change the filer's configuration.

To alter the filer configuration, you change information that is displayed in forms and then save the information.

Help button: The top of the window contains a Help button that you can click to view Help for the form that is currently displayed in the right frame.

Time zone selection

About this section You must enter one of the following time zones when **setup** prompts for a time zone.

Africa

Africa/Abidjan	Africa/Accra	Africa/Addis_Ababa
Africa/Algiers	Africa/Asmera	Africa/Bamako
Africa/Bangui	Africa/Banjul	Africa/Bissau
Africa/Blantyre	Africa/Brazzaville	Africa/Bujumbura
Africa/Cairo	Africa/Casablanca	Africa/Conakry
Africa/Dakar	Africa/Dar_es_Salaam	Africa/Djibouti
Africa/Douala	Africa/Freetown	Africa/Gaborone
Africa/Harare	Africa/Johannesburg	Africa/Kampala
Africa/Khartoum	Africa/Kigali	Africa/Kinshasa
Africa/Lagos	Africa/Libreville	Africa/Lome
Africa/Luanda	Africa/Lumumbashi	Africa/Lusaka
Africa/Malabo	Africa/Maputo	Africa/Maseru
Africa/Mbabane	Africa/Mogadishu	Africa/Monrovia
Africa/Nairobi	Africa/Ndjamena	Africa/Niamey
Africa/Nouakchott	Africa/Ouagadougou	Africa/Porto-Novo
Africa/Sao_Tome	Africa/Timbuktu	Africa/Tripoli
Africa/Tunis	Africa/Windhoek	

America

America/Adak	America/Anchorage	America/Anguilla
America/Antigua	America/Aruba	America/Asuncion
America/Atka	America/Barbados	America/Belize
America/Bogota	America/Boise	America/Buenos_Aires
America/Caracas	America/Catamarca	America/Cayenne
America/Cayman	America/Chicago	America/Cordoba
America/Costa_Rica	America/Cuiaba	America/Curacao
America/Dawson	America/Dawson_Creek	America/Denver
America/Detroit	America/Dominica	America/Edmonton
America/El_Salvador	America/Ensenada	America/Fort_Wayne
America/Fortaleza	America/Glace_Bay	America/Godthab
America/Goose_Bay	America/Grand_Turk	America/Grenada
America/Guadeloupe	America/Guatemala	America/Guayaquil
America/Guyana	America/Halifax	America/Havana
America/Indiana	America/Indianapolis	America/Inuvik
America/Iqaluit	America/Jamaica	America/Jujuy
America/Juneau	America/Knox_IN	America/La_Paz
America/Lima	America/Los_Angeles	America/Louisville
America/Maceio	America/Managua	America/Manaus
America/Martinique	America/Mazatlan	America/Mendoza
America/Menominee	America/Mexico_City	America/Miquelon
America/Montevideo	America/Montreal	America/Montserrat
America/Nassau	America/New_York	America/Nipigon
America/Nome	America/Noronha	America/Panama
America/Pangnirtung	America/Paramaribo	America/Phoenix
America/Port_of_Spain	America/Port-au-Prince	America/Porto_Acre
America/Puerto_Rico	America/Rainy_River	America/Rankin_Inlet
America/Regina	America/Rosario	America/Santiago
America/Santo_Domingo	America/Sao_Paulo	America/Scoresbysund
America/Shiprock	America/St_Johns	America/St_Kitts
America/St_Lucia	America/St_Thomas	America/St_Vincent
America/Swift_Current	America/Tegucigalpa	America/Thule
America/Thunder_Bay	America/Tijuana	America/Tortola
America/Vancouver	America/Virgin	America/Whitehorse
America/Winnipeg	America/Yakutat	America/Yellowknife

Antarctica

Antarctica/Casey	Antarctica/DumontDUrville	Antarctica/Mawson
Antarctica/McMurdo	Antarctica/Palmer	Antarctica/South_Pole

Asia

Asia/Aden	Asia/Alma-Ata	Asia/Amman
Asia/Anadyr	Asia/Aqtau	Asia/Aqtobe
Asia/Ashkhabad	Asia/Baghdad	Asia/Bahrain
Asia/Baku	Asia/Bangkok	Asia/Beirut
Asia/Bishkek	Asia/Brunei	Asia/Calcutta
Asia/Chungking	Asia/Colombo	Asia/Dacca
Asia/Damascus	Asia/Dubai	Asia/Dushanbe
Asia/Gaza	Asia/Harbin	Asia/Hong_Kong
Asia/Irkutsk	Asia/Ishigaki	Asia/Istanbul
Asia/Jakarta	Asia/Jayapura	Asia/Jerusalem
Asia/Kabul	Asia/Kamchatka	Asia/Karachi
Asia/Kashgar	Asia/Katmandu	Asia/Krasnoyarsk
Asia/Kuala_Lumpur	Asia/Kuching	Asia/Kuwait
Asia/Macao	Asia/Magadan	Asia/Manila
Asia/Muscat	Asia/Nicosia	Asia/Novosibirsk
Asia/Omsk	Asia/Phnom_Penh	Asia/Pyongyang
Asia/Qatar	Asia/Rangoon	Asia/Riyadh
Asia/Saigon	Asia/Seoul	Asia/Shanghai
Asia/Singapore	Asia/Taipei	Asia/Tashkent
Asia/Tbilisi	Asia/Tehran	Asia/Tel_Aviv
Asia/Thimbu	Asia/Tokyo	Asia/Ujung_Pandang
Asia/Ulan_Bator	Asia/Urumqi	Asia/Vientiane
Asia/Vladivostok	Asia/Yakutsk	Asia/Yekaterinburg
Asia/Yerevan		

Atlantic

Atlantic/Azores	Atlantic/Bermuda	Atlantic/Canary
Atlantic/Cape_Verde	Atlantic/Faeroe	Atlantic/Jan_Mayen
Atlantic/Madeira	Atlantic/Reykjavik	Atlantic/South_Georgia
Atlantic/St_Helena	Atlantic/Stanley	

Australia

Australia/ACT	Australia/Adelaide	Australia/Brisbane
Australia/Broken_Hill	Australia/Canberra	Australia/Darwin
Australia/Hobart	Australia/LHI	Australia/Lindeman
Australia/Lord Howe	Australia/Melbourne	Australia/NSW
Australia/North	Australia/Perth	Australia/Queensland
Australia/South	Australia/Sydney	Australia/Tasmania
Australia/Victoria	Australia/West	Australia/Yancowinna

Brazil	Brazil/Acre Brazil/West	Brazil/DeNoronha	Brazil/East
Canada	Canada/Atlantic Canada/Eastern Canada/Pacific	Canada/Central Canada/Mountain Canada/Saskatchewan	Canada/East-Saskatchewan Canada/Newfoundland Canada/Yukon
Chile	Chile/Continental	Chile/EasterIsland	
Etc	Etc/GMT Etc/GMT+2 Etc/GMT+5 Etc/GMT+8 Etc/GMT+11 Etc/GMT-0 Etc/GMT-3 Etc/GMT-6 Etc/GMT-9 Etc/GMT-12 Etc/Greenwich Etc/UTC	Etc/GMT+0 Etc/GMT+3 Etc/GMT+6 Etc/GMT+9 Etc/GMT+12 Etc/GMT-1 Etc/GMT-4 Etc/GMT-7 Etc/GMT-10 Etc/GMT-13 Etc/UCT Etc/Zulu	Etc/GMT+1 Etc/GMT+4 Etc/GMT+7 Etc/GMT+10 Etc/GMT0 Etc/GMT-2 Etc/GMT-5 Etc/GMT-8 Etc/GMT-11 Etc/GMT-14 Etc/Universal
Europe	Europe/Amsterdam Europe/Belfast Europe/Bratislava Europe/Budapest Europe/Dublin Europe/Istanbul Europe/Lisbon Europe/Luxembourg Europe/Minsk Europe/Oslo Europe/Riga Europe/Sarajevo Europe/Sofia Europe/Tirane	Europe/Andorra Europe/Belgrade Europe/Brussels Europe/Chisinau Europe/Gibraltar Europe/Kiev Europe/Ljubljana Europe/Madrid Europe/Monaco Europe/Paris Europe/Rome Europe/Simferopol Europe/Stockholm Europe/Vaduz	Europe/Athens Europe/Berlin Europe/Bucharest Europe/Copenhagen Europe/Helsinki Europe/Kuybyshev Europe/London Europe/Malta Europe/Moscow Europe/Prague Europe/San_Marino Europe/Skopje Europe/Tallinn Europe/Vatican

	Europe/Vienna Europe/Zagreb	Europe/Vilnius Europe/Zurich	Europe/Warsaw
GMT	GMT GMT+3 GMT+6 GMT+9 GMT+12 GMT-2 GMT-5 GMT-8 GMT-11	GMT+1 GMT+4 GMT+7 GMT+10 GMT+13 GMT-3 GMT-6 GMT-9 GMT-12	GMT+2 GMT+5 GMT+8 GMT+11 GMT-1 GMT-4 GMT-7 GMT-10
Indian (Indian Ocean)	Indian/Antananarivo Indian/Cocos Indian/Mahe Indian/Mayotte	Indian/Chagos Indian/Comoro Indian/Maldives Indian/Reunion	Indian/Christmas Indian/Kerguelen Indian/Mauritius
Mexico	Mexico/BajaNorte	Mexico/BajaSur	Mexico/General
Miscellaneous	Arctic/Longyearbyen Cuba Eire Factory Greenwich Iceland Jamaica Libya MST7MDT NZ-CHAT PRC ROK UCT WET	CET EET EST GB Hongkong Iran Japan MET Navajo Poland PST8PDT Singapore Universal W-SU	CST6CDT Egypt EST5EDT GB-Eire HST Israel Kwajalein MST NZ Portugal ROC Turkey UTC Zulu

Pacific

Pacific/Apia	Pacific/Auckland	Pacific/Chatham
Pacific/Easter	Pacific/Efate	Pacific/Enderbury
Pacific/Fakaofu	Pacific/Fiji	Pacific/Funafuti
Pacific/Galapagos	Pacific/Gambier	Pacific/Guadalcanal
Pacific/Guam	Pacific/Honolulu	Pacific/Johnston
Pacific/Kiritimati	Pacific/Kosrae	Pacific/Kwajalein
Pacific/Majuro	Pacific/Marquesas	Pacific/Midway
Pacific/Nauru	Pacific/Niue	Pacific/Norfolk
Pacific/Noumea	Pacific/Pago_Pago	Pacific/Palau
Pacific/Pitcairn	Pacific/Ponape	Pacific/Port_Moresby
Pacific/Rarotonga	Pacific/Saipan	Pacific/Samoa
Pacific/Tahiti	Pacific/Tarawa	Pacific/Tongatapu
Pacific/Truk	Pacific/Wake	Pacific/Wallis
Pacific/Yap		

System V

SystemV/AST4	SystemV/AST4ADT	SystemV/CST6
SystemV/CST6CDT	SystemV/EST5	SystemV/EST5EDT
SystemV/HST10	SystemV/MST7	SystemV/MST7MDT
SystemV/PST8	SystemV/PST8PDT	SystemV/YST9
SystemV/YST9YDT		

US (United States)

US/Alaska	US/Aleutian	US/Arizona
US/Central	US/East-Indiana	US/Eastern
US/Hawaii	US/Indiana-Starke	US/Michigan
US/Mountain	US/Pacific	US/Pacific-New
US/Samoa		

Aliases

GMT=Greenwich, UCT, UTC, Universal, Zulu

CET=MET (Middle European Time)

US/Eastern=Jamaica

US/Mountain=Navajo

Introduction

About the worksheets

The worksheets in this appendix are designed to assist you in collecting the information you need in order to configure your new filer.

You may not need to complete every worksheet. Use only those worksheets that match your filer's configuration and options.

Worksheet 1: Host name and interfaces

About this worksheet

This worksheet contains information about your filer’s host name and its interfaces.

The worksheet contains four sections of interface information:

- ◆ Virtual interfaces
- ◆ Ethernet interfaces
- ◆ Fore/IP SPANS interfaces
- ◆ ATM LANE interfaces

Complete the sections for the interfaces that your filer uses.

Host name

The host name is a unique 1- to 32-character name that uses only alphanumeric characters and hyphens.

Note _____
If you purchased a license for the CIFS protocol and want to use the same host name for both NFS and CIFS, select a name of 1- to 15- characters.

Host Name	
------------------	--

Virtual interfaces

Complete this section only if you plan to use virtual interfaces with your filer.
You can define up to 32 virtual interfaces. Each virtual interface must have a 1- to 15-character name, and can be defined as a single or multiple virtual interface.

For each virtual interface, enter a name, the number of links, and the link names.

Virtual interface names	Number of links	Link names
1:		1:
		2:
		3:
		4:
2:		1:
		2:
		3:
		4:
3:		1:
		2:
		3:
		4:
4:		1:
		2:
		3:
		4:
5:		1:
		2:
		3:
		4:

Virtual interface names	Number of links	Link names
6:		1:
		2:
		3:
		4:
7:		1:
		2:
		3:
		4:
8:		1:
		2:
		3:
		4:

Ethernet interfaces

Filers can contain a maximum of 31 interfaces. The interface names in this table are assigned by **setup** automatically.

For a single filer only: You do not need to fill out the partner IP addresses; they are for a cluster configuration only.

For a cluster configuration only: Fill in the host's IP addresses and subnet masks, fill in the partner's IP addresses that the host can take over, and record the host's interface names when **setup** runs.

#	Host interface name	Host IP address	Host subnet mask	Partner IP address
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				

#	Host interface name	Host IP address	Host subnet mask	Partner IP address
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				

Fore/IP SPANS

Complete this section if your filer uses Fore/IP SPANS interfaces.

#	SPANS interface name	Enter the host IP address and subnet mask OR the Partner IP address		
		Host IP address	Host subnet mask	Partner IP address
1				
2				
3				
4				
5				
6				
7				
8				

ATM LANE interfaces

Complete this section if your filer uses ATM LANE interfaces.

ATM adapter #	ATM interface name	Partner Name
1		
2		
3		
4		
5		
6		
7		
8		

ATM Adapter #	ELAN Name	LECS Address (Use well known or specify address)
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		

ATM Adapter #	ELAN Name	LECS Address (Use well known or specify address)
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		

Default gateway

The default gateway, which is an optional entry, specifies the name and address of your network’s router.

Gateway name	
IP address	

Worksheet 2: Administration host

About this worksheet

- The administration host is a client that is authorized to access the filer for administration purposes. The administration host can do the following tasks:
- ◆ Mount the filer’s root directory (/) as an NFS client (if the filer is licensed for the NFS protocol).
 - ◆ Access the filer’s root directory as a Windows shared directory, C\$ (if the filer is licensed for the CIFS protocol).
 - ◆ Access the filer’s virtual console remote using a remote shell (rsh) program or a Telnet client.
 - ◆ Manage the filer using the FilerView Web-based tool.

If you do not assign an administration host, any client using a licensed protocol (NFS or CIFS) can perform the preceding tasks.

Note_____

After you complete the first-time configuration, you can grant additional hosts administration privileges by modifying the NFS exports or the CIFS shares.

Administration host name	
IP address	

Worksheet 3: Time zone

About this worksheet

Your filer needs to be set to the proper time zone. Refer to Appendix A, “[Time zones](#),” on page 41 for a complete list of time zones. If you do not enter a time zone during first-time configuration, the filer uses Greenwich Mean Time (GMT) as the default time zone.

Time Zone	
------------------	--

Worksheet 4: DNS and NIS information

About this worksheet

This worksheet covers the information you need to configure your filer for DNS and NIS service. It contains the following entries:

- ◆ DNS domain name
- ◆ DNS servers
- ◆ NIS domain name

DNS domain name

If you use Domain Name Service (DNS) to resolve host names into IP addresses, you need to provide the name of your DNS domain. For example: netapp.com.

DNS domain name	
------------------------	--

DNS servers

If you use DNS, you must also provide the names and IP addresses of one to three DNS servers.

DNS server names	IP addresses

NIS domain name

If you use Network Information Services (NIS) to validate user names and passwords, you must provide the name of your NIS domain, such as netapp.com.

NIS domain name	
------------------------	--

Worksheet 5: Password

**About this
worksheet**

Your filer can be protected by a password to prevent unauthorized users from making changes to its configuration. If you do not create a password, any user can gain access to the filer at the console, or through telnet or FilerView.

Password	
-----------------	--

Worksheet 6: Disks

About this worksheet

During first-time configuration, the `setup` command creates a default volume. The default size for the default volume is 2 disks, but you can specify that the volume contain from 2 to 14 disks.

If you specify a default volume size of less than 14 disks, you can add disks to the volume after your filer configuration is complete by following the instructions in Chapter 3, “Managing disks and file systems,” in the *System Administrator’s Guide*.

If your filer only has 14 disks installed and want to take advantage of the multiple-volume support in Data ONTAP, you should specify 12 or fewer disks for the default volume.

WARNING

If you plan to create additional volumes after the filer is set up, do not allocate all your disks to the default volume; this ensures that disks remain available for the additional volumes.

Number of disks in the default volume	
---------------------------------------	--

Worksheet 7: CIFS information

About this worksheet

This worksheet contains information that you need to supply if you purchased a license for the CIFS protocol. The information consists of the following entries:

- ◆ WINS server addresses
- ◆ Code page
- ◆ File permission semantics
- ◆ Authentication mode
- ◆ Filer name
- ◆ Windows NT domain or Windows workgroup name

WINS server addresses

If your network uses the Windows Internet Naming Service (WINS), you must provide the IP address for one to four WINS servers.

Server #	IP address
1	
2	
3	
4	

Code page

Choose which language the filer supports by entering the appropriate code page. Set the filer and all its clients to the same code page or use only ASCII characters.

Caution

Select the code page carefully; consider your choice unalterable. See the *System Administrator's Guide* for more information.

Note

None of the supported code pages contain the Eurodollar symbol.

The following code pages are supported:

- ◆ Arabic = 864
- ◆ Baltic Rim = 775
- ◆ Cyrillic = 855
- ◆ Cyrillic Russian (former USSR) = 866
- ◆ English and Western and Northern European languages, except Icelandic and Portuguese, and languages that use the Nordic character “o with a stroke” = 437 (default)
- ◆ French Canada = 863
- ◆ Hebrew = 862
- ◆ Icelandic = 861
- ◆ Greek = 737
- ◆ Modern Greek = 869
- ◆ Multilingual (Latin -1) and Northern European languages = 850
- ◆ Nordic = 865
- ◆ Portuguese = 860
- ◆ Slavic (Latin -2) = 852
- ◆ Thai = 874
- ◆ Turkish = 857

Code page	
------------------	--

File permission semantics

Your filer can use PC (Windows) or UNIX style permission semantics. For additional information about PC and UNIX style permission semantics, refer to [“Choosing between PC-style or UNIX-style permissions”](#) on page 77.

File permission semantics	Circle one: ◆ PC (Windows) style ◆ UNIX style
----------------------------------	---

Authentication mode

The filer can use a Windows NT domain controller or a UNIX password database to authenticate users.

Note

If the filer is in a Windows workgroup, the filer uses the UNIX password database.

Authentication mode	Circle one: ◆ Windows NT domain controller ◆ UNIX password database
----------------------------	---

Filer name

The CIFS service can use the same host name you selected for the filer (the default) or a different name. The CIFS name cannot exceed 15 characters, and can consist of the following characters:

letters (A–Z), numerals (0–9), !, #, \$, @, %, ‘, (,), -, ^, _, {, }, and ~

If the host name you selected for the filer does not meet the CIFS naming conventions, **setup** creates a legal name by discarding illegal characters and truncating the name to 15 characters.

Filer name	
-------------------	--

Windows NT domain or Windows workgroup name

The filer can be a member of a Windows NT domain or a Windows workgroup. Enter the name of the domain or workgroup to which the filer belongs. For additional information about domain and workgroup configurations, refer to “[Deciding on a domain or workgroup configuration](#)” on page 74.

Domain or workgroup name	
---------------------------------	--

CIFS information needed

About this appendix This appendix contains information to help you understand the following CIFS configuration issues:

- ◆ [Deciding on a domain or workgroup configuration](#)
- ◆ [Choosing between PC-style or UNIX-style permissions](#)
- ◆ [Adding the filer to a Windows NT domain](#)

Deciding on a domain or workgroup configuration

About this section

You can install the filer into a Windows NT domain or Windows workgroup. Use the information in this section to help you decide which to choose.

Caution

It is difficult to change this decision after you run **setup**.

Definition of a domain

A domain

- ◆ Is a collection of Windows NT computers that share a common directory database defined by a Windows NT server administrator
- ◆ Has a unique domain name
- ◆ Provides access to centralized user and group accounts
- ◆ Enables centralized administration of user and group accounts

Definition of a workgroup

A workgroup

- ◆ Is a collection of Windows NT computers
- ◆ Has a unique workgroup name
- ◆ Is grouped for viewing purposes
- ◆ Does not provide access to centralized user and group accounts
- ◆ Does not enable centralized administration of user and group accounts

When to install into a Windows NT domain

Install the filer into a Windows NT domain

- ◆ If you want centralized administration using a Windows NT domain
- ◆ If you want to integrate the filer into the Windows NT domain topology
- ◆ If you want user authentication to be handled by Windows NT domain controllers

Caution

Your network must have at least one Windows NT domain controller to install the filer into a Windows NT domain.

When to install into a Windows workgroup

Install the filer into a Windows workgroup

- ◆ If you do not want centralized administration through a Windows NT domain
- ◆ If you want UNIX-style authentication using an */etc/passwd* file or NIS

Caution

If you install the filer into a Windows workgroup, it is not compatible with clients that have Windows NT 4.0 Service Pack 3.0 or Windows 95 clients with Microsoft Distributed File System (DFS) 4.1 installed. Clients can be made compatible by adding a registry entry to reenable plain-text passwords.

To reenable plain-text passwords on a Windows NT client, consult the Microsoft Knowledge Base on the Web at <http://www.microsoft.com/kb/default.asp>; refer to article Q166730, "With Unencrypted Password SP3 Fails to Connect to SMB Server."

To reenable plain-text passwords on a Windows 95 client, consult the following file in the Microsoft Knowledge Base on the Web at <http://www.microsoft.com/ntserver/dfs/readme.asp>.

Summary of domain and workgroup features

The following table shows which authentication features are available to domains and which are available to workgroups.

Feature	Domain	Workgroup
Compatible with Windows NT 4.0 Service Pack 3 (encryption).	Y	N
Compatible with Windows NT 4.0 Service Pack 3 (message signing).	N	N
Support for Windows NT-only users.	Y	N
Encrypted password sent to filer.	Y	N
<i>/etc/passwd</i> and <i>/etc/group</i> files on the filer determine User Identification numbers (UIDs) and Group Identification numbers (GIDs) for multiprotocol.	Y	Y
<i>/etc/passwd</i> file on the filer contains users' passwords.	N	Y
Single login.	Y	N

Feature	Domain	Workgroup
Change password remotely.	Y	Y (only with NIS)
Multiple net segments.	Y	N

Choosing between PC-style or UNIX-style permissions

About this section

When you configure the CIFS protocol, you must choose whether the filer uses PC-style or UNIX-style permissions.

Note

If you are setting up a filer in a Windows NT-only environment, you can skip this section.

This section provides a brief overview of PC-style and UNIX-style permissions and provides guidelines for choosing which style to use. PC-style permissions are similar to FAT (File Allocation Table); they maintain security with share level ACLs (Access Control Lists). In addition, PC-style permissions also allow you to further restrict file security using file permissions. UNIX-style permissions do not use share level ACLs. Therefore, using PC-style permissions only affects PC access to files with UNIX security.

How PC-style permissions work

PC-style permissions are determined by the rights assigned in a share's ACL and are limited by the UNIX permissions assigned to a file. To write to a file when PC-style permissions are in effect, a user must meet the following criteria:

- ◆ The user must have write permission for the file in the ACL.
- ◆ The user must have write permission for the file according to the UNIX-style permissions associated with the file.

If the user is the owner of the file, the filer uses the UNIX-style permissions set for the owner of the file. If the user is not the owner of the file, the filer uses the UNIX-style permissions set for the UNIX group associated with the file. Note that the UNIX "other" permissions are not used.

When to choose PC-style permissions

Choose PC-style permissions if you need file access to be controlled by ACLs.

How UNIX-style permissions work

UNIX-style permissions are determined by the rights associated with the UNIX UID and GID and are limited by the ACL permissions assigned to a file. To write to a file when UNIX-style permissions are in effect, a user must meet the following criteria:

- ◆ If the user is the owner of the file, the write permission for the user's UID must be set.
- ◆ If the user is not the owner of the file, he or she must be a member of the group (GID) associated with the file and the write permission for the group's GID must be set.
- ◆ The user must have write permission for the file in the ACL.

When to choose UNIX-style permissions

Choose UNIX-style permissions if you want to implement simple security and need access to be controlled using exact UNIX rules.

Note

If you choose UNIX-style permissions, set the share ACL permission to **rwX** for **everyone**. With this setting, the UNIX rights work just as they do on a UNIX system.

Adding the filer to a Windows NT domain

About this section

Use the information in this section to add the filer to a Windows NT domain before you configure the filer.

Note

This section presents one method of adding the filer to a Windows NT domain. For alternative ways of adding the filer to a Windows NT domain, consult the Microsoft Knowledge Base on the Web at <http://www.microsoft.com/kb/default.asp>; refer to article Q140387, “Batch File Adds/Removes Machine Accounts in Server Manager.”

Prerequisites

To add the filer to a Windows NT domain, you must meet the following prerequisites:

- ◆ You must have a permanent Windows NT domain.

Caution

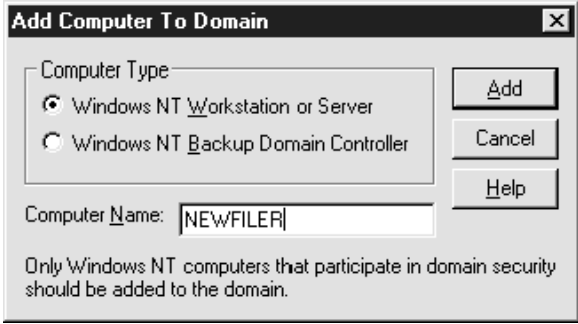
It is difficult to change this decision after you have run `setup`.

- ◆ You must have the “add workstation to domain” privilege.
- ◆ You must be able to connect to the Primary Domain Controller (PDC).

Procedure

Complete the following steps to add the filer to a Windows NT domain.

Step	Action
1	Log in as Administrator at a Windows NT server that is a member of the Windows NT domain into which you are adding the filer.
2	Run Server Manager.

Step	Action
3	From the Computer menu, select Add to Domain. The Add Computer To Domain window appears. 
4	Click the Windows NT Workstation or Server option button.
5	Enter the name of the filer. The filer name can have up to 15 of the following characters: letters (A–Z), numerals (0–9), !, #, \$, @, %, ‘, (,), -, ^, _, {, }, and ~
6	Click Add.

Results

The filer was added to the Windows NT domain.

Caution

Do not use this account until you finish configuring the filer.

Prerequisites

About this chapter

If you are setting up a cluster, this chapter explains how to cable a cluster either within system cabinets or within a standard 19-in. (48.26 cm) equipment rack (rack).

Note

For an explanation of a cluster, refer to the *System Administrator's Guide* (5.2 or later).

Prerequisites

You need the following items to set up your cluster:

Required equipment and tools: Assemble the following equipment and tools to assist you in setting up the cluster:

- ◆ #1, #2, and #3 Phillips screwdrivers
- ◆ antistatic wrist strap and grounding leash

Required manuals: Assemble the following manuals to assist you in setting up the cluster:

- ◆ If your cluster components are in system cabinets, the *System Cabinet Installation Guide*.
- ◆ If you are installing your cluster components in racks
 - ❖ Hardware Guide for your filer
 - ❖ *Fibre Channel StorageShelves Hardware Guide*

Required labels: Assemble the following labels that were provided with your cluster:

- ◆ solid-colored labels that you use to label cables for all Channel A loops
- ◆ striped labels matching the solid-colored labels that you use to label cables for all Channel B loops

Note

In the figures illustrating the cabled clusters later in this chapter, the cables are shown in color for clarity: a solid-colored line represents a Channel A cable and a dashed-colored line represents a Channel B cable. However, the cables you receive are not colored; only the labels you receive are colored. The colors of the cables in the figures reflect the colors of the labels you receive.

Setting up your cluster

For system cabinets

You need to complete the following procedures to set up your cluster.

Note

The factory delivers the filers in your cluster with the cabling for the Channel A loops and the cabling between disk shelves for the Channel B loops complete.

Stage	Procedure	Refer to...
1	Remove the front and rear doors of the system cabinets.	<i>System Cabinet Installation Guide</i>
2	Remove the side panels from the system cabinets. Note ————— Only remove the panels from the sides that will be connected. —————	<i>System Cabinet Installation Guide</i>
3	Connect the system cabinets.	<i>System Cabinet Installation Guide</i>
4	Connect the system cabinets to power sources.	<i>System Cabinet Installation Guide</i>
5	Cable the cluster.	“Cabling a cluster in a system cabinet” on page 85 and “How to cable the Channel B loop between the filer and disk shelf 0 in a maximum configuration” on page 117.
6	Reinstall the front and rear doors of the system cabinets.	<i>System Cabinet Installation Guide</i>

For equipment racks

You need to complete the following procedures to set up your cluster.

Stage	Procedure	Refer to...
1	Install the filers.	Hardware Guide for your filer
2	Install the disk shelves and set the disk shelf IDs.	<i>Fibre Channel StorageShelf Hardware Guide</i>
3	Cable the Channel A loops.	For a minimum cluster: “How to cable the Channel A loops between your filer and disk shelves in a minimum configuration” on page 99. For a maximum cluster: “How to cable the Channel A loops between your filer and disk shelves in a maximum configuration” on page 105.
4	Cable the Channel B loops.	For a minimum cluster: “How to terminate the Channel B loops in a minimum configuration” on page 101. For a maximum cluster: “How to cable the Channel B loops between your disk shelves in a maximum configuration” on page 110.

Stage	Procedure	Refer to...
5	Cable the cluster.	For a minimum cluster: “How to connect the filers in a minimum configuration” on page 102. For a maximum cluster: “How to connect the filers in a maximum configuration” on page 115 and “How to cable the Channel B loop between the filer and disk shelf 0 in a maximum configuration” on page 117.

Cabling a cluster in a system cabinet

How to cable a cluster in a system cabinet

To cable a cluster in a system cabinet, follow these steps.

Note_____

There should be one 4m cluster interconnect cable and one 2m filer-to-shelf (HSSDC-to-DB-9) cable stored in tie-wraps above the filer in each system cabinet.

Step	Action
1	Remove from the tie-wraps the cables that are stored above the filer in the system cabinet.
2	Run a <code>cf status</code> command on each filer. The resulting output should be as follows: cluster monitor not initialized. Interconnect is down.
3	Connect one end of the 4m cluster interconnect cable to the X port of the cluster interconnect adapter on one filer. Note _____
4	Slide the connector on the other end of the 4m cluster interconnect cable through the cable routing space at the rear of the system cabinet base.
5	Pull the connector through the cable routing space at the rear of the base of the partner system cabinet.
6	Connect the cable to the X port on the partner filer. Caution _____

Step	Action
7	Run a <code>cf status</code> command on each filer. The resulting output should be as follows: <pre>cluster monitor not initialized. Y link is down.</pre>
8	Repeat Steps 3 through 7 for the Y port of the cluster interconnect adapters on both filers. Run a <code>cf status</code> command on each filer. The resulting output should be as follows: <pre>cluster monitor not initialized.</pre> Note_____ The cluster interconnect adapter has two ports; the Y port is below the X port. _____ Caution_____ Verify that you connected the cable to the Y port. Connecting to the wrong port disables the takeover feature. _____
9	At the consoles of each filer, enter halt to shut down the system.
10	Connect the filer to the Channel B LRC card on disk shelf 0 of the partner filer by ◆ Connecting the HSSDC end of the FC-AL filer-to-shelf cable to one of the FC-AL adapters labeled Channel B on the filer ◆ Connecting the DB-9 end of the FC-AL filer-to-shelf cable to the Input connector of the LRC card labeled Channel B on disk shelf 0 of the partner filer Note_____ Due to cable length constraints, the filer-to-shelf cables crisscross behind the vertical trim piece on the rear of the system cabinets. _____ Repeat this step for the partner filer. The section “How to cable the Channel B loop between the filer and disk shelf 0 in a maximum configuration” on page 117 illustrates how to complete the Channel B loop to the partner filer.
11	At the console of each filer, enter boot to run the filers.

Configuring your cluster for an equipment rack

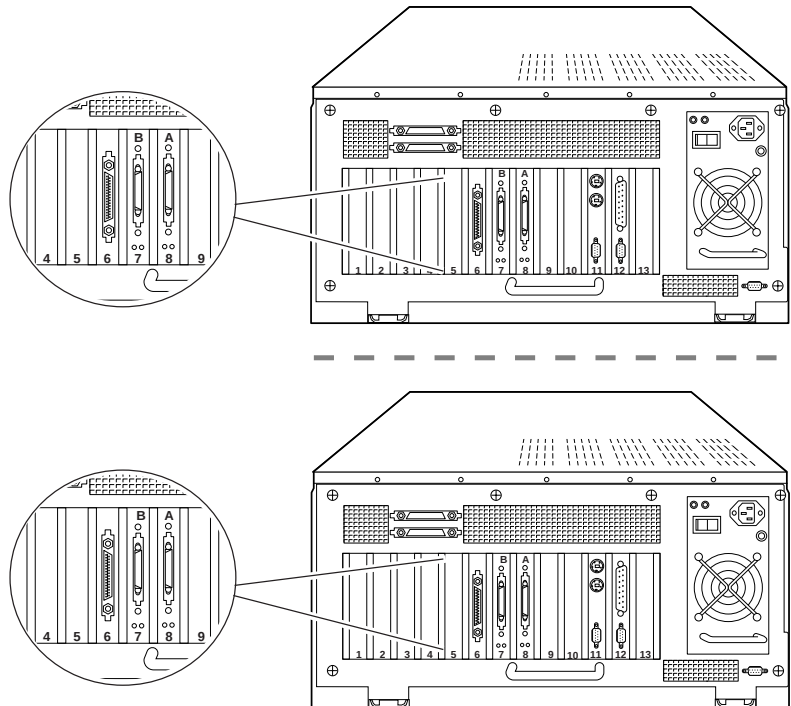
About this section

This section provides you with the cluster configuration possibilities for your filer type, if you are installing your filers and disk shelves in an equipment rack.

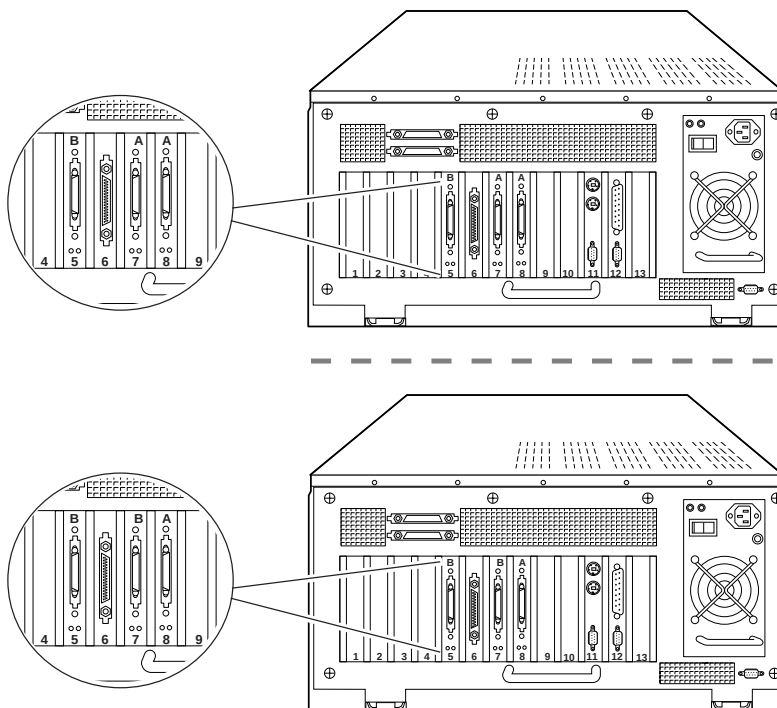
Cluster configuration possibilities for F630 filers

The following cluster configurations are possible:

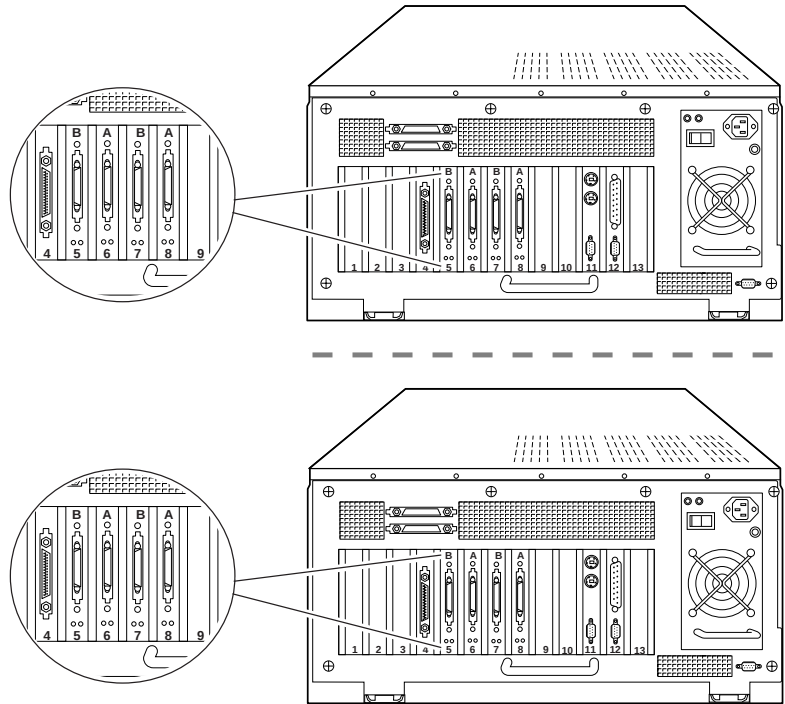
- ◆ Two FC-AL adapters in each filer, with one labeled Channel A and the other labeled Channel B. The following figure is an example of how you can label a minimum cluster configuration.



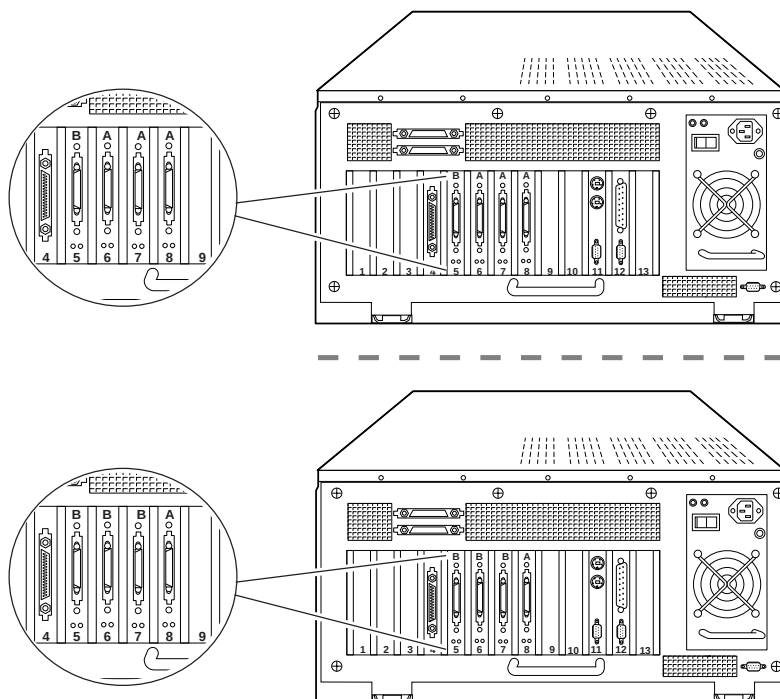
- ◆ Three FC-AL adapters in each filer, with two labeled Channel A and one labeled Channel B in one filer, and one labeled Channel A and two labeled Channel B in the partner filer. The following figure is one example of how you can label a maximum cluster configuration.



- ◆ Four FC-AL adapters in each filer, with two labeled Channel A and two labeled Channel B in each filer. The following figure is another example of how you can label a maximum cluster configuration.



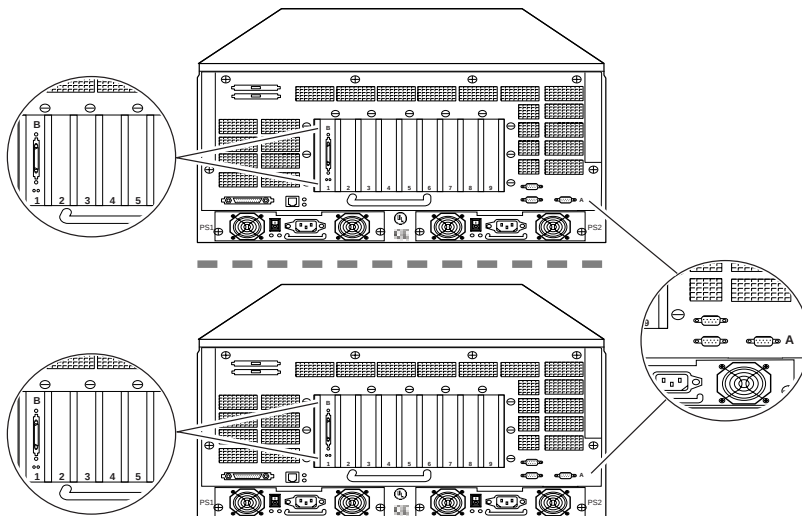
- ◆ Four FC-AL adapters in each filer, with three labeled Channel A and one labeled Channel B in one filer, and one labeled Channel A and three labeled Channel B in the partner filer. The following figure is a final example of how you can label a maximum cluster configuration.



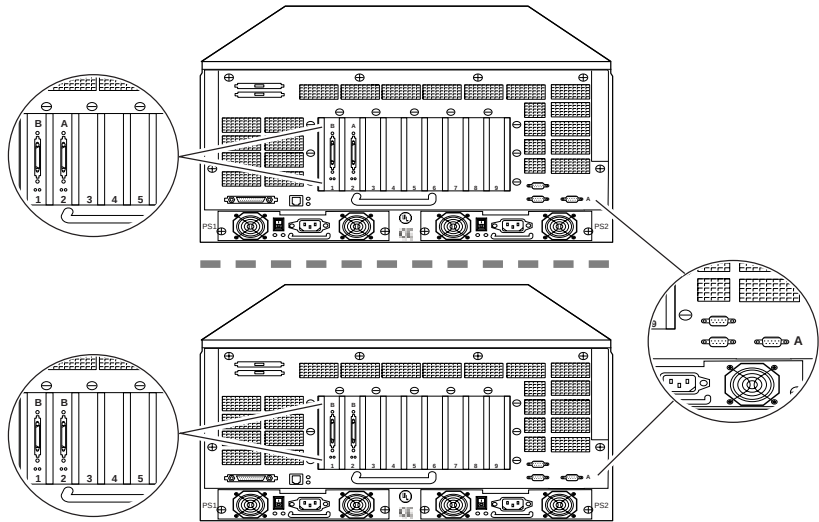
Cluster configuration possibilities for F740 filers

If you are installing your cluster components in racks, the following cluster configurations are possible:

- ◆ Two FC-AL interfaces in each filer, with the onboard FC-AL interface labeled Channel A and the FC-AL adapter labeled Channel B in each filer. The following figure is an example of how you can label a minimum cluster configuration.



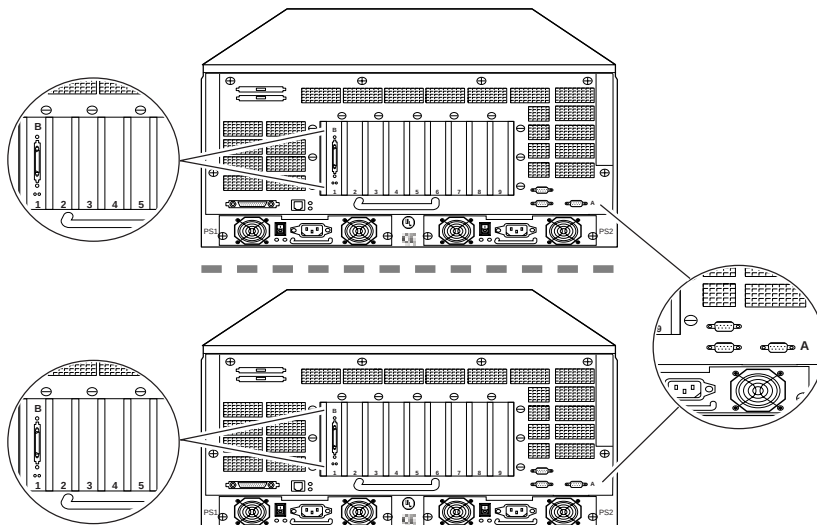
- ◆ Three FC-AL interfaces in each filer, with the onboard FC-AL interface and one FC-AL adapter labeled Channel A and one FC-AL adapter labeled Channel B in one filer, and the onboard FC-AL interface labeled Channel A and two FC-AL adapters labeled Channel B in the partner filer. The following figure is one example of how you can label a maximum cluster configuration.



Cluster configuration possibilities for F760 filers

If you are installing your cluster components in racks, the following cluster configurations are possible:

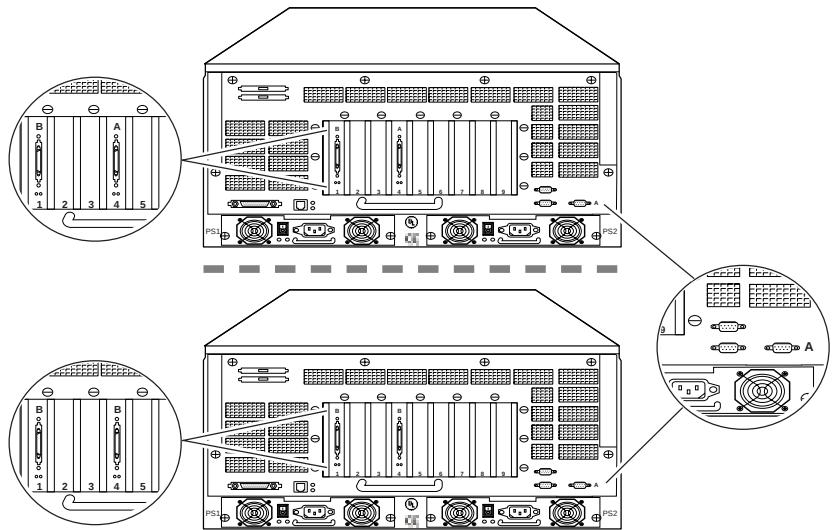
- ◆ Two FC-AL interfaces in each filer, with the onboard FC-AL interface labeled Channel A and the FC-AL adapter labeled Channel B in each filer. The following figure is an example of how you can label a minimum cluster configuration.



- ◆ Three FC-AL interfaces in each filer, with the onboard FC-AL interface and one FC-AL adapter labeled Channel A and one FC-AL adapter labeled Channel B in one filer, and the onboard FC-AL interface labeled Channel A and two FC-AL adapters labeled Channel B in the partner filer. The following figure is one example of how you can label a maximum cluster configuration.

Note

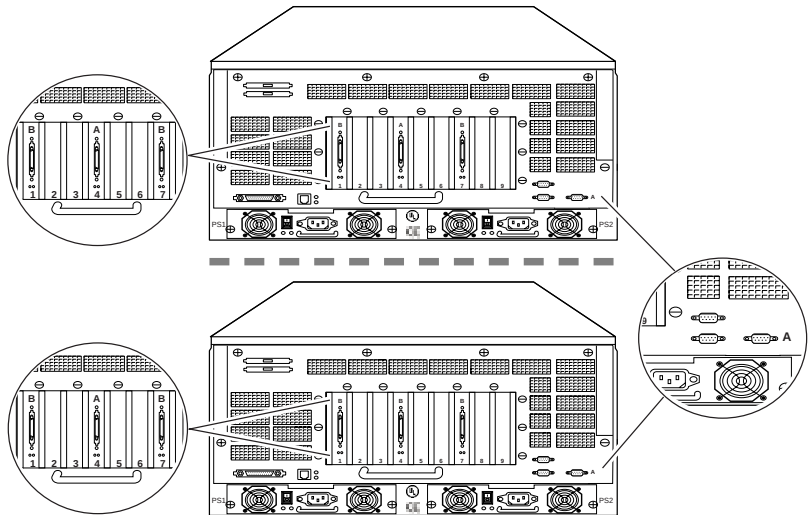
The following figure reflects one possible configuration. If you have four Gigabit Ethernet adapters in each of your filers, the FC-AL adapters occupy expansion slots 1 and 2, 1 and 3, or 2 and 3.



- ◆ Four FC-AL interfaces in each filer, with the onboard FC-AL interface and one FC-AL adapter labeled Channel A and two FC-AL adapters labeled Channel B in each filer. The following figure is another example of how you can label a maximum cluster configuration.

Note

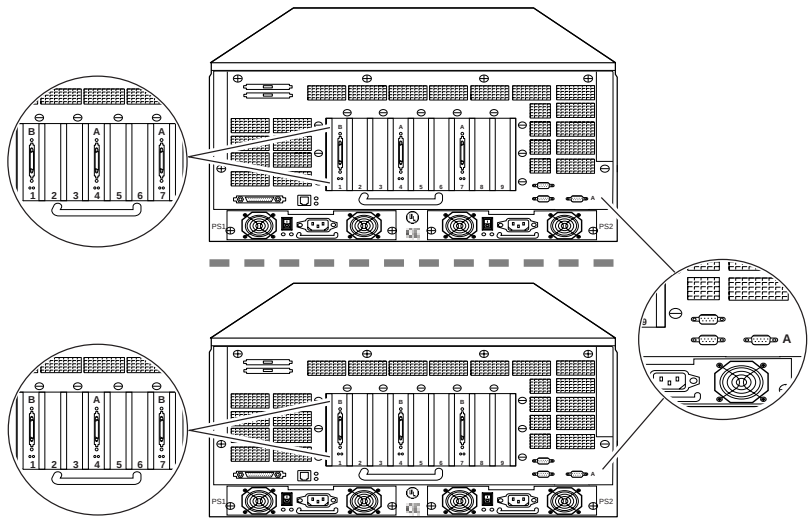
The following figure reflects one possible configuration. If you have four Gigabit Ethernet adapters in each of your filers, the FC-AL adapters occupy expansion slots 1 through 3.



- ◆ Four FC-AL interfaces in each filer, with the onboard FC-AL interface and two FC-AL adapters labeled Channel A and one FC-AL adapter labeled Channel B in one filer, and the onboard FC-AL interface labeled Channel A and three FC-AL adapters labeled Channel B in the partner filer. The following figure is a final example of how you can label a maximum cluster configuration.

Note

The following figure reflects one possible configuration. If you have four Gigabit Ethernet adapters in each of your filers, the FC-AL adapters occupy expansion slots 1 through 3.



Cabling a cluster in an equipment rack

About this section

This section provides you with the procedures required to cable the cluster if you have

- ◆ a minimum cluster configuration of one disk shelf per filer
- ◆ a maximum cluster configuration

You must cable the cluster in the following order:

- ◆ Cable the Channel A connections on your filer and disk shelves
- ◆ Cable the Channel B connections on your disk shelves
- ◆ Cable the cluster by
 - ❖ using the cluster interconnect cable to connect the cluster interconnect adapter in each filer
 - ❖ connecting the Channel B connection between disk shelf 0 and the partner filer.

Note

An FC-AL interface can connect to a maximum of eight daisy-chained disk shelves. Both filers in a cluster, each with two or more FC-AL interfaces, can connect to disk shelves with a storage capacity of 1.5 TB. The distribution of the 1.5 TB storage capacity for a filer with two or more FC-AL interfaces is left to your discretion.

Assumptions made in this section

The following assumptions are made in this section:

- ◆ You installed your filers and disk shelves in the equipment rack based on the procedures provided in the hardware guides for your filer and disk shelves.

Note

If you mix Fibre Channel StorageShelf FC8s (which contain only 18-GB fibre channel disks) with Fibre Channel StorageShelf FC7s (which contain only 9-GB fibre channel disks) in a loop of daisy-chained disk shelves, one Fibre Channel StorageShelf FC7 (9GB) must be disk shelf 0. Disk shelf 0 is the disk shelf that is directly connected to the filer.

- ◆ You labeled the FC-AL interfaces as described in [“Configuring your cluster for an equipment rack”](#) on page 87.
- ◆ You labeled the LRC card above the EDM card in each disk shelf as Channel A, if this identification is not etched on the disk shelf fans.

Note

Associate a solid-colored label for each Channel A interface. You apply labels of this color on every cable in the loop connected to this interface.

- ◆ You labeled the LRC card below the EDM card in each disk shelf as Channel B, if this identification is not etched on the disk shelf fans.

Note

Identify the color of the label that you applied in the middle of each shelf-to-shelf cable for the Channel A loop. For the Channel B loop, choose the striped label matching the solid-colored label. For example, if you applied a red label for the Channel A loop, use the red-striped label for the Channel B loop.

Cabling a minimum cluster configuration in an equipment rack

How to cable the Channel A loops between your filer and disk shelves in a minimum configuration

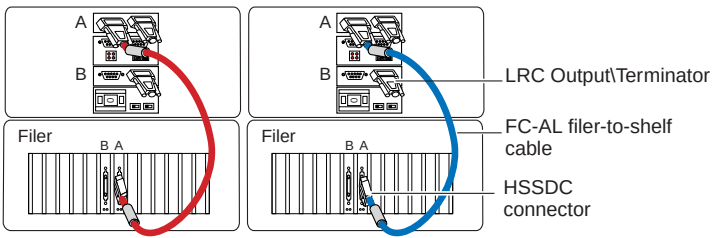
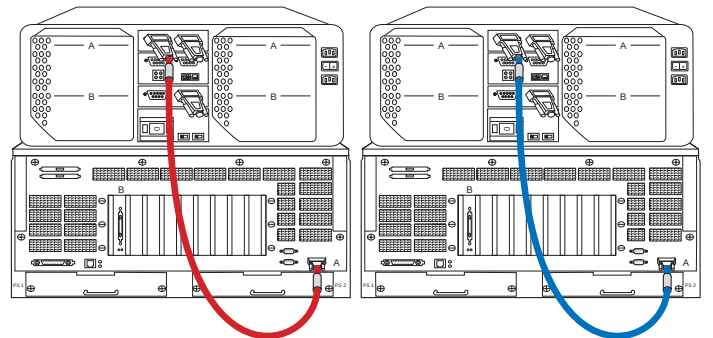
To cable the Channel A connections of your cluster, follow these steps.

Step	Action
1	For an F630 filer: Connect the filer to disk shelf 0 by ◆ Connecting the HSSDC connector on the FC-AL filer-to-shelf cable to the FC-AL adapter labeled Channel A on the filer ◆ Connecting the other DB-9 connector on the FC-AL filer-to-shelf cable to the Input connector of the LRC card labeled Channel A on disk shelf 0 Note_____ Apply a label of the selected color on each end of the cable.
	For an F740 and an F760 filer: Connect the filer to disk shelf 0 by ◆ Connecting a DB-9 connector on the FC-AL filer-to-shelf cable to the onboard FC-AL interface on the filer ◆ Connecting the other DB-9 connector on the FC-AL filer-to-shelf cable to the Input connector of the LRC card labeled Channel A on disk shelf 0 Note_____ Apply a label of the selected color on each end of the cable.
2	Terminate the loop by putting a terminator on the LRC Output/Terminator connector.
3	Repeat Steps 1 through 3 for the partner filer.

Step	Action
	For an F630 filer: The cabling for the minimum configuration should be as shown in the following figure. For an F740 and an F760 filer: The cabling for the minimum configuration should be as shown in the following figure.
4	Proceed to “How to terminate the Channel B loops in a minimum configuration” on page 101.

How to terminate the Channel B loops in a minimum configuration

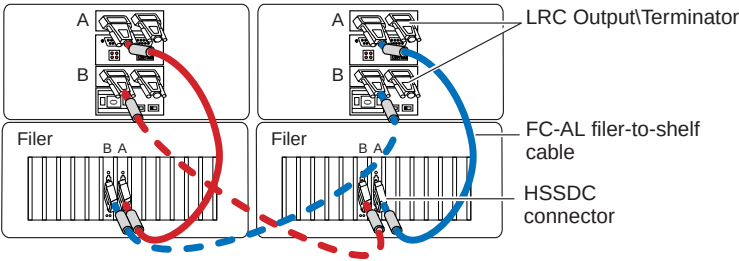
To terminate the Channel B connections of the disk shelves in your minimum cluster configuration, follow these steps.

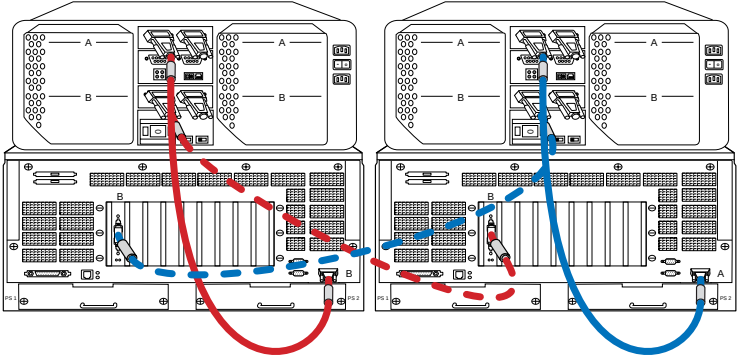
Step	Action
1	Place a terminator on the LRC Output/Terminator connector of the Channel B LRC card. Caution— Do NOT complete the Channel B loop to the partner filer. If you complete the Channel B loop to the partner filer and reboot, the filers try to take ownership of both sets of disks and cause permanent damage to your file systems.
2	Repeat Step 2 for the partner filer. (The Channel A cabling that you did previously is also shown.) For an F630 filer: The result is as shown in the following figure.  For an F740 and an F760 filer: The result is as shown in the following figure. 
3	Proceed to “How to connect the filers in a minimum configuration” on page 102.

How to connect the filers in a minimum configuration

To connect the filers, follow these steps.

Step	Action
1	Run a <code>cf status</code> command on each filer. The resulting output should be as follows: <pre>cluster monitor not initialized. Interconnect is down.</pre>
2	Using the 4m cluster interconnect cable, connect the X port of the cluster interconnect adapter on one filer to the X port on the partner filer. Perform a <code>cf status</code> on each filer. The resulting output should be as follows: <pre>cluster monitor not initialized. Y link is down.</pre> Note_____ The cluster interconnect adapter has two ports; the X port is above the Y port. _____ Caution_____ Verify that you connected the cable to the Y port. Connecting to the wrong port disables the takeover feature. _____
3	Using the 4m cluster interconnect cable, connect the Y port of the cluster interconnect adapter on one filer to the Y port on the partner filer. Perform a <code>cf status</code> on each filer. The resulting output should be as follows: <pre>cluster monitor not initialized.</pre> Note_____ The cluster interconnect adapter has two ports; the Y port is below the X port. _____ Caution_____ Verify that you connected the cable to the Y port. Connecting to the wrong port disables the takeover feature. _____
4	At the consoles of each filer, enter halt to shut down the system.

Step	Action
5	Connect the filer to the Channel B LRC card on disk shelf 0 of the partner filer by ◆ Connecting the HSSDC end of the FC-AL filer-to-shelf cable to the FC-AL adapter labeled Channel B on the filer ◆ Connecting the DB-9 end of the FC-AL filer-to-shelf cable to the Input connector of the LRC card labeled Channel B on disk shelf 0 of the partner filer Note_____ Apply a label on each end of the filer-to-shelf cable. _____
6	Repeat Step 5 for the partner filer. Note_____ These figures only show how to complete the Channel B loop to the partner filer; they do not show the cabling between the cluster interconnect adapters in both filers. The cabling between the cluster interconnect adapters is not shown in these figures to reduce the possible confusion resulting from the number of cables involved. _____ For an F630 filer: The following figure illustrates the completed cabling for the Channel B loops in a minimum configuration.  _____

Step	Action
7	For an F740 and an F760 filer: The following figure illustrates the completed cabling for the Channel B loops in a minimum configuration. 
8	At the console of each filer, enter boot to run the filers.

Cabling a maximum cluster configuration in an equipment rack

How to cable the Channel A loops between your filer and disk shelves in a maximum configuration

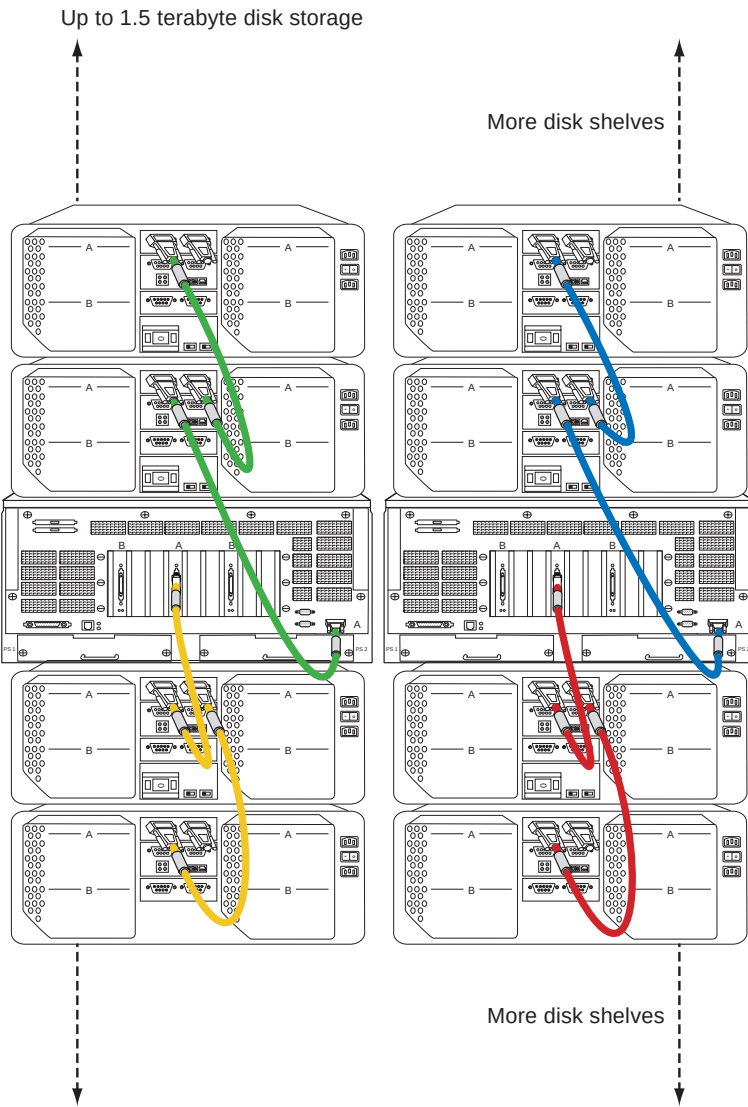
To cable the Channel A connections of your cluster, follow these steps.

Step	Action
1	For an F630 filer: Connect the filer to disk shelf 0 by ◆ Connecting the HSSDC connector on the FC-AL filer-to-shelf cable to one of the FC-AL adapters labeled Channel A on the filer ◆ Connecting the other DB-9 connector on the FC-AL filer-to-shelf cable to the Input connector of the LRC card labeled Channel A on disk shelf 0 Note Apply a label of the selected color on each end of the cable.
	For an F740 and an F760 filer: Connect the filer to disk shelf 0 by ◆ Connecting a DB-9 connector on the FC-AL filer-to-shelf cable to the onboard FC-AL interface on the filer ◆ Connecting the other DB-9 connector on the FC-AL filer-to-shelf cable to the Input connector of the LRC card labeled Channel A on disk shelf 0 Note Apply a label of the selected color on each end of the cable.
2	Connect disk shelf 0 to disk shelf 1 by ◆ Connecting the DB-9 connector of the FC-AL shelf-to-shelf cable to the Output/Terminator connector of the LRC card labeled Channel A on disk shelf 0 ◆ Connecting the other DB-9 connector of the FC-AL shelf-to-shelf cable to the Input connector of the LRC card labeled Channel A on disk shelf 1 Note Apply a label in the middle of the cable.
3	Repeat Step 2 by connecting disk shelf 1 to disk shelf 2, and so on, for the number of disk shelves that you have in this loop.

Step	Action
4	Terminate the daisy-chain by putting a terminator on the LRC card Output/Terminator connector on the last disk shelf.
5	For an F630 filer: Repeat Steps 1 through 4 for all FC-AL adapters labeled Channel A on the filer. For an F740 and an F760 filer: For all remaining FC-AL adapters labeled Channel A on the filer, connect the filer to disk shelf 0 by ◆ Connecting the HSSDC connector on the FC-AL filer-to-shelf cable to the FC-AL adapter labeled Channel A on the filer ◆ Connecting the other DB-9 connector on the FC-AL filer-to-shelf cable to the Input connector of the LRC card labeled Channel A on disk shelf 0 Note Apply a label of the selected color on each end of the cable. Continue by repeating Steps 2 through 4.
6	Repeat Steps 1 through 5 for the partner filer.

Step	Action
	For an F630 filer: The cabling for one possible example of a maximum configuration appears as shown in the following figure. Up to maximum number of disk shelves supporting 1.5 terabytes Up to maximum number of disk shelves supporting 1.5 terabytes

Step	Action
	For an F740 filer: The cabling for one possible example of a maximum configuration appears as shown in the following figure. Up to 1.0 terabyte disk storage 

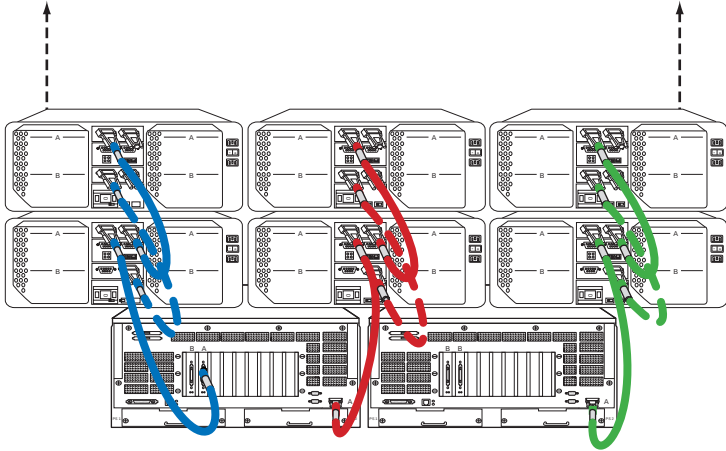
Step	Action
	For an F760 filer: The cabling for one possible example of a maximum configuration appears as shown in the following figure.  Up to 1.5 terabyte disk storage More disk shelves More disk shelves
7	Proceed to “How to cable the Channel B loops between your disk shelves in a maximum configuration” on page 110.

How to cable the Channel B loops between your disk shelves in a maximum configuration

To cable the Channel B connections of the disk shelves in your cluster, follow these steps.

Step	Action
1	Connect disk shelf 0 to disk shelf 1 by ◆ Connecting the DB-9 connector of the FC-AL shelf-to-shelf cable to the Output/Terminator connector of the LRC card labeled Channel B on disk shelf 0 ◆ Connecting the other DB-9 connector of the FC-AL shelf-to-shelf cable to the Input connector of the LRC card labeled Channel B on disk shelf 1 Caution_____ Do NOT complete the Channel B loop to the partner filer. If you complete the Channel B loop to the partner filer and reboot, the filers try to take ownership of both sets of disks and cause permanent damage to your file systems. _____
2	Repeat Step 1 by connecting disk shelf 1 to disk shelf 2, and so on, for the number of disk shelves that you have in this loop.
3	Terminate the daisy-chain by putting a terminator on the LRC Output/Terminator connector on the last disk shelf.
4	Repeat Steps 1 through 3 for all FC-AL adapters labeled Channel B on the filer.
5	Repeat Steps 1 through 5 for the partner filer.

Step	Action
	For an F630 filer: The cabling for one possible example of a maximum configuration appears as shown in the following figure. (The Channel A cabling you did previously is also shown.) The diagram illustrates the cabling for an F630 filer across two columns of disk shelves. Each column contains five shelves, each with two channels labeled A and B. A central 'Filer' unit is connected to both columns. The cabling is as follows: Left Column (Green and Yellow Cables): - Channel A of the top shelf is connected to the top of the Filer. - Channel B of the top shelf is connected to the top of the Filer. - Channel A of the second shelf is connected to the top of the Filer. - Channel B of the second shelf is connected to the top of the Filer. - Channel A of the third shelf is connected to the top of the Filer. - Channel B of the third shelf is connected to the top of the Filer. - Channel A of the fourth shelf is connected to the top of the Filer. - Channel B of the fourth shelf is connected to the top of the Filer. - Channel A of the fifth shelf is connected to the top of the Filer. - Channel B of the fifth shelf is connected to the top of the Filer. Right Column (Blue and Red Cables): - Channel A of the top shelf is connected to the top of the Filer. - Channel B of the top shelf is connected to the top of the Filer. - Channel A of the second shelf is connected to the top of the Filer. - Channel B of the second shelf is connected to the top of the Filer. - Channel A of the third shelf is connected to the top of the Filer. - Channel B of the third shelf is connected to the top of the Filer. - Channel A of the fourth shelf is connected to the top of the Filer. - Channel B of the fourth shelf is connected to the top of the Filer. - Channel A of the fifth shelf is connected to the top of the Filer. - Channel B of the fifth shelf is connected to the top of the Filer. Arrows indicate the range of disk shelves from 'Up to maximum number of disk shelves supporting 1.5 terabytes' at the top to the same at the bottom.

Step	Action
	For an F740 filer: The cabling for one possible example of a maximum configuration appears as shown in the following figure. (The Channel A cabling you did previously is also shown.) Up to 1.0 terabyte disk storage  The diagram illustrates a maximum configuration of F740 filers and disk storage units. It shows three rows of equipment in a rack. The top row consists of three F740 filer units, each with two channels (A and B) and a 1.0 terabyte disk storage unit. The middle row consists of three F740 filer units, each with two channels (A and B) and a 1.0 terabyte disk storage unit. The bottom row consists of two F740 filer units, each with two channels (A and B) and a 1.0 terabyte disk storage unit. The cabling is shown as follows: Blue lines connect the Channel A ports of the filers to the disk storage units. Red lines connect the Channel B ports of the filers to the disk storage units. Green lines connect the Channel A ports of the filers to the disk storage units. Dashed arrows point upwards from the top of the filer units, indicating the direction of the cabling.

Step	Action
	For an F760 filer: The cabling for one possible example of a maximum configuration appears as shown in the following figure. (The Channel A cabling you did previously is also shown.)

Step	Action
6	Turn on the filers and the disk shelves. Among the system messages are the following: <pre> Loop on adapter 7 is open. If adapter is in use, check cabling and seating of LRC cards in FC shelves. isp2100_init: Initialization failed on FC adapter in slot 7. Only 1 Fibre Channel adapter was detected with attached disks, but there are 2 Fibre Channel adapters on the system. Check the cables and the connections for the adapters and disks. No disks were detected on Fibre Channel port B; this node will be unable to takeover correctly. Note_____ These messages occur because the Channel B loop has not been completed. </pre>
7	Proceed to “How to connect the filers in a maximum configuration” on page 115.”

How to connect the filers in a maximum configuration

To connect the filers, follow these steps.

Step	Action
1	Run a <code>cf status</code> command on each filer. The resulting output should be as follows: <pre>cluster monitor not initialized. Interconnect is down.</pre>
2	Using the 4m cluster interconnect cable, connect the X port of the cluster interconnect adapter on one filer to the X port on the partner filer. Perform a <code>cf status</code> on each filer. The resulting output should be as follows: <pre>cluster monitor not initialized. Y link is down.</pre> Note_____ The cluster interconnect adapter has two ports; the X port is above the Y port. _____ Caution_____ Verify that you connected the cable to the Y port. Connecting to the wrong port disables the takeover feature. _____
3	Using the 4m cluster interconnect cable, connect the Y port of the cluster interconnect adapter on one filer to the Y port on the partner filer. Perform a <code>cf status</code> on each filer. The resulting output should be as follows: <pre>cluster monitor not initialized.</pre> Note_____ The cluster interconnect adapter has two ports; the Y port is below the X port. _____ Caution_____ Verify that you connected the cable to the Y port. Connecting to the wrong port disables the takeover feature. _____
4	At the consoles of each filer, enter halt to shut down the system.

Step	Action
5	Connect the filer to the Channel B LRC card on disk shelf 0 of the partner filer by ◆ Connecting the HSSDC end of the FC-AL filer-to-shelf cable to one of the FC-AL adapters labeled Channel B on the filer ◆ Connecting the DB-9 end of the FC-AL filer-to-shelf cable to the Input connector of the LRC card labeled Channel B on disk shelf 0 of the partner filer Note_____ Identify the striped label that you applied in the middle of each shelf-to-shelf cable for the Channel B loop. Apply a label on each end of the filer-to-shelf cable. _____ Repeat this step for the partner filer. The section “How to cable the Channel B loop between the filer and disk shelf 0 in a maximum configuration” on page 117 on the next page illustrates how to complete the Channel B loops to the partner filer.
6	At the console of each filer, enter boot to run the filers.

How to cable the Channel B loop between the filer and disk shelf 0 in a maximum configuration

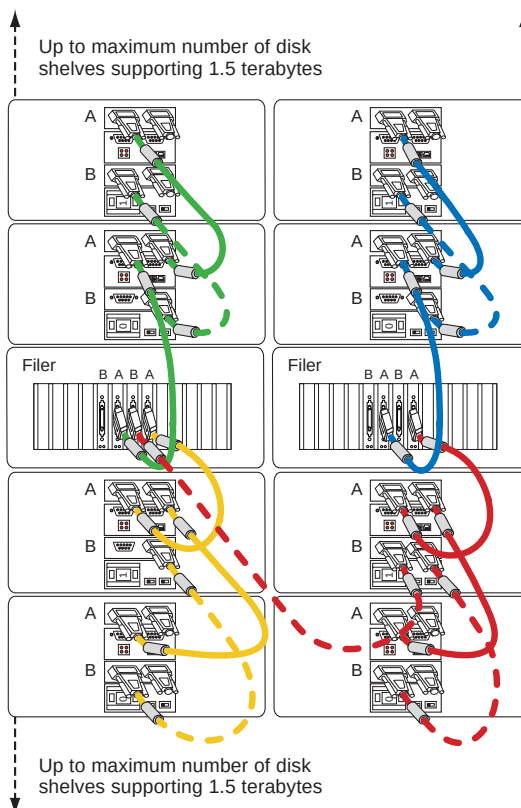
The following series of figures illustrates how to complete the Channel B loops to the partner filer for one possible example of a maximum configuration. The assumption is that the cabling between the cluster interconnect adapters is complete.

Note

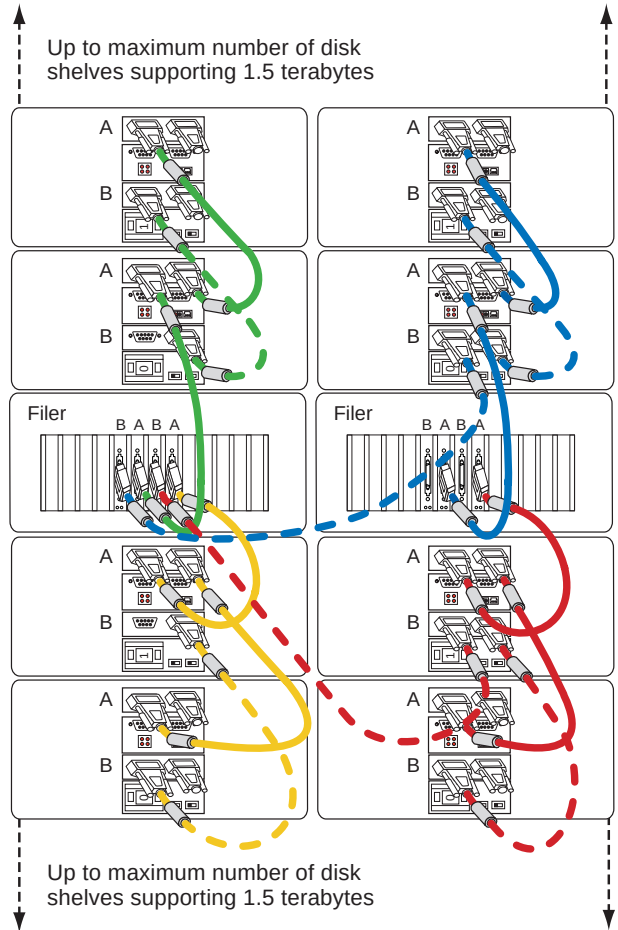
These figures only show how to complete the Channel B loops to the partner filer; they do not show the cabling between the cluster interconnect adapters in both filers. The cabling between the cluster interconnect adapters is not shown in these figures to reduce the possible confusion resulting from the number of cables involved.

For an F630 filer: This configuration has four FC-AL adapters in each filer, with two FC-AL adapters on each filer labeled Channel A and two FC-AL adapters on each filer labeled Channel B.

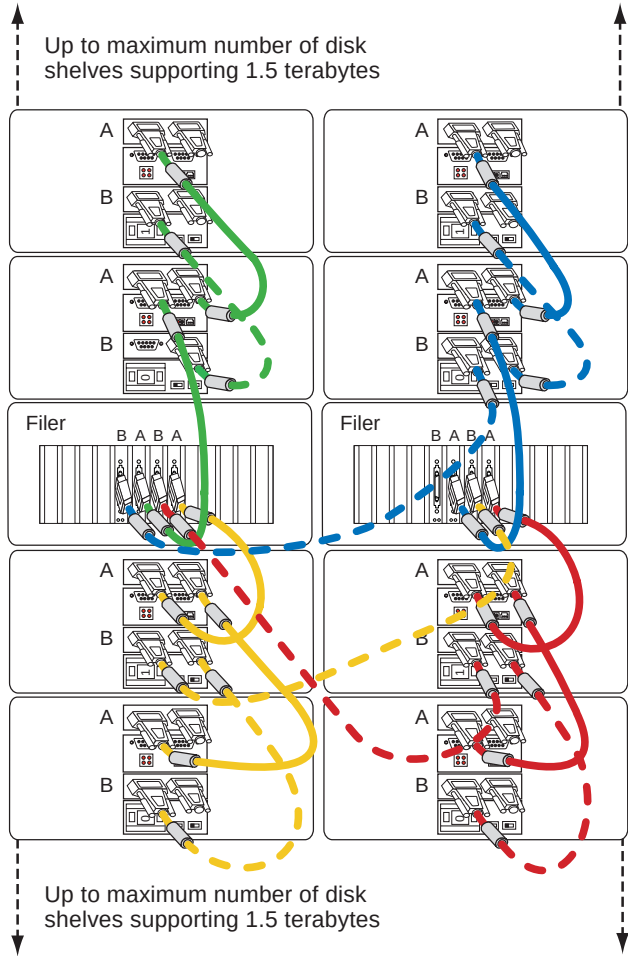
The dashed red line in this figure between the disk shelf on the lower right and the filer on the left illustrates the first completed Channel B loop in this cluster.



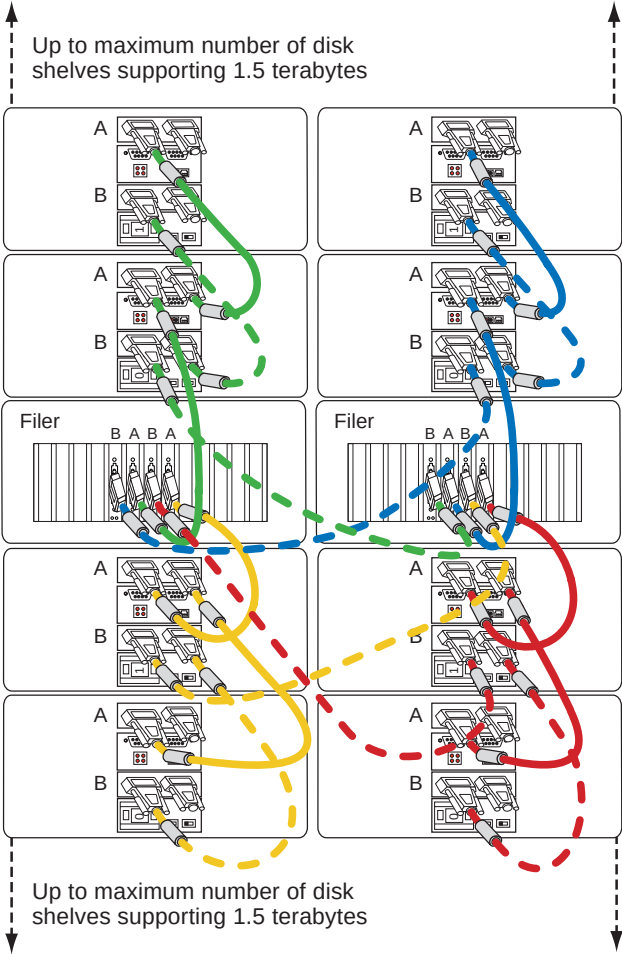
The dashed blue line in this figure between the disk shelf on the upper right and the filer on the left illustrates the second completed Channel B loop in this cluster.



The dashed yellow line in this figure between the disk shelf on the lower left and the filer on the right illustrates the third completed Channel B loop in this cluster.

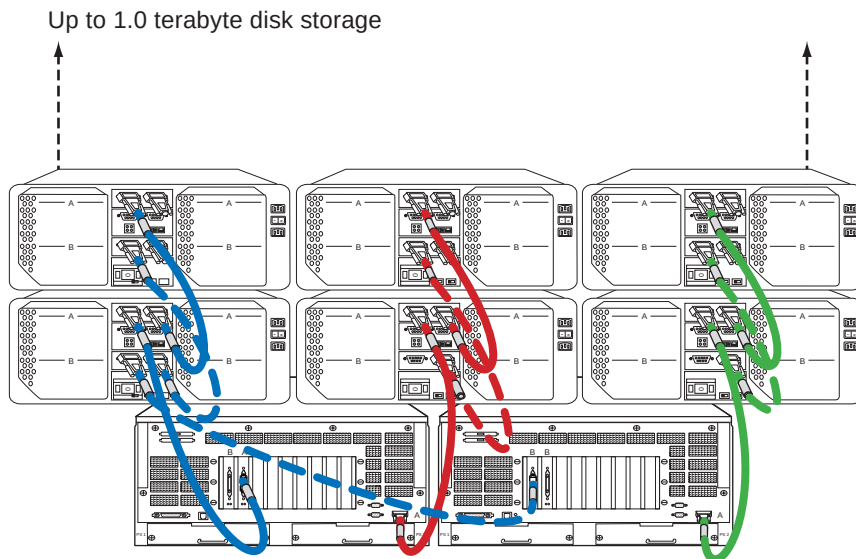


The dashed green line in this figure between the disk shelf on the upper left and the filer on the right illustrates the fourth completed Channel B loop in this cluster.

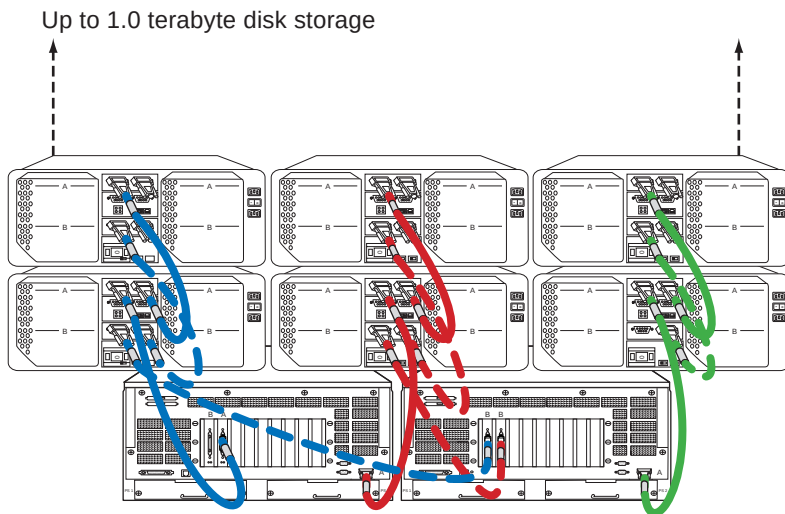


For an 740 filer: This configuration has three FC-AL interfaces in each filer, with two FC-AL interfaces on one filer labeled Channel A and one FC-AL interface on each filer labeled Channel B, and with two FC-AL interfaces on the other filer labeled Channel B and one FC-AL interface on each filer labeled Channel A.

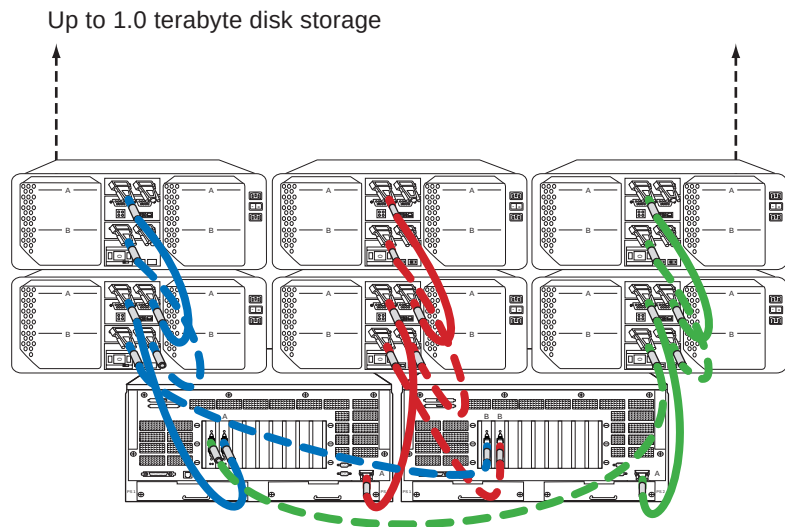
The dashed blue line in this figure between the disk shelf on the left and the filer on the right illustrates the first completed Channel B loop in this cluster.



The dashed red line in this figure between the disk shelf in the middle and the filer on the right illustrates the second completed Channel B loop in this cluster.



The dashed green line in this figure between the disk shelf on the lower right and the filer on the left illustrates the third completed Channel B loop in this cluster.



For an F760 filer: This configuration has four FC-AL interfaces in each filer, with two FC-AL interfaces on each filer labeled Channel A and two FC-AL interfaces on each filer labeled Channel B.

The dashed blue line in this figure between the disk shelf on the upper right and the filer on the left illustrates the first completed Channel B loop in this cluster.



The dashed red line in this figure between the disk shelf on the lower right and the filer on the left illustrates the second completed Channel B loop in this cluster.



The dashed green line in this figure between the disk shelf on the upper left and the filer on the right illustrates the third completed Channel B loop in this cluster.



The dashed yellow line in this figure between the disk shelf on the lower left and the filer on the right illustrates the fourth completed Channel B loop in this cluster.

