

Data ONTAP™ Release 5.0

Quick Start Guide

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 email: support@netapp.com
Information email: info@netapp.com
Web: <http://www.netapp.com>

Part number 210-01811

March, 1998

Legal Information

Copyright

Copyright © 1998 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.

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

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

Portions of this product contain NetBSD, which is copyrighted and publicly distributed by Carnegie Mellon University.

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

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

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

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

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

1. Redistributions of source code must retain the above copyright notices, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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).

Trademarks

Network Appliance and logo, NetApp, and FAServer are registered trademarks of Network Appliance, Inc. in the U.S.A. and other countries. Data ONTAP, SecureShare, NetCache, Web Filer, Filerview, and WAFL are 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.

Table of contents

Chapter 1	Welcome	
	Introduction	1
	Intended audience	1
	Contents of this guide	1
	What to do next	2
Chapter 2	Preparing for Basic and NFS Configuration	
	Introduction	3
	Basic information worksheet	4
	What to do next	6
Chapter 3	Preparing for CIFS Configuration	
	Introduction	7
	What you need to do	7
	Deciding on a domain or workgroup configuration	8
	Introduction	8
	Definition of a domain	8
	Definition of a workgroup	8
	When to install into a Windows NT domain	8
	When to install into a Windows workgroup	9
	Summary of domain and workgroup features	9
	What to do next	10
	Choosing between PC-style or UNIX-style permissions	11
	Introduction	11
	How PC-style permissions work	11
	When to choose PC-style permissions	11
	How UNIX-style permissions work	12
	When to choose UNIX-style permissions	12
	What to do next	12
	CIFS information worksheet.	13
	What to do next	14
	Adding the filer to a Windows NT domain	15
	Introduction	15
	Prerequisites	15
	Procedure	15
	Results	16
	What to do next	16

Chapter 4	Configuring the Filer	
	Introduction	17
	Prerequisites	17
	Procedure	17
	Results	17
	What to do next	18
	Verifying network connections.	19
	Introduction	19
	Procedure	19
	Examples	19
	How to troubleshoot problems	19
	What to do next	19
 Chapter 5	 Configuring HTTP On the Filer	
	Introduction	21
	Prerequisites	21
	Procedure	21
	Results	22
	What to do next	22
 Chapter 6	 Setting Up Password and Group Files	
	Introduction	23
	Who should use this section	23
	The passwd and group files	23
	The default passwd file	23
	The default group file	24
	How the filer uses the passwd and group files	25
	Accessing the files from Windows NT and Windows 95 workstations	25
	Accessing the files from UNIX/ NFS clients	26
	Adding entries to the passwd file	26
	Adding entries to the passwd file with passwords	26
	Adding entries to the passwd file without passwords	27
	Adding entries to the group file	28
	Results	28
	What to do next	28
 Chapter 7	 Configuring Access to CIFS Shares	
	Introduction	29
	Scope of shares access	29
	Introducing the cifs command	29
	Examples of the cifs command	30

Entering commands	31
What to do next	31

Chapter 8

Configuring Clients to Access the Filer

Introduction.	33
What to do next	33
Configuring NFS clients	34
Introduction.	34
Host and interface names	34
If you use DNS or NIS for name resolution	34
If you use /etc/hosts files for name resolution	34
Exporting filer directories	35
Mounting file systems on clients.	35
Procedure	35
Results	35
What to do next	36
Configuring CIFS clients	37
Introduction.	37
Filer is visible to CIFS clients after setup finishes	37
CIFS client connection methods	37
Procedure	38
Results	38
What to do next	38

Chapter 9

About the Filer Software

Introduction.	39
CD and diskette contents	39
Software updates	39
What to do next	40

Chapter 10

Learning About FilerView

Introduction.	41
Prerequisites	41
Accessing FilerView	41
FilerView interface	42
Top frame	42
Bottom frame	43
What to do next	43

Appendix A

Time zones

Chapter 1

Welcome

Introduction

Welcome to the *Data ONTAP™ 5.0 Quick Start Guide*.

Use this guide to get your new Network Appliance® filer configured and operating. If you are upgrading a filer from an older version of Data ONTAP, refer to one of the following documents for upgrade instructions:

- *Upgrade for UNIX*
- *Upgrade for Windows*

Intended audience

The information in this guide is for system administrators who are familiar with basic networking concepts like 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 to seek assistance to complete the initial filer configuration.

Contents of this guide

This guide consists of the information described in the following table.

Chapter or Appendix	Description
Chapter 1, " Welcome "	Contains this introduction.
Chapter 2, " Preparing for Basic and NFS Configuration "	Describes the planning you should do regardless of the protocol licenses you purchased for the filer.
Chapter 3, " Preparing for CIFS Configuration "	Describes the planning and preconfiguration activities you should do if you purchased a license for the CIFS protocol. If you did not purchase a license for the CIFS protocol, you should skip this chapter.

Chapter or Appendix	Description
Chapter 4, "Configuring the Filer"	Describes how to start the filer, use the <code>setup</code> program to enter configuration information, and verify that the filer is communicating on the network after <code>setup</code> finishes.
Chapter 5, "Configuring HTTP On the Filer"	Describes how to configure the filer to deliver HTML service through the HTTP protocol. If you did not purchase a license for the HTTP protocol, you should skip this chapter.
Chapter 6, "Setting Up Password and Group Files"	Describes how to configure the <i>passwd</i> and <i>group</i> files on the filer to authenticate users and groups.
Chapter 7, "Configuring Access to CIFS Shares"	Describes how to assign users and groups access rights to CIFS shares. If you did not purchase a license for the CIFS protocol, you should skip this chapter.
Chapter 8, "Configuring Clients to Access the Filer"	Describes how to configure NFS and CIFS clients so that they can access directories and files on the filer.
Chapter 9, "About the Filer Software"	Describes the software that you received with the filer.
Chapter 10, "Learning About FilerView"	Describes the FilerView™ web-based graphical user interface with which you can manage the filer.
Appendix A, "Time zones"	Lists the names that <code>setup</code> recognizes for time zones.

What to do next

Follow the instructions in ["Preparing for Basic and NFS Configuration"](#) on page 3 to begin the planning process.

Preparing for Basic and NFS Configuration

Introduction

This chapter contains a worksheet that describes the information you supply to configure the basic filer parameters. If you purchased a license for the NFS protocol, no special preparation is needed to enable NFS file service; after the basic configuration information is entered during setup, the filer has all of the information needed to provide NFS file service.

Fill out the Basic Information Worksheet, on pages 4 through 6 so that you are prepared to provide information when `setup` prompts for it.

Basic information worksheet

Filer Host Name					
A unique 1- to 32-character name that uses only alphanumeric characters and hyphens.					
Interfaces					
Filers can contain a maximum of 31 interfaces. The number of interfaces supported by a filer depends on the filer model. The interface names in this table are assigned by the setup program automatically. You should fill in the IP addresses and subnet masks, then record the interface names when the setup program runs.					
Interface Name	IP Address	Subnet Mask	Interface Name	IP Address	Subnet Mask
Default Gateway (optional)					
Name					
IP Address					

Administration Host Information	
Host Name The name of a client to use for administrative tasks, such as - mounting the filer's root directory (/) to an NFS client (if you purchased a license for the NFS protocol) - entering filer commands using the rsh program or a telnet client - sending automatic email to Network Appliance technical support If you do not enter an administration host name and IP address, any NFS client can mount the filer's root file system and modify configuration files.	
IP Address	
Time Zone	
The name of the filer's time zone. Refer to "Time zones" on page 45 for a complete list of time zones.	Default: GMT
DNS Domain Name	
The name of your Domain Name System (DNS) domain, such as netapp.com.	
DNS Servers	
The name and IP addresses of up to three DNS servers.	
DNS Server Name	IP Address
NIS Domain Name	
The name of a Network Information Services (NIS) domain, such as netapp.com.	
Password	
The password required to administer the filer.	

Number of Disks in the Default Volume

The `setup` program creates a default volume. You can choose for the default volume to use from 2 to 14 disks; you can add disks to the default volume after the filer is configured. If you plan to create additional volumes after the filer is set up, do not allocate all your disks to the default volume so that disks remain available for the additional volumes.

To configure multiple volumes or add disks after the filer is configured, refer to Chapter 3, “Managing disks and file systems,” in the *Data ONTAP 5.0 System Administrator’s Guide*.

What to do next

If you purchased a license for the CIFS protocol, continue with Chapter 3, [“Preparing for CIFS Configuration”](#) on page 7; otherwise, continue with Chapter 4, [“Configuring the Filer”](#) on page 17.

Chapter 3

Preparing for CIFS Configuration

Introduction

This chapter contains information for planning CIFS configuration for the filer. If you purchased a license for the CIFS protocol, read this chapter to understand what you need to do to configure CIFS file service; otherwise, continue with Chapter 4, "[Configuring the Filer](#)."

What you need to do

To configure CIFS file service on the filer, you need to

- decide whether to install the filer into a Windows NT domain or Windows workgroup
- gather information that setup prompts you to provide
- add the filer to a Windows NT domain if you selected a Windows NT domain installation

Deciding on a domain or workgroup configuration

Introduction

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.

IMPORTANT: 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

IMPORTANT: 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

IMPORTANT: 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 reenale plain-text passwords.

To reenale 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 reenale plaint-text passwords on a Windows 95 client, consult the following file in 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
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).	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

What to do next

After you decide whether to install the filer into a Windows NT domain or Windows workgroup, read [“Choosing between PC-style or UNIX-style permissions”](#) on page 11 to decide which permission style the filer should use.

Choosing between PC-style or UNIX-style permissions

Introduction

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

This section provides a brief overview of PC-style and UNIX-style permissions and provides guidelines for choosing which style to use. For detailed information about permissions, refer to Chapter 7, “CIFS Administration,” in the *System Administrator's Guide*.

How PC-style permissions work

PC-style permissions are determined by the rights assigned in a share's Access Control List (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-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.

What to do next

After you choose which permission style the filer should use, complete the [CIFS information worksheet](#) on page 13.

CIFS information worksheet

WINS Server Addresses	
The addresses of any Windows Internet Naming Service (WINS) servers for the filer.	
Server #	IP Address
1	
2	
3	
4	
File Permission Style	
Whether the filer is using PC (Windows) or UNIX permissions.	☐ PC ☐ UNIX
Authentication Mode	
Whether you are using a Windows NT domain controller or a UNIX password database for authentication. If the filer is in a Windows workgroup, the filer uses the UNIX password database.	☐ 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.	
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.	

What to do next

Use the following table to decide what to do next.

If...	See...
You decided to make the filer a member of a Windows NT domain	“Adding the filer to a Windows NT domain” on page 15
You decided to make the filer a member of a Windows workgroup	“Configuring the Filer” on page 17

Adding the filer to a Windows NT domain

Introduction

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

NOTE: This section presents one method of adding the filer into a Windows NT domain. For alternative ways of installing the filer into 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 into a Windows NT domain, you must meet the following prerequisites:

- You must have a permanent Windows NT domain.

IMPORTANT: 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).

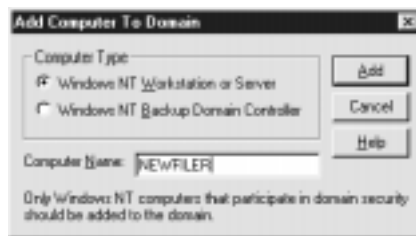
Procedure

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.

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.

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

What to do next

Finish configuring the filer using the instructions in [“Configuring the Filer”](#) on page 17.

Chapter 4

Configuring the Filer

Introduction

This chapter contains instructions for configuring the filer. After you complete the instructions in this chapter, the filer will be running the protocols for which you purchased licenses.

Prerequisites

Install the filer hardware and the serial console according to the instructions in your hardware guide before using the following procedure.

Procedure

1. Turn on the filer's power switch to begin the configuration process.

The first time the filer boots, it runs `setup`.

If `setup` does not run automatically, type `setup` and press the Enter key.

2. Enter the information from the configuration worksheets.

The `setup` program prompts you to enter the configuration information from the Basic Information Worksheet and, if you purchased a license for the CIFS protocol, the CIFS Information Worksheet.

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. Paths such as `/etc/passwd` are referenced as `/vol/vol0/etc/passwd`.

If you purchased a license for the CIFS protocol, `/vol/vol0` is shared as C\$; only the 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.

What to do next

After you configure the filer, follow the instructions in [“Verifying network connections”](#) on page 19 to ensure that the filer is communicating on the network.

Verifying network connections

Introduction

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

At a client attached to the network, enter the following command:

```
ping hostname-interface
```

Replace the variable *hostname* with the host name that you assigned to the filer when you ran `setup`; replace the variable *interface* with one of the interface names that the filer assigned when you ran `setup`.

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 on an Ethernet card containing different media connectors
- the routers function properly with correct routing information if the `ping` command is issued from a network not directly attached to the interface

What to do next

After the `ping` tests indicate that all network interfaces on the filer are working properly, use the following table to decide what to do next.

If you want to...	See...
Configure the filer to provide HTTP file service	Chapter 5, " Configuring HTTP On the Filer " on page 21. If you did not purchase a license for the HTTP protocol, you should skip this chapter.
Configure the filer to authenticate users and groups with <i>passwd</i> and <i>group</i> files	Chapter 6, " Setting Up Password and Group Files " on page 23
Configure the filer to use multiple volumes	Chapter 3, " Managing disks and file systems ," in the <i>System Administrator's Guide</i>

Chapter 5

Configuring HTTP On the Filer

Introduction

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 6, "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 named *vol0* volume, you use the following path:

/vol/vol0/home/html_files

Procedure

Complete the following steps to configure HTTP service:

1. At the filer console, enter the following command to enable the HTTP daemon:

options httpd.enable on

2. Use the following command syntax to specify the root of the path that HTTP requests can use:

options httpd.rootdir *pathname*

For example, if you want HTTP clients to gain access to files or subdirectories under */vol0/home/html_files*, enter

options httpd.rootdir /vol/vol0/home/html_files

When web browsers request files using HTTP, the filer delivers the files using the root directory. For example, if a browser requests the URL *http://toaster/demo/index.htm*, the filer sends the file */vol0/home/html_files/demo/index.htm*.

3. If you want the HTTP service started whenever the filer is booted, use an editor from an NFS or Windows client to add the following lines to the filer's */etc/rc* file:

```
options httpd.enable on
options httpd.rootdir pathname
```

Be sure to replace *pathname* with the path that you selected for the HTTP root directory.

Results

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

What to do next

Use the following table to determine what to do next.

If...	See...
Your filer is not using NIS to authenticate NFS and CIFS users, or your filer is not using a Windows NT domain controller to authenticate CIFS users	Chapter 6, "Setting Up Password and Group Files" on page 23
Your filer is using NIS to authenticate NFS and CIFS users, or your filer is using a Windows NT domain controller to authenticate users	Chapter 8, "Configuring Clients to Access the Filer" on page 33

Chapter 6

Setting Up Password and Group Files

Introduction

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 section

You should use the information in this section if your filer meets any of the following criteria:

- Your filer is licensed for the NFS protocol and does not use NIS to authenticate users.
- Your filer is licensed for the CIFS protocol and does not use a Windows NT domain controller to authenticate users.
- Your filer is licensed for the CIFS protocol and uses a Windows NT domain controller to authenticate users but does not use NIS to authenticate users.

If your filer does not meet any of the preceding criteria, continue with [“Configuring Access to CIFS Shares”](#) on page 29.

The passwd and group files

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

The default passwd file

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

The diagram shows a line from the *passwd* file: `root:o/zowZkYJMELA:0:1:Operator:/:`. Vertical lines connect each field to a label below it. The labels are: User name (root), Encrypted password (o/zowZkYJMELA), UID (0), User's full name (Operator), and Default shell (if any) (/). Additionally, a vertical line connects the field '1' to the label 'GID' above it, and another vertical line connects the field '/' to the label 'UNIX home directory' above it.

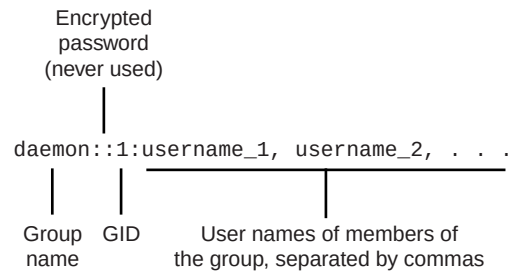
root	:o/zowZkYJMELA	:0	:1	:Operator	:/	
						UNIX home directory
						GID
User name	Encrypted password	UID	User's full name	Default shell (if any)		

The fields in the entry are as follows:

user name	Contains a user name for the user.
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.
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.

The default group file

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



The fields in the entry are as follows:

groupname	Contains a unique group name.
password	Contains a password. This field is never used and is blank.

GID	Contains a unique integer that is the GID.
user name	Contains a comma-separated list of user names that belong to the group.

How the filer uses the passwd and group files

The filer uses *passwd* and *group* files

- to authenticate users for CIFS or PC-NFSD 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*.

Accessing the files from Windows NT and Windows 95 workstations

To access the files from a Windows NT or Windows 95 workstation

1. Map a drive to the root of the default filer volume using the following Universal Naming Convention (UNC) path; replace *filename* with the name of your filer:

`\\filename\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 *passwd* file to authenticate users, use the administration password that you entered when you ran setup.

2. Change to the *etc* directory

Accessing the files from UNIX/NFS clients

To access the files from a UNIX / NFS client

1. Mount the root of the default filer volume to the client's file system using the following path; replace *filename* with the name of your filer:

filename:/vol/vol0

2. Change to the */etc* 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 27.

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, and 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:gid:uid:full name:default shell
```

Follow these steps to add entries to a *passwd* file:

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

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 *passwd* 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 *username*
The *passwd* program prompts you to enter the new password twice.
9. Copy the *passwd* file from the UNIX host to the */etc* directory on the filer.
10. Delete the *passwd* file from the UNIX host and rename the saved file to *passwd*.

Continue with [“Adding entries to the group file”](#) on page 28.

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
```

Follow these steps to add entries:

1. In a text editor, open the *passwd* file from the */etc* directory of the default filer volume.
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.

Continue with [“Adding entries to the group file”](#) on page 28.

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 25
- [“Accessing the files from UNIX / NFS clients”](#) on page 26

Follow these steps to edit the group file:

1. In a text editor, open the *group* file from the */etc* directory of the default filer volume.
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.

What to do next

Use the following table to determine what to do next.

If...	See...
You purchased a license for the CIFS protocol	Chapter 7, “Configuring Access to CIFS Shares” on page 29
You did not purchase a license for the CIFS protocol	Chapter 8, “Configuring Clients to Access the Filer” on page 33

Chapter 7

Configuring Access to CIFS Shares

Introduction

This chapter describes how to assign users and groups access rights to CIFS shares (directories). If you did not purchase a license for the CIFS protocol, continue with Chapter 8, "[Configuring Clients to Access the Filer](#)" on page 33.

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
access	Specifies that an access entry is to be created.
share	Specifies the name of the share.
-g	Specifies that the user group name is a group.

Parameter	Description
user group	Specifies the name of the user or group for which access to the share is granted.
rights	Specifies which rights the user or group have to the share. Rights are specified by three characters—<code>rwX</code>—which stand for read, write, and execute. A dash (-) in any position denies the user the right specified by the character it replaces. Examples: <code>rwX</code> grants read, write, and execute rights. <code>r--</code> grants only the right to read files. <code>rw-</code> grants only the rights to read and write files. <code>r-X</code> 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
- Follow these steps to establish access to shares:
1. Select a method for entering filer commands.
 2. Enter the `cifs` 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.
- What to do next** Follow the instructions in Chapter 8, ["Configuring Clients to Access the Filer"](#) on page 33.

Chapter 8

Configuring Clients to Access the Filer

Introduction

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 you...	See...
Purchased a license for the NFS protocol	“Configuring NFS clients” on page 34
Purchased a license for the CIFS protocol	“Configuring CIFS clients” on page 37

Configuring NFS clients

Introduction

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 37.

Host 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:

```
255.255.255.145    toaster-e0 toaster
255.255.255.155    toaster-e1
255.255.255.165    toaster-f0
255.255.255.175    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:

```
255.255.255.145    toaster-e0 toaster
255.255.255.155    toaster-e1
255.255.255.165    toaster-f0
255.255.255.175    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 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* files, 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.

1. Create a directory on the client to act as a mount point. For example, */n/toaster/home*.
2. To mount the filer's */vol/vol0/home* directory to */n/toaster/home*, add the following line to the client's */etc/fstab* or */etc/vfstab* file:

```
toaster-e0:/vol/vol0/home /n/toaster/home nfs rw 0 0
```

In the preceding example, the client is on the same network as the filer Ethernet interface *e0*. If the client is on the same network as Ethernet interface *e1*, use the following line instead:

```
toaster-e1:/vol/vol0/home /n/toaster/home nfs rw 0 0
```

The file system is mounted when the client reboots.

3. To mount the */vol/vol0/home* directory without a client reboot, enter the following command at the client:

```
mount toaster-e1:/vol/vol0/home /n/toaster/home
```

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 you...	See...
Purchased a license for the CIFS protocol	“Configuring CIFS clients” on page 37
Did not purchase a license for the CIFS protocol	Chapter 9, ”About the Filer Software” on page 39

Configuring CIFS clients

Introduction

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 <code>net use</code> command	<code>net use</code> command	Map a share to a drive letter on the command line. For example: <code>net use f:\\toaster\home</code>

Procedure

Follow these steps to inform users how to access the filer.

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:

`\\computer_name\share_name`

For example: If the filer is named toaster and the directory that contains users' directories is shared with the name home, the UNC path is `\\toaster\home`.

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.

What to do next

Read Chapter 9, "[About the Filer Software](#)" on page 39 to learn about the software that you received with the filer.

Chapter 9

About the Filer Software

Introduction

This chapter describes the software that shipped with the filer.

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

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

CD and diskette contents

The following list describes the CD and system boot diskette:

Data ONTAP CD	This CD contains the system software and documentation. If you need to reinstall the system software for any reason, you need this CD; call Network Appliance Technical Support for instructions before reinstalling system software on the filer. The Data ONTAP CD 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, read the file named <i>intro.txt</i> on the CD.
System boot diskette	If the filer fails to boot from hard disk, or if you forget your password, you must boot the filer from the system boot diskette.
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>.

What to do next

The filer is now configured and operational. Your clients can access the filer to store and retrieve files. Use the following table to determine what to do next.

If you want to...	See...
Learn about the FilerView product, the Network Appliance web-based administration tool for Data ONTAP	Chapter 10, " Learning About FilerView " on page 41
Learn about managing Data ONTAP using commands	The Data ONTAP 5.0 <i>System Administrator's Guide</i>
Learn how to install the Data ONTAP MIB on your management station	The Data ONTAP 5.0 <i>System Administrator's Guide</i>

Chapter 10

Learning About FilerView

Introduction

This chapter introduces FilerView, the Network Appliance web-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

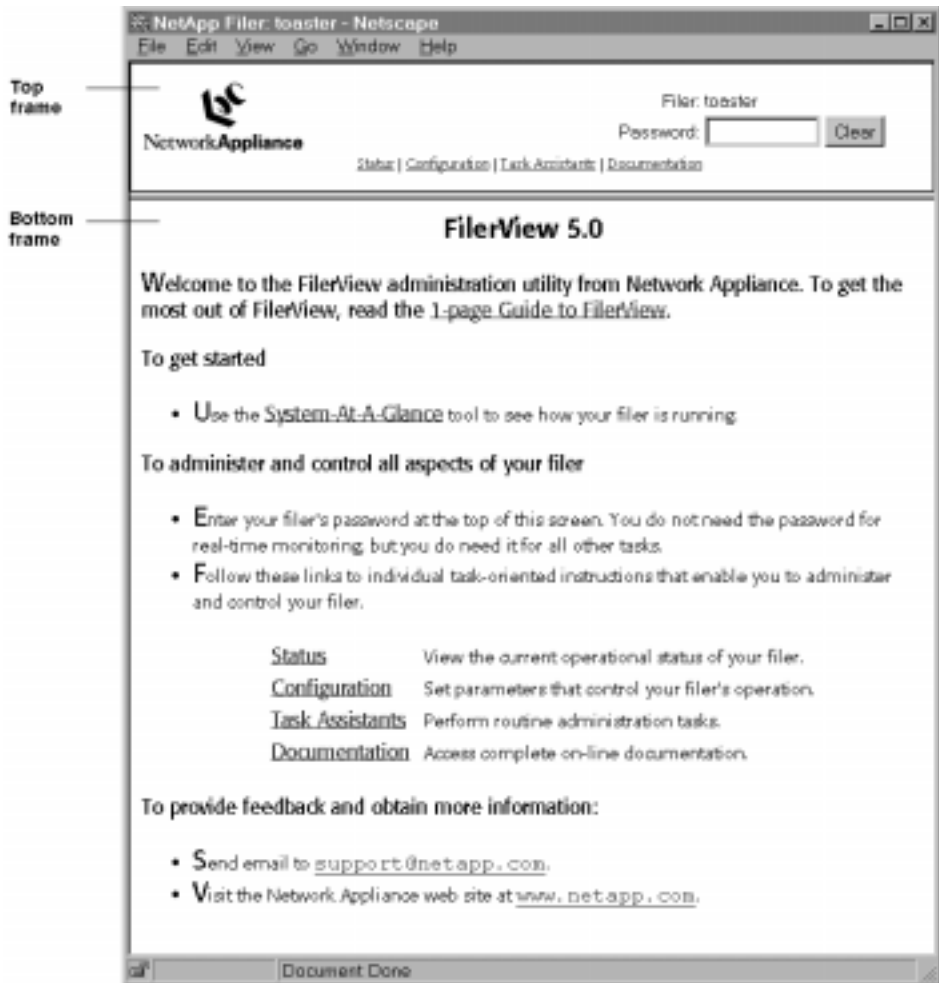
You need Netscape Navigator 3.0 or later to access FilerView. FilerView has not been tested with other web browsers.

Accessing FilerView

To access FilerView, point your browser to `http://hostname/na_admin`, substituting the filer name for *hostname*. For example, if your host's name is toaster, enter the following URL:

`http://toaster/na_admin`

When your browser connects to FilerView, you see the following page:



FilerView interface

The FilerView interface consists of two frames: a top frame and a bottom frame.

Top frame

The top frame contains a password field and navigation links.

You must enter the filer's administration password in the Password field before you can perform any tasks with FilerView.

The following table describes the navigation links.

Navigation Link	Description
Status	The Status link displays a page from which you can view filer status and launch Java applets that monitor filer performance in real time.
Configuration	The Configuration link displays a page and links from which you can view and change all the filer configuration parameters.
Task Assistants	The Task Assistants link displays a page from which you can select links that enable you to perform common management tasks, such as managing NFS exports and CIFS shares, editing the hosts file, editing quotas, and managing disks and volumes.
Documentation	The Documentation link displays a page from which you can select links that display the FilerView guide and man pages.

Bottom frame

The bottom frame contains a welcome page initially.

As you select links from the welcome page or from the navigation links in the top frame, the bottom frame changes to display forms that provide information about the filer configuration or statistics about filer operation. All the forms that FilerView displays contain a Help button that enables you to display information about how to use them.

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

Some configuration files cannot be changed directly in forms. When you need to perform tasks that require changes to these configuration files, FilerView uses Java applets to display a separate window in which you make modifications.

What to do next

You're ready to begin using FilerView to administer the filer. Point your browser to `http://hostname/na_admin` (using the filer name in place of hostname), and begin exploring FilerView features.

Select the Documentation link to learn more about FilerView features, and use the Help button on individual forms to get information about using them.

Appendix A

Time zones

You must enter one of the following time zones when the setup program prompts for a time zone.

Africa	Africa/Porto-Novo	America/Guatemala	America/Rosario
Africa/Abidjan	Africa/Sao_Tome	America/Guayaquil	America/Santiago
Africa/Accra	Africa/Timbuktu	America/Guyana	America/Santo_Domingo
Africa/Addis_Ababa	Africa/Tripoli	America/Halifax	America/Sao_Paulo
Africa/Algiers	Africa/Tunis	America/Havana	America/Scoresbysund
Africa/Asmera	Africa/Windhoek	America/Indiana	America/Shiprock
Africa/Bamako		America/Indianapolis	America/St_Johns
Africa/Bangui	America	America/Inuvik	America/St_Kitts
Africa/Banjul	America/Adak	America/Iqaluit	America/St_Lucia
Africa/Bissau	America/Anchorage	America/Jamaica	America/St_Thomas
Africa/Blantyre	America/Anguilla	America/Jujuy	America/St_Vincent
Africa/Brazzaville	America/Antigua	America/Juneau	America/Swift_Current
Africa/Bujumbura	America/Aruba	America/Knox_IN	America/Tegucigalpa
Africa/Cairo	America/Asuncion	America/La_Paz	America/Thule
Africa/Casablanca	America/Atka	America/Lima	America/Thunder_Bay
Africa/Conakry	America/Barbados	America/Los_Angeles	America/Tijuana
Africa/Dakar	America/Belize	America/Louisville	America/Tortola
Africa/Dar_es_Salaam	America/Bogota	America/Maceio	America/Vancouver
Africa/Djibouti	America/Boise	America/Managua	America/Virgin
Africa/Douala	America/Buenos_Aires	America/Manaus	America/Whitehorse
Africa/Freetown	America/Caracas	America/Martinique	America/Winnipeg
Africa/Gaborone	America/Catamarca	America/Mazatlan	America/Yakutat
Africa/Harare	America/Cayenne	America/Mendoza	America/Yellowknife
Africa/Johannesburg	America/Cayman	America/Menominee	
Africa/Kampala	America/Chicago	America/Mexico_City	Antarctica
Africa/Khartoum	America/Cordoba	America/Miquelon	Antarctica/Casey
Africa/Kigali	America/Costa_Rica	America/Montevideo	Antarctica/DumontDurville
Africa/Kinshasa	America/Cuiaba	America/Montreal	Antarctica/Mawson
Africa/Lagos	America/Curacao	America/Montserrat	Antarctica/McMurdo
Africa/Libreville	America/Dawson	America/Nassau	Antarctica/Palmer
Africa/Lome	America/Dawson_Creek	America/New_York	Antarctica/South_Pole
Africa/Luanda	America/Denver	America/Nipigon	
Africa/Lumumbashi	America/Detroit	America/Nome	Asia
Africa/Lusaka	America/Dominica	America/Noronha	Asia/Aden
Africa/Malabo	America/Edmonton	America/Panama	Asia/Alma-Ata
Africa/Maputo	America/El_Salvador	America/Pangnirtung	Asia/Amman
Africa/Maseru	America/Ensenada	America/Paramaribo	Asia/Anadyr
Africa/Mbabane	America/Fort_Wayne	America/Phoenix	Asia/Aqtai
Africa/Mogadishu	America/Fortaleza	America/Port_of_Spain	Asia/Aqtobe
Africa/Monrovia	America/Glace_Bay	America/Port-au-Prince	Asia/Ashkhabad
Africa/Nairobi	America/Godthab	America/Porto_Acre	Asia/Baghdad
Africa/Ndjamena	America/Goose_Bay	America/Puerto_Rico	Asia/Bahrain
Africa/Niamey	America/Grand_Turk	America/Rainy_River	Asia/Baku
Africa/Nouakchott	America/Grenada	America/Rankin_Inlet	Asia/Bangkok
Africa/Ouagadougou	America/Guadeloupe	America/Regina	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/DeNoronha
Brazil/East
Brazil/West

Canada

Canada/Atlantic
Canada/Central
Canada/East-
Saskatchewan
Canada/Eastern
Canada/Mountain

Canada/Newfoundland
Canada/Pacific
Canada/Saskatchewan
Canada/Yukon

Chile

Chile/Continental
Chile/EasterIsland

Etc

Etc/GMT
Etc/GMT+0
Etc/GMT+1
Etc/GMT+2
Etc/GMT+3
Etc/GMT+4
Etc/GMT+5
Etc/GMT+6
Etc/GMT+7
Etc/GMT+8
Etc/GMT+9
Etc/GMT+10
Etc/GMT+11
Etc/GMT+12
Etc/GMT0
Etc/GMT-0
Etc/GMT-1
Etc/GMT-2
Etc/GMT-3
Etc/GMT-4
Etc/GMT-5
Etc/GMT-6
Etc/GMT-7
Etc/GMT-8
Etc/GMT-9
Etc/GMT-10
Etc/GMT-11
Etc/GMT-12
Etc/GMT-13
Etc/GMT-14
Etc/Greenwich
Etc/UCT
Etc/Universal
Etc/UTC
Etc/Zulu

Europe

Europe/Amsterdam
Europe/Andorra
Europe/Athens
Europe/Belfast
Europe/Belgrade
Europe/Berlin
Europe/Bratislava

Europe/Brussels
Europe/Bucharest
Europe/Budapest
Europe/Chisinau
Europe/Copenhagen
Europe/Dublin
Europe/Gibraltar
Europe/Helsinki
Europe/Istanbul
Europe/Kiev
Europe/Kuybyshev
Europe/Lisbon
Europe/Ljubljana
Europe/London
Europe/Luxembourg
Europe/Madrid
Europe/Malta
Europe/Minsk
Europe/Monaco
Europe/Moscow
Europe/Oslo
Europe/Paris
Europe/Prague
Europe/Riga
Europe/Rome
Europe/San_Marino
Europe/Sarajevo
Europe/Simferopol
Europe/Skopje
Europe/Sofia
Europe/Stockholm
Europe/Tallinn
Europe/Tirane
Europe/Vaduz
Europe/Vatican
Europe/Vienna
Europe/Vilnius
Europe/Warsaw
Europe/Zagreb
Europe/Zurich

GMT

GMT
GMT+1
GMT+2
GMT+3
GMT+4
GMT+5
GMT+6
GMT+7
GMT+8
GMT+9
GMT+10
GMT+11

GMT+12	Egypt	Pacific/Apia	Pacific/Yap
GMT+13	Eire	Pacific/Auckland	
GMT-1	EST	Pacific/Chatham	System V
GMT-2	EST5EDT	Pacific/Easter	SystemV/AST4
GMT-3	Factory	Pacific/Efate	SystemV/AST4ADT
GMT-4	GB	Pacific/Enderbury	SystemV/CST6
GMT-5	GB-Eire	Pacific/Fakaofu	SystemV/CST6CDT
GMT-6	Greenwich	Pacific/Fiji	SystemV/EST5
GMT-7	Hongkong	Pacific/Funafuti	SystemV/EST5EDT
GMT-8	HST	Pacific/Galapagos	SystemV/HST10
GMT-9	Iceland	Pacific/Gambier	SystemV/MST7
GMT-10	Iran	Pacific/Guadalcanal	SystemV/MST7MDT
GMT-11	Israel	Pacific/Guam	SystemV/PST8
GMT-12	Jamaica	Pacific/Honolulu	SystemV/PST8PDT
	Japan	Pacific/Johnston	SystemV/YST9
	Kwajalein	Pacific/Kiritimati	SystemV/YST9YDT
Indian (Indian Ocean)	Libya	Pacific/Kosrae	
Indian/Antananarivo	MET	Pacific/Kwajalein	US (United States)
Indian/Chagos	MST	Pacific/Majuro	US/Alaska
Indian/Cocos	MST7MDT	Pacific/Marquesas	US/Aleutian
Indian/Comoro	Navajo	Pacific/Midway	US/Arizona
Indian/Kerguelen	NZ	Pacific/Nauru	US/Central
Indian/Mahe	NZ-CHAT	Pacific/Niue	US/East-Indiana
Indian/Maldives	Poland	Pacific/Norfolk	US/Eastern
Indian/Mauritius	Portugal	Pacific/Noumea	US/Hawaii
Indian/Mayotte	PRC	Pacific/Pago_Pago	US/Indiana-Starke
Indian/Reunion	PST8PDT	Pacific/Palau	US/Michigan
	ROC	Pacific/Pitcairn	US/Mountain
Mexico	ROK	Pacific/Ponape	US/Pacific
Mexico/BajaNorte	Singapore	Pacific/Port_Moresby	US/Pacific-New
Mexico/BajaSur	Turkey	Pacific/Rarotonga	US/Samoa
Mexico/General	UCT	Pacific/Saipan	
	Universal	Pacific/Samoa	Aliases
Miscellaneous	UTC	Pacific/Tahiti	GMT=Greenwich, UCT,
Arctic/Longyearbyen	WET	Pacific/Tarawa	UTC, Universal, Zulu
CET	W-SU	Pacific/Tongatapu	CET=MET (Middle
CST6CDT	Zulu	Pacific/Truk	European Time)
Cuba		Pacific/Wake	US/Eastern=Jamaica
EET	Pacific	Pacific/Wallis	US/Mountain=Navajo