

PMDF Installation Guide Linux Edition

Order Number: S-5302-66-NN-L

February 2020

This document describes the installation and configuration of version 6.8 of the PMDF-MTA, PMDF-MSGSTORE, and PMDF-TLS software on a Linux system.

Revision/Update Information: This manual supersedes the V6.7 *PMDF Installation Guide, Linux Edition*.

Software Version: PMDF V6.8

Operating System and Version: Red Hat Enterprise Linux 7.0 or later on x86_64; (or other compatible Linux distribution)

Copyright ©2020 Process Software, LLC.
Unpublished — all rights reserved under
the copyright laws of the United States

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means electronic, mechanical, magnetic, optical, chemical, or otherwise without the prior written permission of:

Process Software, LLC
959 Concord Street
Framingham, MA 01701-4682 USA
Voice: +1 508 879 6994; FAX: +1 508 879 0042
info@process.com

Process Software, LLC ("Process") makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Process Software reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Process Software to notify any person of such revision or changes.

Use of PMDF, PMDF-MSGSTORE, PMDF-MTA, and/or PMDF-TLS and associated documentation is authorized only by a Software License Agreement. Such license agreements specify the number of systems on which the software is authorized for use, and, among other things, specifically prohibit use or duplication of software or documentation, in whole or in part, except as authorized by the Software License Agreement.

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 252.227-7013 or as set forth in the Commercial Computer Software — Restricted Rights clause at FAR 52.227-19.

The PMDF mark and all PMDF-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries and are used under license.

ALL-IN-1, Alpha AXP, AXP, Bookreader, DEC, DECnet, HP, I64, IA64, Integrity, MAILbus, MailWorks, Message Router, MicroVAX, OpenVMS, Pathworks, PSI, RMS, TeamLinks, TOPS-20, Tru64, TruCluster, ULTRIX, VAX, VAX Notes, VMScluster, VMS, and WPS-PLUS are registered trademarks of Hewlett-Packard Company.

AS/400, CICS, IBM, Office Vision, OS/2, PROFS, and VTAM are registered trademarks of International Business Machines Corporation. CMS, DISOSS, OfficeVision/VM, OfficeVision/400, OV/VM, and TSO are trademarks of International Business Machines Corporation.

dexNET is a registered trademark of Fujitsu Imaging Systems of America, Inc.

FaxBox is a registered trademark of DCE Communications Group Limited.

InterConnections is a trademark of InterConnections, Inc.

LANmanager and Microsoft are registered trademarks of Microsoft Corporation.

MHS, Netware, and Novell are registered trademarks of Novell, Inc.

PGP and Pretty Good Privacy are registered trademarks of Pretty Good Privacy, Inc.

Attachmate is a registered trademark and PathWay is a trademark of Attachmate Corporation.

PostScript is a registered trademark of Adobe Systems Incorporated.

SPARC is a trademark of SPARC International, Inc.

UNIX is a registered trademark of UNIX System Laboratories, Inc.

Gold-Mail is a trademark of Data Processing Design, Inc.

libedit/editline is Copyright (c) 1992, 1993, The Regents of the University of California. All rights reserved.

AlphaMate is a registered trademark of Motorola, Inc.

cc:Mail is a trademark of cc:Mail, Inc., a wholly-owned subsidiary of Lotus Development Corporation. Lotus Notes is a registered trademark of Lotus Development Corporation.

RC2 and RC4 are registered trademarks of RSA Data Security, Inc.

Ethernet is a registered trademark of Xerox Corporation.

GIF and "Graphics Interchange Format" are trademarks of CompuServe, Incorporated.

InterDrive is a registered trademark of FTP Software, Inc.

Memo is a trade mark of Verimaton ApS.

LaserJet and PCL are registered trademarks of Hewlett-Packard Company.

Jnet is a registered trademark of Wingra, Inc.

Pine and Pico are trademarks of the University of Washington, used by permission.

Solaris, Sun, and SunOS are trademarks of Sun Microsystems, Inc.

TCPware and MultiNet are registered trademarks of Process Software.

TIFF is a trademark of Aldus Corporation.

Copyright (c) 1990-2000 Sleepycat Software. All rights reserved.

Contents

CHAPTER 1	INSTALLING PMDF AND PMDF LAYERED PRODUCTS	1-1
1.1	WHAT YOU SHOULD HAVE	1-1
1.1.1	Supported Linux Versions _____	1-1
1.1.2	Distribution Media _____	1-1
1.1.3	Disk Space Requirements _____	1-2
1.2	PRELIMINARY TASKS FOR NEW INSTALLATIONS	1-2
1.2.1	Create PMDF and PMDFUSER Accounts _____	1-2
1.2.1.1	Using GROUPADD and USERADD to Add the Accounts •	1-3
1.2.1.2	Editing the /etc/passwd and /etc/shadow Files to Add the Accounts •	1-3
1.3	PRELIMINARY TASKS FOR UPGRADE INSTALLATIONS	1-4
1.3.1	Prepare to Convert Databases _____	1-4
1.3.2	Save Tailor File _____	1-4
1.4	STEP-BY-STEP INSTALLATION INSTRUCTIONS	1-4
1.5	POST-INSTALLATION TASKS FOR UPGRADES	1-6
1.6	POST-INSTALLATION TASKS FOR NEW SITES	1-8
1.7	DEINSTALLING PMDF	1-12
1.7.1	Step-by-Step Deinstallation Instructions _____	1-12
1.7.2	Problems Deinstalling _____	1-12
1.8	AFTER UPGRADING THE LINUX OPERATING SYSTEM	1-13
<hr/>		
CHAPTER 2	PMDF EXAMPLE INSTALLATION	2-1
<hr/>		
CHAPTER 3	GENERATING AN INITIAL PMDF CONFIGURATION	3-1
3.1	BEFORE YOU BEGIN	3-1
3.1.1	Selecting a System Name _____	3-1
3.1.2	Authentication and Security _____	3-2
3.2	USING THE WEB-BASED PMDF-MTA CONFIGURATION UTILITY	3-2
3.3	USING THE COMMAND LINE CONFIGURATION PROCEDURE	3-3
<hr/>		
CHAPTER 4	CONFIGURING PMDF POP AND IMAP MAILBOX SERVERS	4-1
4.1	BEFORE YOU BEGIN	4-1
4.2	USING THE WEB-BASED POP AND IMAP MAILBOX SERVERS CONFIGURATION UTILITY	4-3
4.3	USING THE COMMAND LINE POP AND IMAP MAILBOX SERVERS CONFIGURATION UTILITY	4-4

Contents

CHAPTER 5	PMDF-MTA AND IMAP EXAMPLE CONFIGURATION	5-1
5.1	COMMAND LINE EXAMPLE CONFIGURATION	5-2
5.1.1	MTA/SMTP Sample Configuration _____	5-2
5.1.2	IMAP/POP Server Sample Configuration _____	5-7
5.2	WEB-BASED EXAMPLE CONFIGURATION	5-12
5.3	MTA/SMTP CONFIGURATION	5-13
5.4	IMAP/POP SERVER SAMPLE CONFIGURATION	5-21

CHAPTER 6	CONFIGURING PMDF-MTA TO ACT AS AN E-MAIL FIREWALL	6-1
6.1	BEFORE YOU BEGIN	6-1
6.2	USING THE FIREWALL CONFIGURATION UTILITY	6-3

CHAPTER 7	E-MAIL FIREWALL EXAMPLE CONFIGURATION	7-1
------------------	--	------------

INDEX

EXAMPLES

2-1	Example Installation _____	2-1
5-1	Sample pmdf configure mta dialogue _____	5-2
5-2	Sample pmdf configure mailbox_servers dialogue _____	5-7
7-1	Example PMDF-MTA configuration as a firewall _____	7-3
7-2	Example checklist file for firewall configuration _____	7-9

FIGURES

5-1	Sample PMDF Site EXAMPLE.COM _____	5-1
5-2	HTTP Server Standalone Main Page _____	5-13
5-3	HTTP Server Main Page _____	5-14
5-4	Configuration Main Page _____	5-15
5-5	PMDF-MTA/SMTP Configuration, Local Host Information _____	5-16
5-6	PMDF-MTA/SMTP Configuration, Local Network Information _____	5-17
5-7	PMDF-MTA/SMTP Configuration, Security Information _____	5-18
5-8	PMDF-MTA/SMTP Configuration, Final Details Page _____	5-19
5-9	Configuration Main Page, MTA Configuration Entered _____	5-20
5-10	IMAP/POP Configuration, Select Servers _____	5-21
5-11	IMAP/POP Configuration, popstore/MessageStore Information _____	5-22
5-12	IMAP/POP Configuration, Server Information _____	5-23
5-13	Configuration Main Page, MTA and IMAP/POP Configurations Entered _____	5-24
5-14	Generate Files _____	5-25
5-15	MTA and IMAP/POP Checklist File _____	5-26
7-1	Sample PMDF Site EXAMPLE.COM _____	7-1

1 Installing PMDF and PMDF layered products

This chapter presents the procedure for installing version 6.8 of PMDF on a Linux system.

If you are installing any PMDF add-on layered product *e.g.*, PMDF-TLS, such product has been included with the base PMDF kit on your distribution media.

You will *not* be asked during the installation procedure what components should be installed along with PMDF. Everything is installed. For each additional component, however, you will need an additional license in order to activate that component.

1.1 What You Should Have

Prior to performing an installation or upgrade you should have received a PMDF distribution kit containing the distribution media and any necessary licenses. You can install PMDF including all components even if you do not currently have a license for a given component: you just will not be able to use that component until you have installed the proper license.

1.1.1 Supported Linux Versions

The Linux kit is supplied as an RPM kit, and is built on Red Hat Enterprise Linux version 6.10 update 8 on an x86_64 64-bit processor. It should work on any distribution of 64-bit Linux that supports RPM installations. It will not install or work on 32-bit systems.

The Linux core version supported is 2.6.32-696 or later.

1.1.2 Distribution Media

PMDF for Linux is distributed on a single CD-ROM. Included on the CD-ROM are all the PMDF layered products. The PMDF for Linux product family includes the following:

- PMDF-MTA
- PMDF-MSGSTORE
- PMDF-TLS

Installing PMDF and PMDF layered products

What You Should Have

Prior to installation, the CD-ROM should be inserted into a CD-ROM drive accessible to the system. The exact command to use to mount a CD-ROM varies from one Linux distribution to the next. On Red Hat Enterprise Linux, mount the CD-ROM as follows:

```
# cd /  
# mount -o ro file-system directory
```

where *file-system* is the CD-ROM device, and *directory* is the location in the file tree file tree where you want to attach the PMDF distribution files. Usually the file-system can be found at `/dev/cdrom`. If this is the case, and you want to put the PMDF distribution files under `/cdrom`, you would use the following commands:

```
# cd /  
# mount -o ro /dev/cdrom /cdrom
```

The PMDF kit for Linux is located under the directory `/Linux-X86/PMDF680` on the CD-ROM. Thus the example above would result in the Linux kit being present under `/cdrom/Linux-X86/PMDF680`.

The PMDF on-line documentation resides on the PMDF distribution CD-ROM under the directory `/documentation`.

Once mounted, use the RPM installation procedure as presented in Section 1.4. Or, if you move the PMDF RPM kit to disk, you can install PMDF from that on-disk copy similarly, specifying as the location argument to RPM the path to the kit's directory.

1.1.3 Disk Space Requirements

The PMDF on Linux kit requires 76 MB of free space in the partition on which you install PMDF (by default `/opt`). You can use the `df` command to check total space and free space for the filesystems in which you want to have PMDF reside.

1.2 Preliminary Tasks for New Installations

There are several tasks that should be performed prior to installing PMDF for the first time. These tasks are outlined in the sections below.

1.2.1 Create PMDF and PMDFUSER Accounts

You must add two user accounts for PMDF to the system password file and specify (but not create) the accounts' home directories. Specify `pmdf` as the first username with `/pmdf/queue` as its home directory, and specify `pmdfuser` as the second username, also with `/pmdf/queue` as its home directory. Be sure that the user ids and group ids for the `pmdf` and `pmdfuser` accounts are distinct from each other and from those of any other accounts on your system.

Installing PMDF and PMDF layered products

Preliminary Tasks for New Installations

To add these accounts, you may use the `groupadd` and `useradd` utilities, making sure to specify but not create the home directories, as described in Section 1.2.1.1 below, or you may use the `/usr/sbin/vipw` utility to manually edit the system password file, `/etc/passwd`, and add the accounts, and then edit the system shadow file, `/etc/shadow`, similarly, as described in Section 1.2.1.2 below. Or you may use any other utility provided by your Linux distribution to create accounts.

Note: Make sure to specify that the home directory of the `pmdf` and `pmdfuser` accounts (`/pmdf/queue`) should not be created.

1.2.1.1 Using GROUPADD and USERADD to Add the Accounts

This section describes how to use the `groupadd` and `useradd` utilities to add the required `pmdf` and `pmdfuser` accounts.

Issue the commands

```
# groupadd pmdf
# useradd -c "PMDF" -d /pmdf/queue -M -s /bin/sh -f 0 -e "" -g pmdf pmdf
# groupadd pmdfuser
# useradd -c "PMDF user" -d /pmdf/queue -M -s /bin/sh -f 0 -e "" -g pmdfuser pmdfuser
```

Then use the `passwd` command to set real passwords for the two new accounts.

1.2.1.2 Editing the /etc/passwd and /etc/shadow Files to Add the Accounts

This section describes how to use the `/usr/sbin/vipw` utility to manually edit the system password file, and add the required `pmdf` and `pmdfuser` accounts. Specify `/pmdf/queue` as the home directory for both accounts. Be sure that the user ids and group ids of the `pmdf` and `pmdfuser` accounts are distinct from each other and from those of any other accounts on your system.

Invoke `vipw` to manually edit the system password file. Upon saving the system password file, you will be prompted to also update the system shadow file, `/etc/shadow`, with entries for these accounts. (Note that in order to make system administration more manageable, it is usually recommended that shadow entries be added in exactly the same order as password entries.) Create entries for the `pmdf` and `pmdfuser` accounts in the system shadow file having arbitrary random strings in place of real passwords, save the system shadow file, and then use the `passwd` command to set real passwords for the two new accounts.

For example, if your system has no accounts with user id or group id 30 or 31, then an example of appropriate entries to add to `/etc/passwd` is:

```
pmdf:x:30:30:PMDF:/pmdf/queue:/bin/sh
pmdfuser:x:31:31:PMDF user:/pmdf/queue:/bin/sh
```

An example of appropriate initial entries for the system shadow file is:

```
pmdf:xxxxxxxxxxxxxxxx:::
pmdfuser:yyyyyyyyyyyyyy:::

```

Then use the `passwd` command to set real passwords for the two new accounts.

Installing PMDF and PMDF layered products

Preliminary Tasks for New Installations

1.3 Preliminary Tasks for Upgrade Installations

1.3.1 Prepare to Convert Databases

As of PMDF V6.5, the format of PMDF databases has changed from Berkeley DB (SleepyCat) to PBL. If you are upgrading from V6.4 or earlier, you must either convert or rebuild all of your databases. Before the upgrade, there are several steps you must take to prepare for the database format change.

If you do not have sources for databases that you wish to use `pmdf crdb` to rebuild after the upgrade, you must run `pmdf dumpdb` on those databases before the upgrade to generate the corresponding sources.

Databases created by `pmdf db`, such as personal alias databases, can best be handled by before the upgrade using the `pmdf db write` command to create a source file, and then after the upgrade using the `pmdf db run` command on that source file to create the database in the current format.

1.3.2 Save Tailor File

If you have made any changes to your PMDF tailor file (`/etc/pmdf_tailor`), you **must** save this file before you upgrade because it will be overwritten by the installation.

After upgrading, you should check the new `pmdf_tailor` file and merge in any changes that you made to your version of the file.

1.4 Step-by-Step Installation Instructions

1. If you have previously installed PMDF, you must shutdown the PMDF detached processes before attempting to reinstall or upgrade PMDF. Issue the command:

```
# pmdf shutdown
```

2. If you have previously installed PMDF, you must first deinstall PMDF before attempting to reinstall or upgrade PMDF. To deinstall PMDF, see Section 1.7.
3. Installation of PMDF should be done by `root`. If you are not logged in as `root`, do so now.

Installing PMDF and PMDF layered products

Step-by-Step Installation Instructions

4. If you are upgrading PMDF, you should check on your PMDF licenses and update them, if necessary, at this time. (If this is your initial PMDF installation, instructions on initially installing PMDF licenses are given in Section 1.6, Post-Installation Tasks for New Sites.) PMDF license information is stored in files with names of the form *product-name.license*, located in the PMDF table directory. You will have a separate license file for each PMDF product you have licensed for the system in question. For instance, a PMDF-MTA license would be stored in a file `/pmdf/table/PMDF-MTA-LINUX.license` and look something like:

```
Issuer:Process
Authorization Number:auth-number
Product Name:PMDF-MTA-LINUX
Producer:Innosoft
Product Release Date:February 2020
Product Token:token
Checksum:checksum
```

where *auth-number*, *token*, and *checksum* are specific to your own site's license. You should have received the correct license information for your system when you licensed PMDF, and new licenses for PMDF at renewal time. A PMDF-MTA system will need a PMDF-MTA-LINUX license.

If you will also be installing any add-on layered product such as PMDF-MSGSTORE, then for each such layered product, an additional license will be required, named, *e.g.*, PMDF-MSGSTORE-LINUX; note that such layered products can only be licensed and installed on a system already licensed for PMDF-MTA.

If you already have existing licenses, you should check to make sure that they are valid for this release. Check that the release date for each product, *i.e.*, that found on the fifth line of the file, is later than the release date of the new version of each PMDF product that you want to install.¹

New PMDF product licenses are issued when your maintenance contract is renewed, not when new versions of software are released. If you have received new PMDF licenses at your renewal time, you should register the new licenses. Edit the appropriate license file and enter the new license information.

Note that the `pmdf license -verify` utility may be used to check the validity of the syntax, data, and checksum of PMDF license files.

The following discussion outlines the steps in the PMDF installation procedure. Refer to Chapter 2 for a sample installation dialogue.

5. Begin the installation procedure by invoking the RPM utility as shown below:

```
# cd /
# rpm -i rpm-kit
```

where *rpm-kit* specifies the appropriate PMDF package. If you are installing the PMDF kit directly from CD-ROM, then you need to mount the distribution media first and then invoke the RPM command. For instance:

¹ PMDF licenses do not use a termination date; they instead use a release date. The release date merely prevents you from running newer versions of PMDF released after your maintenance contract has expired. The licenses do not prevent your current version of PMDF from running after your maintenance contract has expired. This is intentional.

Installing PMDF and PMDF layered products

Step-by-Step Installation Instructions

```
# cd /
# mount -o ro /dev/cdrom /cdrom
# rpm -i /cdrom/Linux-X86_64/PMDF680/pmdf-6.8.0-0.x86_64.rpm
```

There will be no questions asked during the installation. If the installation is completed successfully, it will print out nothing, and just return you to your shell prompt.

Note that in some cases you may have to specify the `--nodeps` option on the `rpm -i` command, for example, if you have just installed RPM on your Linux system for the purpose of installing PMDF, and you have no other RPM packages installed.

6. By default, PMDF is installed under `/opt` and `/pmdf` is created as a link to the `/opt/pmdf` directory. If you wish to install PMDF into a different location, you must specify that on the `rpm -i` command by using the `--prefix` option. For example, to install PMDF directly into the `/pmdf` directory, use the following command:

```
# rpm -i --prefix / pmdf-6.8.0-0.x86_64.rpm
```

7. After the kit is installed, if you have been installing directly from the CD-ROM, you should unmount the distribution media. The exact command needed depends on which Linux distribution you have. For example, on Red Hat Enterprise Linux, use a command such as:

```
# umount /cdrom
```

1.5 Post-Installation Tasks for Upgrades

1. Run the script `/pmdf/bin/upgrade_all_dbs.sh`.

This script performs the following actions (which can also be performed by hand if desired):

- a. If you are using a compiled configuration, it is recompiled with the command:

```
# pmdf cnbuild
```

- b. If necessary, the MessageStore user database is rebuilt with the command:

```
# pmdf msgstore x-build-user-db
```

- c. If you are upgrading from PMDF V6.4 or earlier, all other databases in the `/pmdf` tree are found and converted to the format used in V6.5 and later using the command:

```
# pmdf convertdb <old-database> <new-database>
```

Note that the defragment database `/pmdf/table/defragment_cache.*` is excluded from this process. It does not need to be converted as the defragment

Installing PMDF and PMDF layered products

Post-Installation Tasks for Upgrades

channel will rebuild the database if necessary from the messages in the `/pmdf/queue/defragment` directory the first time it runs.

Also note that databases outside the `/pmdf` tree, such as personal alias databases in users' home directories, are not found and converted by `upgrade_all_dbs.sh`.

- d. The Berkeley DB (SleepyCat) environment files are no longer used, so they are deleted if necessary, using the commands:

```
# rm /pmdf/tmp/__db.0*
# rm /pmdf/table/__db.0*
# rm /pmdf/table/queue_cache/__db.0*
```

2. If necessary, rebuild or convert all remaining databases.

If you are upgrading from PMDF V6.4 or earlier, all databases must be rebuilt or converted in order for PMDF V6.5 or later to be able to read them. PMDF V6.5 and later cannot read any databases in V6.4 or earlier formats.

Note that PMDF V6.5 and later uses PBL as its database software. PMDF's PBL databases consist of three files: `database.pbl` which contains the data, `database.idx` which contains the index, and `database.lck` which is used for locking the database.

- a. All databases for which you have sources (including those sources you created before the upgrade using the `pmdf dumpdb` command) can be rebuilt using the `pmdf crdb` command.
- b. All databases created by `pmdf db` should be rebuilt. This includes the personal alias databases located in users' home directories (which are not converted by `upgrade_all_dbs.sh`). Before doing the upgrade, you should have generated source files for these databases by using the `pmdf db write` command. At this time, you should rebuild these databases from those source files using the `pmdf db run` command. If you do not have a source file, the database can be recreated by using the `pmdf db` utility and adding each entry back in by hand.

If you cannot rebuild these databases, they can be converted using the `pmdf convertdb` command if necessary.

- c. Databases created by utilities such as `pmdf profile` or `pmdf password`, and the databases created by MessageStore/popstore such as the forward database and the group names database must either be converted using `pmdf convertdb` or recreated by running the corresponding utility and adding each entry back in by hand.
3. Check the contents of the PMDF tailor file `/etc/pmdf_tailor` that was supplied by this installation. Merge in any changes that you made to the file, using the copy that you saved before you started the upgrade.
4. Start up the PMDF Job Controller and PMDF Service Dispatcher using the command:

```
# pmdf startup
```

PMDF supports the `systemctl` method used in modern versions of Linux. To enable PMDF to be started at system boottime, issue the following commands:

Installing PMDF and PMDF layered products

Post-Installation Tasks for Upgrades

```
# systemctl enable pmdf
# systemctl start pmdf
```

1.6 Post-Installation Tasks for New Sites

The following is a list of tasks which must be completed following a new installation of PMDF.

1. For an initial PMDF installation, load the appropriate PMDF license by entering your license information into the appropriate PMDF license file. PMDF license information is stored in files with names of the form *product-name.license*, located in the PMDF table directory. You will have a separate license file for each PMDF product you have licensed for the system in question. For instance, a PMDF-MTA license would be stored in a file named `/pmdf/table/PMDF-MTA-LINUX.license`.

You should have received the correct license information for your system when you licensed PMDF. A PMDF-MTA system will need a PMDF-MTA-LINUX license.

If you will also be installing any add-on layered product such as PMDF-TLS, then for each such layered product, an additional license will be required, named, *e.g.*, PMDF-TLS-LINUX; note that such layered products can only be licensed and installed on a system already licensed for PMDF-MTA.

A PMDF license file has the format:

```
Issuer:Process
Authorization Number:auth-number
Product Name:product-name
Producer:Innosoft
Product Release Date:release-date
Product Token:token
Checksum:checksum
```

where *auth-number*, *token*, *release-date*, and *checksum* are specific to your PMDF license, and where *product-name* is a product name such as PMDF-MTA-LINUX, PMDF-MSGSTORE-LINUX, or PMDF-TLS-LINUX.

Check that the release date for each product, *i.e.*, the value on the fifth line of the file, is later than the release date of the current version of each PMDF product you have installed. PMDF licenses allow operation of PMDF software released before the license release date. New PMDF product licenses are issued when your maintenance contract is renewed, not when new versions of software are released.

2. PMDF documentation assumes that your UNIX shell process includes `/usr/bin` in the shell's search path, thereby making the `pmdf` command available in the form documented. If this is not the case, then you may either add `/usr/bin` to your shell's search path, or use the fully qualified command name, `/usr/bin/pmdf`.

Installing PMDF and PMDF layered products

Post-Installation Tasks for New Sites

3. Create PMDF's site specific configuration files using the automatic configuration generation utility; see Chapter 3. *e.g.*, for a PMDF-MTA system, issue the command:

```
# /pmdf/bin/http_server -s
```

and then point your web browser, with JavaScript enabled, to:

```
http://localhost:7633/
```

Refer to Chapters 3 and 5 (PMDF-MTA regular configuration), Chapters 6 and 7 (PMDF-MTA firewall configuration), for information, step-by-step procedures, and an example configuration.

4. Once you have generated an initial configuration, you should take whatever additional steps may be required to complete the configuration of PMDF. The automatic configuration generator produces a check list which details any additional steps required to complete the configuration of PMDF. Make sure to look over this checklist file.
5. PMDF includes two shell scripts called `post.sh` and `return.sh` in the `/pmdf/bin` directory. You need to use `cron` to schedule two periodic jobs to run these shell scripts. It is recommended that the shell script `post.sh` be scheduled to run every four hours and that the shell script `return.sh` be scheduled to run at 30 minutes after midnight each day; however, you may want to schedule them differently according to the needs of your site. It is also suggested, particularly if your site includes multiple PMDF nodes, that you consider setting the minutes-after-the-hour offset at which the `post.sh` shell script runs to different values on different nodes to better balance mail flow.

Typical scheduling for such `cron` jobs can be established by issuing the commands:

```
# su pmdf
$ crontab /pmdf/table/cronjobs
$ exit
```

Note: If you want to set up site-specific `cron` entries manually, perform the following steps:

Become the `pmdf` user:

```
# su pmdf
```

Edit the `crontab` entries by using the following command:

```
$ crontab -e
```

Use the editor to add entries similar to the following:

```
30 0 * * * /pmdf/bin/return.sh >/pmdf/log/return.log-`/pmdf/bin/unique_id` 2>&1
0 0,4,8,12,16,20 * * * /pmdf/bin/post.sh >/pmdf/log/post.log-`/pmdf/bin/unique_id` 2>&1
```

The first value in the second line, shown as 0 in the above example, is the minutes-after-the-hour offset. If you have multiple PMDF nodes, then this is a value that you might want to stagger between different nodes. For example, 0 on one node, 10 on a second node, 20 on a third node, *etc.* Also note the use of log files in the above. These log files can be useful in tracking down problems with the operation of `return.sh` and `post.sh`.

Make sure to exit from the `pmdf` user shell when you have finished adding these entries. For example,

Installing PMDF and PMDF layered products

Post-Installation Tasks for New Sites

```
$ exit
```

6. Replace the `sendmail` system startup script with PMDF's `pmdf` startup script. This may be performed by issuing the command:

```
# /pmdf/bin/symlink install
```

Note that the effect of the `/pmdf/bin/symlink` may be undone by issuing the command:

```
# /pmdf/bin/symlink backout
```

Note: If you need to set up the `pmdf` startup script by hand, perform the following steps:

```
# systemctl stop sendmail
# systemctl disable sendmail
# systemctl enable pmdf
# systemctl start pmdf
```

7. When installing PMDF for the first time, or after an upgrade of the operating system if that upgrade installed a new version of `sendmail`, you must replace `sendmail` with PMDF's `sendmail`.

Note that the `symlink` script that you executed in the previous step will have already performed this operation. But in case you need to do it by hand, for example after an upgrade of the operating system, the steps are as follows.

First save the original `sendmail` by renaming it to `sendmail.org`, and then create a symbolic link that links `sendmail` to `/pmdf/bin/sendmail` as follows:

```
# mv /usr/lib/sendmail /usr/lib/sendmail.org
# ln -s /pmdf/bin/sendmail /usr/lib/sendmail
```

You should also kill any old, pre-PMDF `sendmail` processes which might exist and be accepting connections. This may also be necessary if an operating system upgrade starts up non-PMDF `sendmail` processes. (Note that killing such processes is not necessary after an upgrade of PMDF. Even after the first installation of PMDF or after an upgrade of the operating system, there will be no non-PMDF `sendmail` processes if the system has been rebooted and the previous post-installation tasks have been performed.)

To see if there are any such `sendmail` processes, issue the command:

```
# ps -ef | grep sendmail
```

If there are any such `sendmail` processes, you will see something similar to the following:

```
root 23913      1  0   Apr 05 ?           0:01 /usr/lib/sendmail -bd -qlh
```

You should kill any such processes using the `kill` command; e.g.,

```
# kill 23913
```

Installing PMDF and PMDF layered products

Post-Installation Tasks for New Sites

8. The multithreaded POP3 and IMAP servers are handled by the PMDF Service Dispatcher. If you were previously using non-PMDF servers then you must shut down your old servers before you can use the PMDF multithreaded servers. Before you can use the multithreaded POP3 or IMAP servers, you must also configure the Dispatcher to run the desired service. Dispatcher configuration is normally performed as part of the initial web-based PMDF-MTA configuration; see Chapters 3 and 5 for instructions and sample configurations of the Dispatcher. See Chapter 4 for instructions and Chapter 3 for an example of configuring the POP3 and IMAP servers.

Note: If you are using the PMDF legacy POP or IMAP servers to Berkeley BSD mailboxes, you must make sure the protection on the `/var/spool/mail` directory is set to `world=rwt`, for example, by using:

```
# chmod 1777 /var/spool/mail
```

9. Many Linux distributions are initially configured for security purposes with all ports blocked, except for a select few. In order to use PMDF for services such as SMTP, POP, or IMAP, Linux must be configured to open the related ports. How such configuration is done varies from one Linux distribution to the next. If you do not open the ports, PMDF will still start up, but will not be able to receive connections for those services. You must configure your Linux system to be able to accept connections on the ports for any PMDF services that you wish to use.

10. Start up the PMDF Job Controller and PMDF Service Dispatcher using the command:

```
# pmdf startup
```

11. If you chose to install the PMDF on-line documentation, then the installation will have placed the HTML versions of the PMDF documentation under the `/pmdf/doc` directory. PMDF provides an HTTP server for serving out this documentation to Web browsers. To start up the PMDF HTTP server, the PMDF Service Dispatcher must be configured to handle the HTTP service, access to the HTTP server must be enabled, and then the Dispatcher must be started up (or restarted, if it was already running). The web-based PMDF-MTA configuration utility, discussed in Chapter 3 and Chapter 5, will automatically configure the PMDF Dispatcher.

12. The PMDF installation installs man pages. You should add the PMDF section numbers to the `/etc/man.config` file. That file will look something like:

```
#
# Default manual sections (and order) to search if -S is not specified
# and the MANSECT environment variable is not set (1x-8x sections are used by
# xorg packages).
#
MANSECT 1:1p:8:2:3:3p:4:5:6:7:9:0p:n:1:p:o:1x:2x:3x:4x:5x:6x:7x:8x
```

You should add `1pmdf`, `8pmdf` to the list of MANSECT, so that the file is along the lines of:

```
MANSECT 1:1p:8:2:3:3p:4:5:6:7:9:0p:n:1:p:o:1x:2x:3x:4x:5x:6x:7x:8x:1pmdf:8pmdf
```

This will enable users to use commands such as `man pmdf_convertddb` instead of having to specify a section as `man 8pmdf pmdf_convertddb`.

Installing PMDF and PMDF layered products

Post-Installation Tasks for New Sites

1.7 Deinstalling PMDF

Deinstallation of PMDF deletes only those files present in the distribution kit. In particular, deinstallation will not remove files such as the PMDF configuration file, `/pmdf/table/pmdf.cnf`, and other such site-generated files, and thus you will not need to reconfigure PMDF after deinstalling and reinstalling or upgrading.

1.7.1 Step-by-Step Deinstallation Instructions

1. Deinstallation should be done by `root`. If you are not already logged in as `root`, do so now. ².

2. Move to the root directory:

```
# cd /
```

3. Check what PMDF package you currently have installed; *e.g.*,

```
# rpm -qa | grep pmdf
pmdf-6.8.0-0.x86_64
```

4. Use the `rpm -e` command to deinstall any PMDF package you have installed, *e.g.*:

```
# rpm -e pmdf-6.8.0-0.x86_64
```

1.7.2 Problems Deinstalling

Sometimes there can be problems deinstalling PMDF, and error messages similar to the following may be displayed:

```
# rpm -e pmdf-6.8.0-0.x86_64
error: %preun(pmdf-6.8.0-0.x86_64) scriptlet failed, exit status 1
```

This can occur if you have modified the PMDF installation, such as for Linux clusters. The `%preun` section (pre-uninstallation scriptlet) can get an error if the PMDF files, directories, and links are not set up the way that the PMDF installation created them.

To get around these problems and successfully deinstall PMDF, you can specify the `--nopreun` option on the `rpm -e` command. If you are installing a new PMDF kit after deinstalling, you may have to use the `--force` option, since the pre-uninstall tasks were never performed during the deinstall. For example:

```
# rpm -e --nopreun pmdf-6.8.0-0.x86_64
# rpm -i --force pmdf-6.8.0-0.x86_64.rpm
```

² If you are deinstalling PMDF so that you can upgrade to a later version, then the steps listed above are all that you need to do. However, if you are deinstalling PMDF permanently, and you want to restore native `sendmail` links, see the description of `/pmdf/bin/symlink` backout in Section 1.6. You also might want to remove the PMDF cron jobs.

1.8 After Upgrading the Linux Operating System

After upgrading the Linux operating system, you should perform steps 6, 7, and 9 of the post-installation tasks as described in Section 1.6; *i.e.*, remove `sendmail` files and create PMDF symbolic links in their place, replace `sendmail` with `/pmdf/bin/sendmail` and kill off any non-PMDF `sendmail` processes, and start the PMDF Job Controller and PMDF Service Dispatcher.

2 PMDF Example Installation

Example 2-1 shows a PMDF installation dialogue on a Linux system using the `rpm` utility. In this example, the PMDF V6.8 distribution CD-ROM has been mounted and attached to the file tree at the location `/cdrom`, and the PMDF product kit is then being installed straight from the CD-ROM, *i.e.*, from `/cdrom/Linux-X86/PMDF680`.

Example 2-1 Example Installation

```
$ su - root
Password:
# cd /
# rpm -i /cdrom/Linux-X86/PMDF680/pmdf-6.8.0-0.x86_64.rpm
#
```

3 Generating an Initial PMDF Configuration

This chapter describes how to use the PMDF automatic configuration generator to create an initial configuration for your system. In most cases the configuration created by following these steps will suffice without further modification. Additional customization will require manual editing of the configuration file.

Manual editing of the configuration file may also be required as your environment evolves. For example, as networks or gateways are added you may need to add rewrite rules or channel blocks to your `pmdf.cnf` file. In many cases you may find it easier to rerun the configuration generator supplying new answers reflecting the changes in your environment.

3.1 Before You Begin

Prior to running the automatic configuration generator, you should have a good idea of your network configuration and of what input needs to be supplied to the PMDF configuration generator. Note that the PMDF configuration generator will attempt to provide default values to its prompts. These defaults are picked up, whenever possible, from your system environment.

3.1.1 Selecting a System Name

You should give some thought as to what your official local host name should be prior to configuring PMDF. This is not just a matter of picking a name for your system; if you want to communicate with systems on the Internet your system will have to be registered as a member of some network domain. In order to be eligible for registration you must have a connection to a system on the Internet which is able to perform name server functions for you.

If you are using PMDF in an isolated (non-Internet) application you may pick any system name that you want. However, you should remember that networks have a way of growing and at some point in the future you may regret a careless decision about naming conventions you made earlier. Try to pick a sane, sensible name which is appropriate to your users, system, and site.

If you've already chosen a TCP/IP hostname, you might use that as your official local host name. Alternately, you could use a more generic e-mail hub name for your official local host name. Should you choose to do that, the PMDF configuration generator will also need to know your TCP/IP hostname. It will prompt for that, with a default answer, when asking about your TCP/IP network.

Generating an Initial PMDF Configuration Before You Begin

3.1.2 Authentication and Security

There are various contexts in which users may need to authenticate themselves (*i.e.*, supply a password): connecting to read their e-mail via a POP or IMAP client, setting up a personal mailbox filter, sending e-mail using SASL. PMDF supports performing such authentication against various authentication sources, such as `/etc/passwd`, the PMDF password database, PMDF user profiles (PMDF MessageStore or PMDF popstore account profiles), or even an LDAP directory. The PMDF default, allowing authentication against any of a PMDF user profile, the PMDF password database, or system login passwords, is usually a good starting point for most sites. See the *PMDF System Manager's Guide* for further information on PMDF authentication and security configuration.

3.2 Using the Web-based PMDF-MTA Configuration Utility

This section describes using the web-based PMDF-MTA configuration utility. This web-based utility subsumes the command line utilities `pmdf configure mta`, `pmdf configure dispatcher`, and `pmdf configure mailbox_servers`. It is generally recommended to use the web-based configuration utility to generate a PMDF-MTA configuration, but the command line utilities may be a useful alternative for sites for whom web configuration is inconvenient.

If this is a new installation, be sure to follow the preliminary tasks for new installations described in Section 1.2. In particular, a PMDF-MTA license must be installed, and the `pmdf` account must be created, prior to running the configuration utility.

The web-based configuration utility may be used to generate an initial configuration, or may be used to generate a new configuration of an existing PMDF installation. If you will be configuring multiple components, *e.g.*, MTA/SMTP and IMAP/POP servers, these components may either be configured at the same time or may be configured at separate times. Configuring components at the same time allows the configuration utility to mesh some of the configuration files itself, minimizing the number of post-configuration checklist tasks you will need to perform; in particular, configuring IMAP/POP server use at the same time as the base MTA/SMTP configuration is often convenient.

If this is a new installation where PMDF is not already running, then the web-based configuration utility may be accessed as follows. Log in either as `root` or as the `pmdf` user. Then issue the command:

```
% /pmdf/bin/http_server -s
```

The above command starts the PMDF HTTP server up in standalone mode, to make the web-based configuration utility available. (Sites with PMDF already running do not need to issue the above command when they want to re-run the configuration utility, as the PMDF HTTP server will already be running normally for them.)

Then, using Netscape (version 3.0 or later) or Microsoft Internet Explorer (version 4.0 or later), with JavaScript enabled, connect to

Generating an Initial PMDF Configuration Using the Web-based PMDF-MTA Configuration Utility

`http://localhost:7633/`

where *localhost* is the TCP/IP name of your PMDF system, and then select the “Configuration Utilities” link.

Each screen in the configuration utility will have radio buttons, checkboxes and/or text input fields. If you click on any of these fields, instructions for the field will appear in the “Help” box at the bottom of the page. Note that use of a full-screen web-browser window on a display at least 800 x 600 will avoid unnecessary vertical scrolling.

Once you have made your selections and returned to the main configuration screen, select the “Generate” button, and on the next page the “Confirm” button to generate your configuration. Finally, a checklist of post-install items will be displayed.

3.3 Using the Command Line Configuration Procedure

This section presents a step-by-step procedure for generating your PMDF configuration files using the command line PMDF automatic configuration utility.

1. Configuration of PMDF should be done by `root` to ensure that the necessary privileges are available to create the configuration files. If you are not logged in as `root`, do so now.
2. Begin the configuration procedure by invoking the PMDF configuration utility as follows, assuming that you have `/usr/bin` in your search path:

```
# cd /pmdf/table
# pmdf configure mta
```

3. The configuration procedure will optionally print out detailed explanations of each prompt as it proceeds. Unless you are familiar with the procedure, you should enable the detailed output.
4. The answers to all the prompts are logged to a file in the `/pmdf/table` directory. After the first configuration, `pmdf configure` can use the answers to the previous run as the default answers. The utility will ask:

```
Do you want to use answers from the previous run as defaults?
```

Answer `YES` if you want to have your previous answers presented as default answers. You may use the backslash character, `\`, to clear a default answer.

5. If this is the first time that PMDF has been configured on this system, the configuration utility will ask if you would also like to configure the PMDF Dispatcher. (The PMDF Service Dispatcher is a resident process that listens for incoming TCP/IP connections on various ports and matches those incoming connection requests to various servers, *e.g.*, the multithreaded SMTP server, a POP3 server, an IMAP server, an HTTP server, *etc.* See *PMDF System Manager’s Guide* for a more detailed discussion of the purpose and function of the PMDF Service Dispatcher.)

You may either answer `YES` and perform the Dispatcher configuration then and there, or else answer `NO` and then configure the Dispatcher as a separate step subsequently, by issuing the command

Generating an Initial PMDF Configuration Using the Command Line Configuration Procedure

```
# pmdf configure dispatcher
```

6. If this is the first time that the Dispatcher has been configured, the utility will ask if you would also like to configure PMDF POP and IMAP mailbox servers.

You may either answer YES and perform the Mailbox Servers configuration then and there, or else answer NO and then configure the Mailbox Servers as a separate step subsequently, by issuing the command

```
# pmdf configure mailbox_servers
```

7. Once you have completed running `pmdf configure`, type out or print out the checklist file, `/pmdf/table/pmdf.checklist` for an MTA configuration, and complete the configuration by following the steps outlined in the checklist.

4 Configuring PMDF POP and IMAP Mailbox Servers

The PMDF POP and IMAP servers are multithreaded and run under the control of the PMDF Dispatcher. The PMDF legacy mailbox POP server can serve out native BSD mailboxes or PMDF popstore mailboxes; the PMDF legacy mailbox IMAP server can serve out native BSD mailboxes. The PMDF MessageStore mailbox POP server can serve out PMDF MessageStore mailboxes and PMDF popstore mailboxes; the PMDF MessageStore IMAP server can serve out PMDF MessageStore mailboxes. The PMDF mailbox servers configuration utility allows choosing one or the other POP server and one or the other IMAP server. (PMDF supports running both POP servers, one of which must then be running on a non-standard port, and running both IMAP servers, one of which must then be running on a non-standard port, but such configurations are not generated by the configuration utility.)

The POP and IMAP servers may run on a PMDF-MTA system.

This chapter describes how to use the PMDF Mailbox Servers configuration utility. This utility generates definitions for POP and IMAP servers to insert into the PMDF Dispatcher configuration, as well as basic PMDF POP and PMDF IMAP server configuration files. It also provides a checklist of the steps you need to take to complete the configuration of the PMDF POP and IMAP servers.

4.1 Before You Begin

Prior to running the PMDF Mailbox Servers configuration utility you must have installed PMDF-MTA on your system, and it is recommended that you also configure PMDF itself (and the PMDF Service Dispatcher, normally done automatically as part of the PMDF configuration) before configuring the PMDF POP and IMAP mailbox servers. Refer to Chapter 1 if you have not already installed and configured PMDF-MTA.

If you were previously using non-PMDF servers, then you will need to shut down and disable such servers before you can use PMDF's multithreaded servers. (Before configuring PMDF's servers is a convenient time to do this, although if you prefer you can wait until after you have configured PMDF's servers but before you try to start PMDF's servers.)

The PMDF POP and IMAP mailbox servers configuration utility will prompt for several pieces of information. In particular, it will ask which POP and/or IMAP servers you want to run, and how many simultaneous POP connections and how many simultaneous IMAP connections you want to allow at your site, to which you will need to provide site-appropriate answers. For further questions, the configuration utility attempts to provide reasonable default values. You may want to mostly take the default answers the first time you configure, and then later after observing the actual POP and IMAP usage at your site, reconfigure with answers geared for your site. Configuration questions will include the following:

Configuring PMDF POP and IMAP Mailbox Servers Before You Begin

- Whether you want to run the legacy mailbox POP server, or the MessageStore mailbox POP server, (or neither).
- Whether you want to run the legacy mailbox IMAP server, or the MessageStore mailbox IMAP server, (or neither).
- Whether you want to log POP and IMAP connections.
- Whether you want to run a POPPASSD server to support changing passwords from POP clients using the ad-hoc password changing mechanism used by, for instance, Eudora. Note that the POPPASSD protocol involves sending both the old and the new password “in the clear”, a point to be considered carefully when deciding whether or not to provide this service.
- Whether you want to enable PMDF’s password changing web CGI.
- If you select use of the MessageStore IMAP server or MessageStore POP server, the utility will also configure the PMDF MessageStore and PMDF popstore for you and will therefore present several configuration questions regarding the MessageStore and popstore. These questions will include the following.
 1. What is the pseudo domain name assigned to the MessageStore. This is the domain name which will be used to address mail to PMDF MessageStore users. For instance, if you want MessageStore users to have addresses of the form user@msgstore.naples.example.com, you would use the domain name msgstore.naples.example.com for the MessageStore.
 2. The local postmaster address.
 3. The default primary message storage quota to allow each user. The default account is granted this quota. When you create user accounts, they will be given this primary quota unless you specify a different quota. A primary quota value of 0 grants unlimited storage quota.
 4. The default overdraft message storage quota to allow each user. This is the amount by which users are allowed to exceed their primary quota.¹ The default account is granted this overdraft quota which is then used as a default setting for user accounts you create.
 5. How many days to retain PMDF popstore messages, awaiting user download. If a user has not deleted a message after this limit, it is either deleted silently or returned to its originator as unread. To retain messages indefinitely, specify an age limit of 0.
 6. A special account name for posting to public folders in the MessageStore.
- If you chose to run a POP server, there are a few POP server configuration questions, including:
 1. What is the maximum number of simultaneous POP connections you want to support on your system. Note that this is not the total number of users or even total number of POP users; rather, it is the maximum number of POP users whose POP clients will be connecting simultaneously. Also note that POP connections are typically brief: the POP client connects, downloads messages, and disconnects. Choose a number that will provide reasonable access for your users without overburdening your system resources.

¹ The utility of an overdraft quota is explained in the *PMDF popstore & MessageStore Manager’s Guide*.

Configuring PMDF POP and IMAP Mailbox Servers

Before You Begin

2. What is the maximum number of connections you want to allow per server process. To support a given number of simultaneous connections, there is a tradeoff between the number of processes used and the number of connections handled per process. Fewer connections per process tends to result in greater responsiveness for the individual connections, but the resulting need for more processes incurs greater system overhead. A moderate number of connections per process is usually best.
 3. Whether you want the server to support the POP3 UIDL command. The UIDL command permits POP clients to keep track of messages by an identifier. POP users who enable “leave mail on server” behavior typically appreciate having UIDL supported, as it can allow their client to keep track of which of the messages in their inbox they have actually already read. Sites that want to discourage “leave mail on server” behavior may want to disable UIDL support.
- If you chose to run an IMAP server, there are a few IMAP server questions, including:
 1. What is the maximum number of simultaneous IMAP connections you want to support on your system. Note that this is not the total number of users or even total number of IMAP users; rather, it is the maximum number of simultaneous IMAP connections. Some IMAP clients make (and keep open) more than one connection to the server. So the number of simultaneous IMAP connections may be higher than the number of simultaneous IMAP users. Unlike POP connections, IMAP connections tend to be long lasting: the IMAP client connects and stays connected as the IMAP user reads and moves messages between folders. Choose a number that will provide reasonable access for your users without overburdening your system resources.
 2. What is the maximum number of connections you want to allow per server process. To support a given number of simultaneous connections, there is a tradeoff between the number of processes used and the number of connections handled per process. Fewer connections per process tends to result in greater responsiveness for the individual connections, but the resulting need for more processes incurs greater system overhead. A moderate number of connections per process is usually best.

4.2 Using the Web-based POP and IMAP Mailbox Servers Configuration Utility

This section describes using the web-based POP and IMAP mailbox servers configuration utility, which may be used to configure mailbox servers for a PMDF-MTA system. A command line variant, `pmdf configure mailbox_servers`, is also available for sites for whom web configuration is not convenient. The web-based configuration utility may be used to generate an initial mailbox servers configuration, or may be used to generate a new mailbox servers configuration of an existing PMDF installation.

Using Netscape (version 3.0 or later) or Microsoft Internet Explorer (version 4.0 or later), with JavaScript enabled, connect to

```
http://localhost:7633/
```

where *localhost* is the TCP/IP name of your PMDF system—you should see a page such as shown in Figure 5–3—and then select the “Configuration” link; at this point you should see a page such as shown in Figure 5–4.

Configuring PMDF POP and IMAP Mailbox Servers

Using the Web-based POP and IMAP Mailbox Servers Configuration Utility

If your last use of the web-based PMDF configuration utility was to configure PMDF-MTA and your PMDF-MTA configuration has not been manually modified since then, you can “Load” your prior PMDF-MTA configuration session before beginning your mailbox servers configuration; or if you want to redo your PMDF-MTA configuration, you may start by doing so now; either will minimize the number of checklist tasks you will later need to perform. Otherwise, you may configure just the mailbox servers during this configuration sessions (and then perform checklist tasks to integrate your mailbox server configuration into your main PMDF-MTA configuration).

Click on the “Configure” button for IMAP/POP Servers to begin the configuration.

Refer to Chapter 5, specifically to Figures 5–9 through Figure 5–15, for a sample configuration session.

4.3 Using the Command Line POP and IMAP Mailbox Servers Configuration Utility

This section presents a step-by-step procedure for generating a basic PMDF POP and IMAP Mailbox Servers configuration files using the `pmdf configure mailbox_servers` utility. Refer to Chapter 5 for a sample configuration session.

1. Configuration of the PMDF POP and IMAP Mailbox Servers should be done by `root`. If you are not logged in as `root`, do so now.
2. Begin the configuration procedure by invoking the PMDF Mailbox Server configuration utility as follows, assuming that you have `/usr/bin` in your search path:

```
# cd /pmdf/table
# pmdf configure mailbox_servers
```

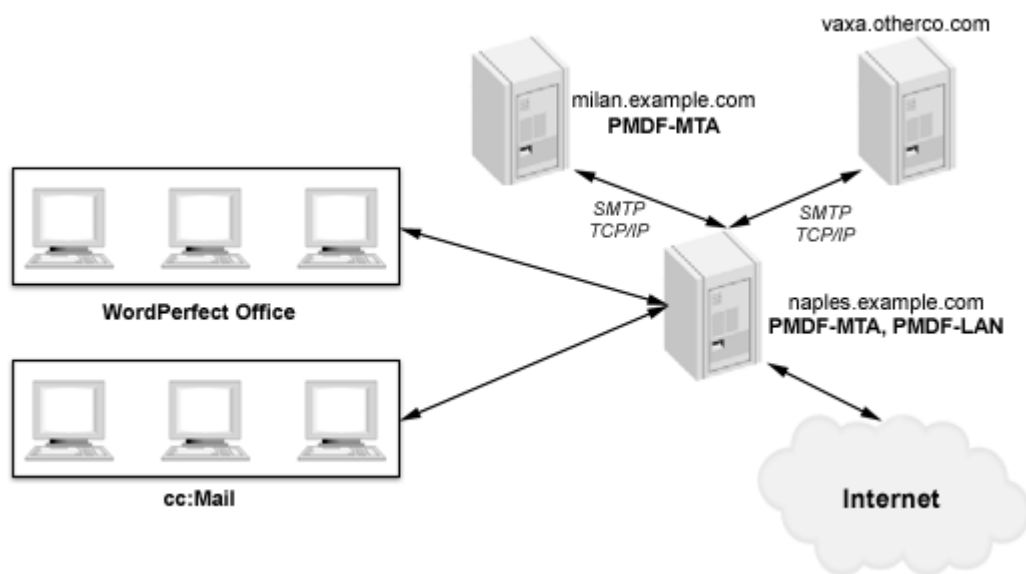
3. The configuration procedure will optionally print out detailed explanations of each prompt as it proceeds. Unless you are familiar with the procedure, you should enable the detailed output.
4. Once you have completed running `pmdf configure mailbox_servers`, type out or print out the checklist file, `/pmdf/table/mailbox_servers.checklist` and complete the configuration by following the steps outlined in the checklist.

5 PMDF-MTA and IMAP Example Configuration

This chapter contains examples of configuring the PMDF MTA and IMAP servers using a sample site as follows.

The sample site EXAMPLE.COM has two Linux nodes, `naples` and `milan`. The node `naples`, which has TCP/IP connections to the Internet and will be acting as a gateway for EXAMPLE.COM's Exchange users, will be a PMDF-MTA node. In addition, EXAMPLE.COM has agreed to act as a gateway for another company in town, OTHERCO.COM, and `naples` will be the node which routes mail for the OTHERCO.COM node `vaxa.otherco.com`. `milan`, which is an internal EXAMPLE.COM node not necessarily registered on the Internet, will be a PMDF-MTA node, routing all of its mail to EXAMPLE.COM's Exchange users and to the Internet, by way of `naples`. PMDF-MTA has been installed on node `naples`.

Figure 5-1 Sample PMDF Site EXAMPLE.COM



Note that the sample configurations shown in this chapter only handle the base PMDF-MTA configuration with IMAP and POP mailbox servers.

Whenever appropriate, both the web-based and the command line configuration utilities attempt to provide reasonable default answers.

PMDF-MTA and IMAP Example Configuration

Remember that the values entered in this sample are for purposes of example only. Be sure to use the values appropriate for your system when you perform the actual configuration.

5.1 Command Line Example Configuration

This section shows sample sessions for the `pmdf configure mta` and `pmdf configure mailbox_servers` utilities.

Note that if you have previously run the command line configuration utilities, you will be asked whether or not your previous answers should be presented as the default answers; in the sample dialogues shown below, the configuration utilities had been run previously, but we did not choose to be reminded of those previous answers. Simply pressing return, `RETURN`, selects the default answer. Entering a backslash, `\`, clears the default answer.

5.1.1 MTA/SMTP Sample Configuration

Example 5-1 Sample `pmdf configure mta` dialogue

```
# pmdf configure mta
```

```
PMDF Configuration File Creation Utility, V6.8
```

```
This utility creates an initial PMDF configuration file
(/pmdf/table/pmdf.cnf), an initial PMDF aliases file
(/pmdf/table/aliases), an initial PMDF security configuration file
(/pmdf/table/security.cnf) and an initial PMDF mappings file
(/pmdf/table/mappings). Normally this is done just after
PMDF has been installed. However, it is possible to run this
procedure at any time.
```

```
For best results the various network products PMDF is going to be
attached to should be installed and operational when this procedure
is run. This is by no means required, but the defaults provided by
this procedure cannot be selected intelligently without having
various software packages available to interrogate.
```

```
Important note: No changes are made to existing PMDF configuration
information until all questions have been answered. This utility
can be aborted at any prompt by entering CTRL/C. The files
output by this utility may optionally be redirected to a different
location so they will have no impact on the existing PMDF
configuration.
```

```
You have a history file from a previous run of the configuration utility.
```

```
Do you want to use answers from the previous run as defaults [N]? RETURN
```

```
Do you wish to continue [Y]? RETURN
```

```
Do you wish to have a detailed explanation printed before each question [N]? y
```

```
Part One: TCP/IP networking.
```

Example 5-1 Cont'd on next page

PMDF-MTA and IMAP Example Configuration

Command Line Example Configuration

Example 5-1 (Cont.) Sample pmdf configure mta dialogue

Is your system set up to:

- (1) Do host lookups with MX records (name server required)
- (2) Do host lookups without MX records

MX (Mail eXchange) records are special entries in the TCP/IP Domain Name Service database that redirect mail destined for systems not directly attached to the TCP/IP network to an intermediate gateway system that is directly attached.

If you are on the Internet, you should answer 1 as mandated by RFC1123 (Internet Host Requirements). Otherwise if your site has special requirements to ignore MX records then answer 2 if you have a name server available. Answer 3 if no name server is available.

Choose one of the above options [1]?

This system has one or more names it is known by on TCP/IP. Enter the most 'official' of these names, preferably a name the system is registered under in the Domain Name System.

Name of this system on TCP/IP [naples]? **naples.example.com**

PMDF needs to know the IP addresses for all the interfaces used by TCP/IP on this system. These addresses are needed so that PMDF can recognize domain literals references to this system. Such recognition is mandated by RFC1123.

Enter each IP address separately in a.b.c.d format, pressing CR between each one. When you've entered them all just enter a CR by itself to end the list.

IP addresses for this system [RETURN if no more]? **192.168.1.1**

IP addresses for this system [RETURN if no more]?

Answer YES if this system is attached to the Internet via TCP/IP. Answer YES even if you have to go through a firewall. Answer NO if this system is not attached to the Internet in this way. Note that a UUCP or any other indirect connection to the Internet is not a real connection; answer NO if this is the only type of connection you have.

Is this system connected to the Internet via TCP/IP [Y]?

PMDF has the ability to automatically convert shortform names appearing on the right hand side of the at sign in an address into fully qualified domain names. These addresses are then routed to TCP/IP automatically. This convenience is especially appropriate when a system is only connected via TCP/IP and not via other networks. For example, if you were to specify a default domain of CLAREMONT.EDU and the address USER@SIGURD was used, where SIGURD has no other special meaning, this address will be rewritten as USER@SIGURD.CLAREMONT.EDU and routed via TCP/IP. Enter nothing if you don't want to have shortform addresses handled in this way.

Default domain to attach to shortform host names [none]? **example.com**

Example 5-1 Cont'd on next page

PMDF-MTA and IMAP Example Configuration

Command Line Example Configuration

Example 5-1 (Cont.) Sample pmdf configure mta dialogue

Answer YES if this system is behind a firewall and needs to route Internet mail to the firewall first. Answer NO if no such firewall exists or if this PMDF system is acting as the firewall.

Does this system need to route mail to a firewall [N]?

PMDF needs to know about internal TCP/IP usage. For instance, this information is used to segregate incoming messages from internal vs. external sources. Your configuration file will automatically contain the rules necessary to reach external Internet domains, so it is not necessary to tell PMDF about external Internet systems.

If your site satisfies any of the following conditions:

- (+) POP or IMAP users,
- (+) other internal TCP/IP systems,
- (+) connect to non-Internet TCP/IP systems,

then you will need to answer YES. If you do answer YES, you will then be asked for the names of these systems or domains so that they can be added to your configuration and mappings files. Answer NO if there is no internal TCP/IP use.

Are there any internal or non-Internet systems reachable via TCP/IP [N]? **y**

TCP/IP networks typically provide access to one or more systems or entire domains. This should only include systems or domains that are accessible via TCP/IP from the PMDF-MTA machine. For example if the PMDF-MTA machine is acting as a firewall to the Internet, the non-Internet systems or domains need to be listed here.

Enter each system or domain specification (e.g. systems names such as 'doofus.company.com' or domains such as '.mycollege.edu') separately, pressing CR between each one. When you've entered them all just enter a CR by itself to end the list.

Internal system or domain reachable via TCP/IP [RETURN if no more]? **example.com**
Internal system or domain reachable via TCP/IP [RETURN if no more]? **vaxa.otherco.com**
Internal system or domain reachable via TCP/IP [RETURN if no more]?

PMDF needs to know the IP address of each internal system or subnet, including those of internal POP or IMAP client systems. For instance, this information is used to distinguish between internal and external systems for doing SMTP relay blocking. Enter each IP address separately in a.b.c.d, or a.b.0.0 or a.b.c.0 format, pressing CR between each one. When you've entered them all just enter a CR by itself to end the list.

IP addresses for your internal systems or network [RETURN if no more]? **192.168.1.0**
IP addresses for your internal systems or network [RETURN if no more]?

Part Two: Determining local host's name(s).

Enter the 'most official' name for this system. This should be the official domain name in most cases. This is the name that will appear in mail addresses on this system, among other things.

Example 5-1 Cont'd on next page

PMDF-MTA and IMAP Example Configuration

Command Line Example Configuration

Example 5–1 (Cont.) Sample pmdf configure mta dialogue

Official local host name [naples.example.com]?

Enter the domain or subdomain your systems are part of, if there is one and it is consistent. For example, if your system's domain name is HMCVAX.CLAREMONT.EDU, and in general all your systems are part of the .CLAREMONT.EDU domain, enter '.CLAREMONT.EDU'. If your system is not part of a domain or if your use of domain name is not consistent, just press CR.

Default domain or subdomain for this system [none]? **.example.com**

Enter any aliases for the local host; these names are rewritten to the official local host name with rewrite rules.

Any other aliases for the local host [RETURN if no more]?

Enter a valid user@host type of address for the local Postmaster. This address will receive notifications of bounced or deferred mail as well as various other types of status and error reports. This address is also the one that will receive user queries about electronic mail.

A user@host style address for the local Postmaster [root@naples.example.com]?
postmaster@naples.example.com

Part Three: Security Configuration.

Enter YES if you would like to check passwords against LDAP source and NO if you do not.

Do you want to check passwords against LDAP [N]?

Enter YES if you would like to check passwords against MessageStore/popstore user profiles, which is the fastest, and NO if you do not.

Do you want to check passwords against MessageStore/popstore user profiles [Y]?

Enter YES if you would like to check passwords against PMDF password database and NO if you do not.

Do you want to check passwords against PMDF password database [Y]?

Enter YES if you would like to check passwords against the operating system one (e.g. /etc/passwd), and NO if you do not.

Do you want to check passwords against operating system [Y]?

Enter YES if you would like to allow unprotected passwords for internal users and NO if you do not.

Do you want to allow unprotected password for internal users [Y]?

Enter YES if you would like to allow unprotected passwords for external users and NO if you do not.

Do you want to allow unprotected password for external users [N]?

Enter YES if you would like to allow external users to submit mail using password and NO if you do not.

Do you want to allow external users to submit mail using password [Y]?

Example 5–1 Cont'd on next page

PMDF-MTA and IMAP Example Configuration

Command Line Example Configuration

Example 5–1 (Cont.) Sample pmdf configure mta dialogue

Enter YES if you would like to support for pre-standard unprotected password submission used by Outlook Express and Netscape 4.0x and NO if you do not.

Do you want to support pre-standard unprotected password submission used by Outlook Express and Netscape 4.0x [N]? **y**

Part Four: Process and write files

Enter the name of the configuration file you wish to have output. The default action is to produce a real configuration file; you may wish to choose another file name if you are not sure you have properly answered all the questions in the preceding dialogue.

Configuration file to output [/pmdf/table/pmdf.cnf]?

Enter the name of the aliases file you wish to have output. This file contains system-wide local address aliases PMDF will recognize; special aliases are required for proper operation of some channels. The default action is to produce a real alias file; you may wish to choose another file name if you are not sure you have properly answered all the questions in the preceding dialogue, or if you wish to preserve an existing aliases file.

Alias file to output [/pmdf/table/aliases]?

Enter the name of the mapping file you wish to have output. The default action is to create a real mapping file; you may wish to choose another file name if you are not sure you have properly answered all the questions in the preceding dialogue.

Mapping file to output [/pmdf/table/mappings]?

Enter the name of the security configuration file you wish to have output. The default action is to create a real security.cnf file; you may wish to choose another file name if you are not sure you have properly answered all the questions in the preceding dialogue.

Security configuration file to output [/pmdf/table/security.cnf]?

This procedure generates a checklist file that contains the list of steps you must perform in order to complete your PMDF configuration. This procedure does **NOT** perform these steps itself; you must do them manually.

PMDF checklist file name [/pmdf/table/pmdf.checklist]?

All configuration questions have been answered.

This question gives you a last chance to change your mind before any files are written. Answer NO if you are not sure you want to generate the configuration you have specified. Answer YES if you do.

Example 5–1 Cont'd on next page

PMDF-MTA and IMAP Example Configuration

Command Line Example Configuration

Example 5–1 (Cont.) Sample pmdf configure mta dialogue

```
Do you wish to generate the configuration files [Y]? 
Generating the PMDF configuration file...

Generating the PMDF mapping file

Generating the PMDF aliases file...

Generating the PMDF security configuration file...

Generating the PMDF checklist...
*****
*
*   To complete your PMDF configuration, carry out the steps
*   detailed in the checklist file ./pmdf.checklist.
*
*****

Enter YES if you want to see the checklist now. You can still type
the file out later if you say NO.

Do you want to see the checklist now [Y]? 
Checklist for completing the setup of your PMDF configuration.
Written by root, Thu Nov 17 16:02:30 EST 2011
This file was created by the PMDF configuration generator V6.8

(1) Be sure to configure the PMDF Dispatcher, using the
    command:

    pmdf configure dispatcher

(2) Make sure to perform the remaining post-installation
    tasks as described in the PMDF Installation Guide &
    Release Notes.
```

5.1.2 IMAP/POP Server Sample Configuration

Example 5–2 Sample pmdf configure mailbox_servers dialogue

```
# pmdf configure mailbox_servers
PMDF mailbox servers configuration utility, V6.8
  You have a history file from a previous run of the configuration utility.
```

Example 5–2 Cont'd on next page

PMDF-MTA and IMAP Example Configuration

Command Line Example Configuration

Example 5-2 (Cont.) Sample pmdf configure mailbox_servers dialogue

Do you want to use answers from the previous run as defaults [N]?

This utility creates the following files

- /pmdf/table/dispatcher_mailbox_servers.cnf
- /pmdf/table/pop3d.cnf if native mail file is selected
- /pmdf/table/imapd.cnf if native mail file is selected
- /pmdf/table/imappop.cnf if MessageStore or popstore is selected
- /pmdf/table/msgstore.chans if MessageStore or popstore is selected
- /pmdf/table/msgstore.rules if MessageStore or popstore is selected
- /pmdf/table/msgstore_option if MessageStore or popstore is selected
- /pmdf/table/popstore_option if MessageStore or popstore is selected

Do you wish to continue [Y]?

Do you wish to have a detailed explanation printed before each question [N]? **y**

Enter YES if you want to use a POP3 server in PMDF.
Enter NO if you do not want any POP3 server at all.

Do you wish to run a POP3 server [Y]?

POP server

- (1) Native BSD mail files and popstore
- (2) MessageStore and popstore

There are currently two POP servers in PMDF:
Choosing (1) will select the POP server which serves out native BSD mail files or popstore messages. The POP3 server looks for user account in popstore first; if user does not have a popstore account, then his native BSD mail file is served out. This allows you to migrate POP3 only users to the more efficient popstore.

popstore is optimized for POP3 access. MessageStore is optimized for IMAP, but also can be used for POP. Native mail is not optimized for either POP or IMAP. If most of your users only use POP, then we recommend you choose (1) and put users in popstore. If most of your users use IMAP, then we recommend you use MessageStore, and put your users in MessageStore while specifying each as either a POP or IMAP user. Choose (2) to use MessageStore for your POP users also.

What do you want to use with this server [1]? **2**

Enter the maximum number of connections you want to support concurrently on your system. Each POP3 user would normally have one connection when they connect to the server.

MAXIMUM concurrent POP3 connections you want supported on this system [25]?

Enter the maximum number of connections you want to support concurrently for each POP server process.

MAXIMUM concurrent POP3 connections to allow per server process [5]?

Enter YES if you want to turn on support for the POP3 command UIDL.

Do you want the POP3 server to support the UIDL command [Y]?

Example 5-2 Cont'd on next page

PMDF-MTA and IMAP Example Configuration

Command Line Example Configuration

Example 5-2 (Cont.) Sample pmdf configure mailbox_servers dialogue

Enter YES if you want to use an IMAP server in PMDF.
Enter NO if you do not want any IMAP server at all.

Do you wish to run an IMAP server [Y]?

IMAP server

- (1) Native BSD mail files
- (2) MessageStore

There are currently two IMAP servers in PMDF:
Choosing (1) will select the IMAP server which serves out native BSD mail files
Choosing (2) will select the IMAP server which serves out the mail in the MessageStore.

MessageStore is optimized for IMAP but also can be used for POP. Native mail is not optimized for either POP or IMAP. If you wish to serve out both native mail and MessageStore, you have to run the two servers on different ports, and you have to configure it manually. This procedure does not produce such a configuration for you. Choose the one you want to have on the standard IMAP port, and add the other one manually later to your dispatcher_mailbox_servers.cnf file. It is easier to choose the MessageStore and manually add the native mail than vice versa.

What do you want to use with this server [1]? **2**

Enter the maximum number of connections you want to support concurrently on your system. Each IMAP user would normally have several connections when connected to the server, and some may last hours or days.

MAXIMUM concurrent IMAP connections you want to support on this system [25]?

Enter the maximum number of connections you want to support concurrently per IMAP server process.

MAXIMUM concurrent IMAP connections to allow per server process [5]?

Enter YES if you want to log POP and/or IMAP connection information in the PMDF mail.log_current file.

Do you wish to log connections [N]? **y**

Enter the domain name to associate with the msgstore; e.g., msgstore.example.com.

Domain name corresponding to MessageStore/popstore []? **msgstore.naples.example.com**

Enter the default message quota in Kbytes where 1 Kbyte is 1024 bytes. Users may not receive new mail messages when their current storage usage is at or exceeds the sum of their message quota and message overdraft quota. A message quota of zero conveys unlimited storage quota.

Default message quota in Kbytes [10240]?

Enter the default message overdraft quota in Kbytes where 1 Kbyte is 1024 bytes. The overdraft quota is the amount by which users may exceed their account quota.

Example 5-2 Cont'd on next page

PMDF-MTA and IMAP Example Configuration

Command Line Example Configuration

Example 5–2 (Cont.) Sample pmdf configure mailbox_servers dialogue

Default message overdraft quota in Kbytes [512]? **4096**

Enter the name to reserve for posting to public folders, so that sending to "post+foo" will go into that "Public Folders/foo" if permissions permit,

Name to reserve for posting to public folders [post]?

Enter YES if you wish to permit public posting to public folders by default, and NO if you do not.

Should public folders default to permit public posting [Y]? **n**

Enter the name of the file for the Mailbox Servers to be included in the Dispatcher configuration.

PMDF Mailbox Servers configuration file name [/pmdf/table/dispatcher_mailbox_servers.

Enter the name of the POP/IMAP server configuration option file.

IMAP/POP server for the MessageStore configuration option file name [/pmdf/table/imap

Enter the name of the MessageStore/popstore channel definition file.

MessageStore channel definitions file name [/pmdf/table/msgstore.chans]?

Enter the name of the MessageStore/popstore rewrite rules file.

MessageStore rewrite rules file name [/pmdf/table/msgstore.rules]?

Enter the name of the MessageStore channel option file.

MessageStore/popstore channel option file name [/pmdf/table/msgstore_option]?

Enter the name of the popstore channel option file.
(It is used by the MessageStore also.)

popstore option file name [/pmdf/table/popstore_option]?

>>> WARNING WARNING WARNING <<<

WARNING: If you have popstore accounts which were created with USERNAME_STYLE other than 3 (including all popstore accounts created by versions prior to PMDF 6.0), then running this configuration utility could make those accounts inaccessible. Please see Sections 1.3.1 and 3.3 of the MessageStore and popstore Manager's Guide for information on the USERNAME_STYLE option.

>>> WARNING WARNING WARNING <<<

This procedure generates a checklist file that contains the list of steps you must perform in order to complete your PMDF configuration. This procedure does **NOT** perform these steps itself; you must do them manually.

PMDF checklist file name [/pmdf/table/mailbox_servers.checklist]?

This question gives you a last chance to change your mind before any files are written. Answer NO if you are not sure you want to generate the configuration you have specified. Answer YES if you do.

Do you wish to generate the configuration files [Y]?

Example 5–2 Cont'd on next page

PMDF-MTA and IMAP Example Configuration

Command Line Example Configuration

Example 5–2 (Cont.) Sample pmdf configure mailbox_servers dialogue

```
Generating the file /pmdf/table/dispatcher_mailbox_servers.cnf...
Generating the file /pmdf/table/imappop.cnf...
Generating the file /pmdf/table/msgstore.rules...
Generating the file /pmdf/table/msgstore.chans...
Generating the file /pmdf/table/msgstore_option...
Generating the file /pmdf/table/popstore_option...
Forking a child to create a default user account...
popstore "default" user account successfully created

Generating the checklist file, /pmdf/table/mailbox_servers.checklist...
*****
*
*   To complete your PMDF configuration, carry out the steps
*   detailed in the checklist file /pmdf/table/mailbox_servers.checklist.
*
*****

Enter YES if you want to see the checklist now. You can still type
the file out later if you say NO.

Do you want to see the checklist now [Y]? 
Checklist for completing the setup of your PMDF POP and IMAP servers
Written by root, Thu Nov 17 16:36:53 EST 2011
This file was created by the PMDF configuration generator V6.8

(1) Be sure to shutdown any POP/IMAP servers currently
    running, and if they were not running under the PMDF
    Dispatcher, you should disable them using whatever method
    is appropriate for them so they won't interfere the next
    time the system reboots.

(2) Uncomment the line in the file /pmdf/table/dispatcher.cnf
    which looks like:

!</pmdf/table/dispatcher_mailbox_servers.cnf
    so that it looks like:
</pmdf/table/dispatcher_mailbox_servers.cnf

(3) Uncomment the lines in the file /pmdf/table/http.cnf for popstore
    and/or MessageStore cgi if you want to enable web-based access to
    MessageStore/popstore User Interface,
    popstore Administration, and/or
    MessageStore Administration.

(4) Changes to existing configuration files won't be seen until
    you restart the Dispatcher with the command

        pmdf restart dispatcher

(5) If you want the SMTP/POP/IMAP connections to be logged to
    a different file other than the mail.log_current file, then set
```

Example 5–2 Cont'd on next page

PMDF-MTA and IMAP Example Configuration

Command Line Example Configuration

Example 5–2 (Cont.) Sample pmdf configure mailbox_servers dialogue

```
SEPARATE_CONNECTION_LOG=1  
LOG_CONNECTION=3
```

in the PMDF option file, option.dat.

5.2 Web-Based Example Configuration

Figure 5–4 through Figure 5–15 show a sample PMDF-MTA configuration session, including IMAP/POP server configuration, using the web-based configuration utility.

If this is an initial PMDF configuration where PMDF is not yet running, you will need to start up the PMDF HTTP server in standalone mode via the command (issued from the `root` or `pmdf` account):

```
# /pmdf/bin/http_server -s
```

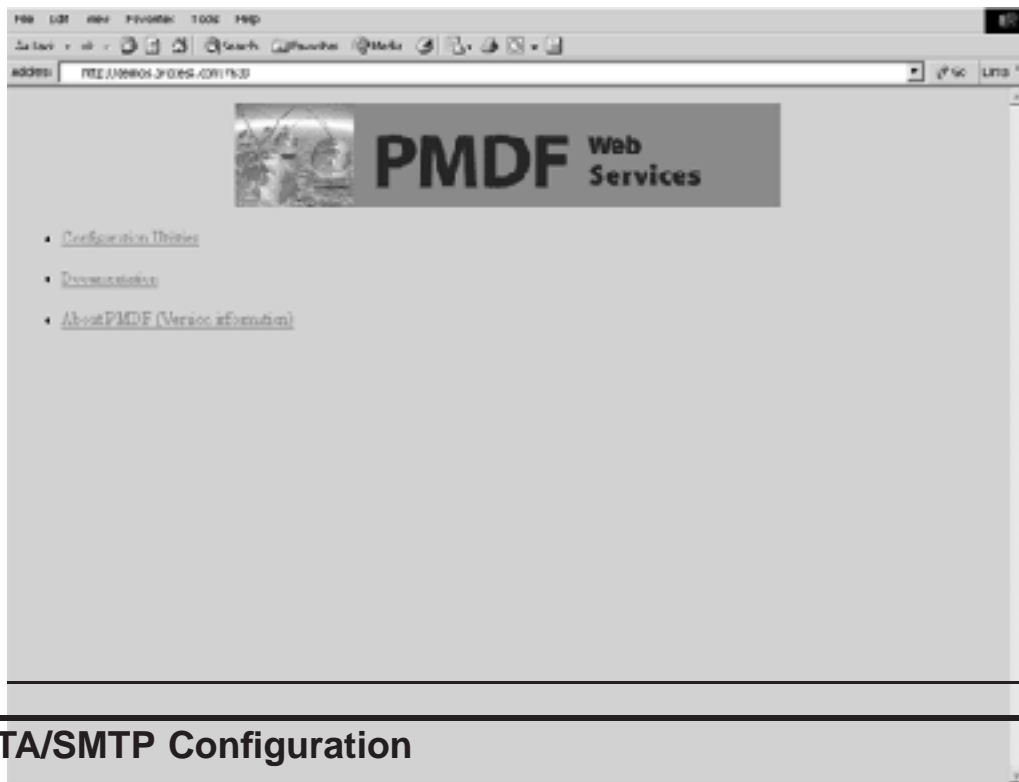
Once the PMDF HTTP server is running, either in standalone mode for a new installation or on a previously configured PMDF system, then to access the web-based configuration utility you must point your web browser at the appropriate URL. Using Netscape (version 3.0 or later) or Microsoft Internet Explorer (version 4.0 or later), with JavaScript enabled, connect to

```
http://localhost:7633/
```

where *localhost* is the TCP/IP name of your PMDF system. If this is a configuration for an initial PMDF installation with the PMDF HTTP server running in standalone mode, you will then see a screen such as shown in Figure 5–2; if this is a configuration (or re-configuration) on a system with PMDF already running, you will then see a screen such as shown in Figure 5–3. To begin the configuration, select the “Configuration Utilities” link from the HTTP server main page as shown in Figure 5–3.

Note that if you have previously run the web-based configuration utility, then you may use the “Load” button of the initial page, Figure 5–4, to load your previous session’s answers; those answers will then become the defaults for this new session. When you are satisfied with the answers on a given page, press the “Next” (or “Done”) button to continue the configuration.

Figure 5–2 HTTP Server Standalone Main Page



5.3 MTA/SMTP Configuration

Figure 5–4 shows the initial page displayed by the PMDF HTTP server when run in standalone mode (`/pmdf/bin/http_server -s`).

Figure 5–5 shows the regular initial page displayed by the PMDF HTTP server, once PMDF has been initially configured. So if you are reconfiguring an existing PMDF, this is the sort of display you would see.

PMDF-MTA and IMAP Example Configuration

MTA/SMTP Configuration

Figure 5-3 HTTP Server Main Page

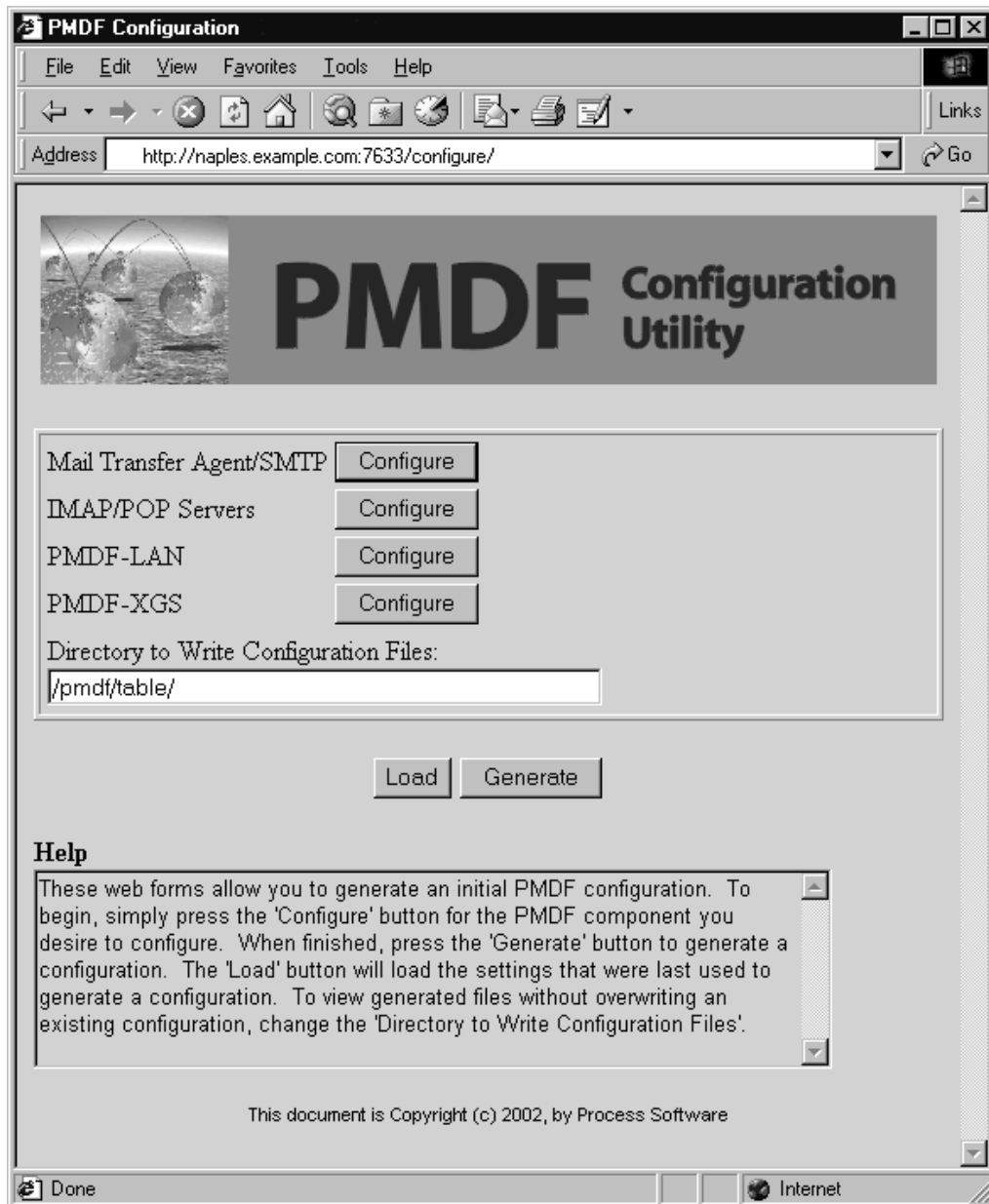


PMDF-MTA and IMAP Example Configuration

MTA/SMTP Configuration

Figure 5-4 shows the PMDF web-based configuration utility main menu, as seen at the beginning of a configuration session. The utility will write files generated during configuration to the directory shown in the “Directory to Write Configuration Files”. The default is `/pmdf/table`, the live configuration directory. If you want to experiment with configuration rather than generate live files, you may specify an alternate directory.

Figure 5-4 Configuration Main Page



PMDF-MTA and IMAP Example Configuration

MTA/SMTP Configuration

Figure 5-5 shows the first page of the PMDF-MTA/SMTP configuration component, which asks for information about the local host (the system running PMDF).

Figure 5-5 PMDF-MTA/SMTP Configuration, Local Host Information

The screenshot shows a web browser window titled "MTA - Local Host Information". The address bar contains "http://naples.example.com:7633/configure/". The page features a header with a globe image and the text "PMDF Configuration Utility". Below the header, there are two text input fields: "Name of this System on TCP/IP:" with the value "naples.example.com" and "Domain Name for Local Channel:" with the value "naples.example.com".

The "Aliases for the Local Host:" section contains a list box with "localhost" and "naples" (the latter is selected). To the right is a text input field for "Alias for the Local Host:" and a "Delete" button.

The "IP Addresses for Local Host:" section contains a list box with "192.168.1.1" and a text input field for "IP Address:" with a "Delete" button.

At the bottom, there are "Main" and "Next >>" buttons. A "Help" section contains a text box with the text: "Enter the IP addresses for all the interfaces used by TCP/IP on this system. These addresses are needed so that domain literal references to this system can be identified. Such recognition is mandated by RFC1123."

The browser status bar at the bottom shows "Done" and "Internet".

PMDF-MTA and IMAP Example Configuration

MTA/SMTP Configuration

Figure 5-6 shows the second page of the PMDF-MTA/SMTP configuration component, which asks for information about any other “internal” systems.

Figure 5-6 PMDF-MTA/SMTP Configuration, Local Network Information

The screenshot shows a web browser window titled "MTA - Local Network Information". The address bar contains "http://naples.example.com:7633/configure/". The page features a header with the PMDF logo and the text "Configuration Utility". Below the header, there are three main sections for configuration:

- If Routing Internet Mail to a Firewall:** This section contains two input fields: "Domain Name of Firewall:" and "IP Address of Firewall:".
- Internal System Domains and Domain Names:** This section includes a list box with "example.com" and "vaxa.otherco.com". To the right of the list box are buttons for "<< Add" and "Delete". To the right of the list box is an input field labeled "Internal System Domains:".
- Internal System IP Sub-Networks and Addresses:** This section includes a list box with "192.168.1.*". To the right of the list box are buttons for "<< Add" and "Delete". To the right of the list box is an input field labeled "Internal System IP:".

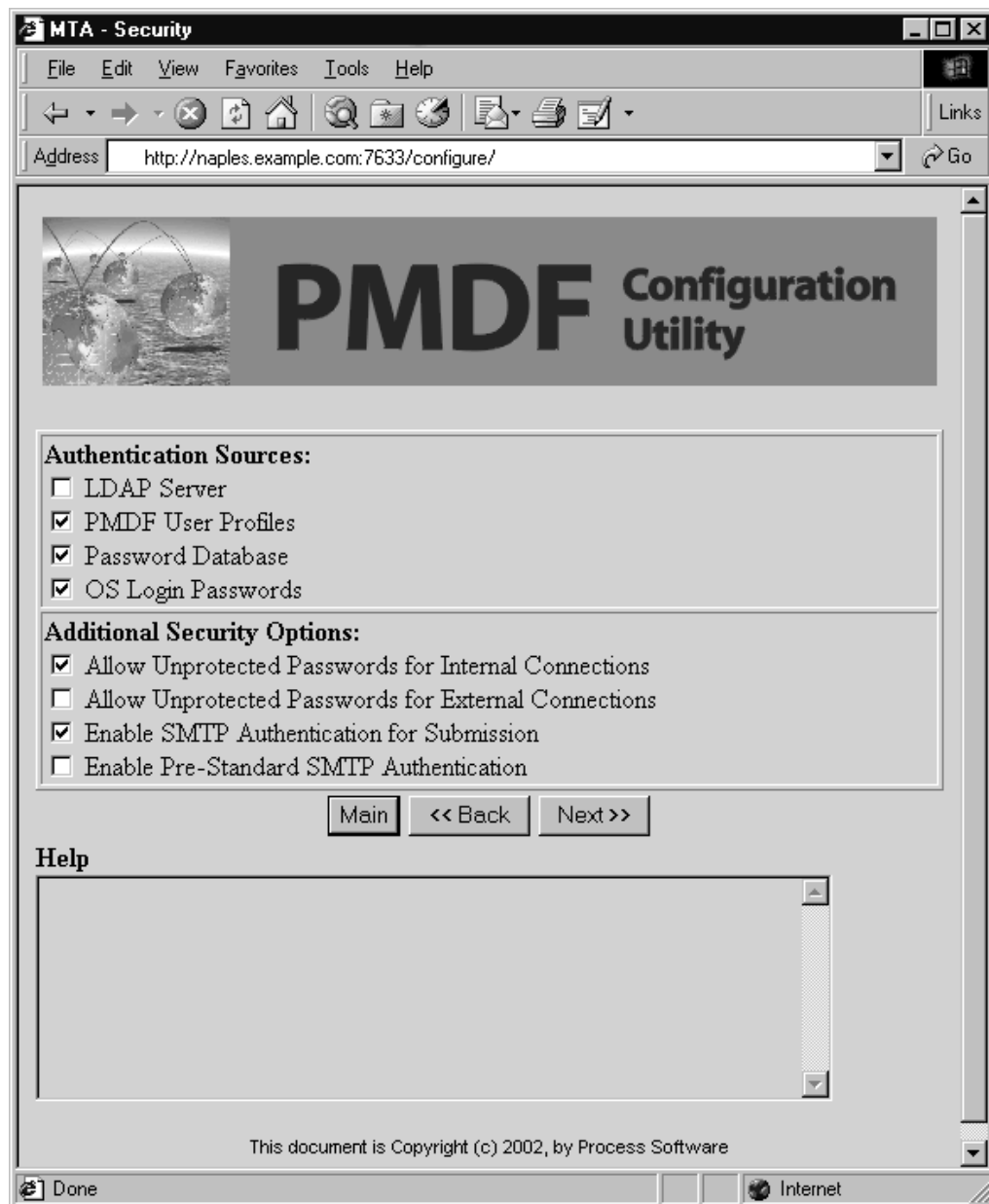
At the bottom of the configuration area, there are three buttons: "Main", "<< Back", and "Next >>". Below these buttons is a "Help" section with a text area containing the following text: "Enter the IP addresses and IP sub-network(s) for hosts internal to your domain. This should include all hosts where users are permitted to run mail clients which submit mail via SMTP without authentication. Use IP addresses in a.b.c.d notation (where a, b, c and d are numbers), or an IP subnet in". The browser's status bar at the bottom shows "Done" and "Internet".

PMDF-MTA and IMAP Example Configuration

MTA/SMTP Configuration

Figure 5–7 shows configuring which authentication sources PMDF will check against when verifying passwords (as for IMAP or POP connections, if IMAP or POP servers are later configured, or for mailbox filter authentication, or for SMTP SASL authentication by clients submitting messages to PMDF), and whether to configure to allow SMTP AUTH (SASL) use.

Figure 5–7 PMDF-MTA/SMTP Configuration, Security Information

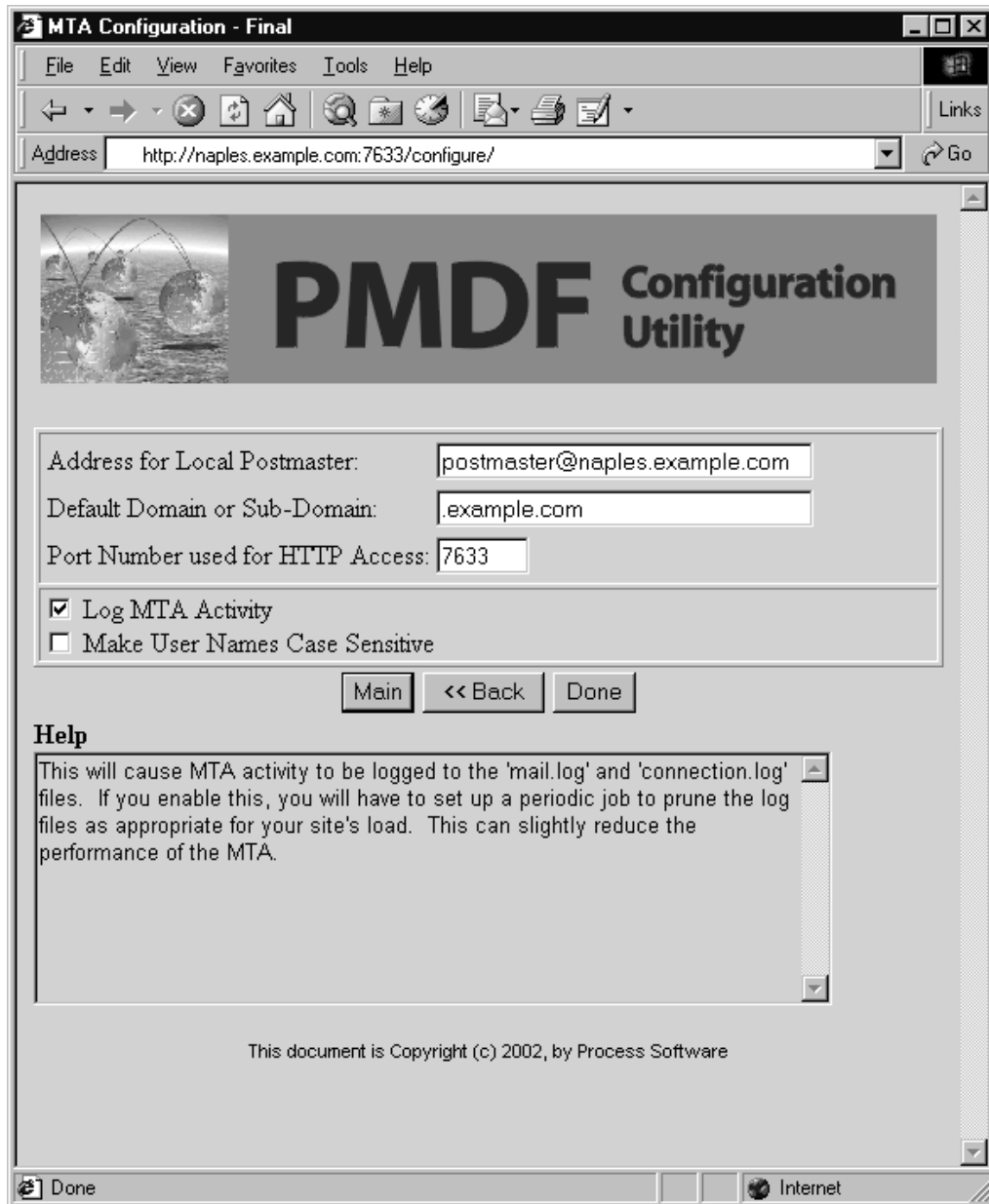


PMDF-MTA and IMAP Example Configuration

MTA/SMTP Configuration

Figure 5–8 shows the final page of entering PMDF-MTA/SMTP configuration information. Clicking on the “Done” button on this page will return you to the PMDF configuration utility main page, as shown in Figure 5–9.

Figure 5–8 PMDF-MTA/SMTP Configuration, Final Details Page

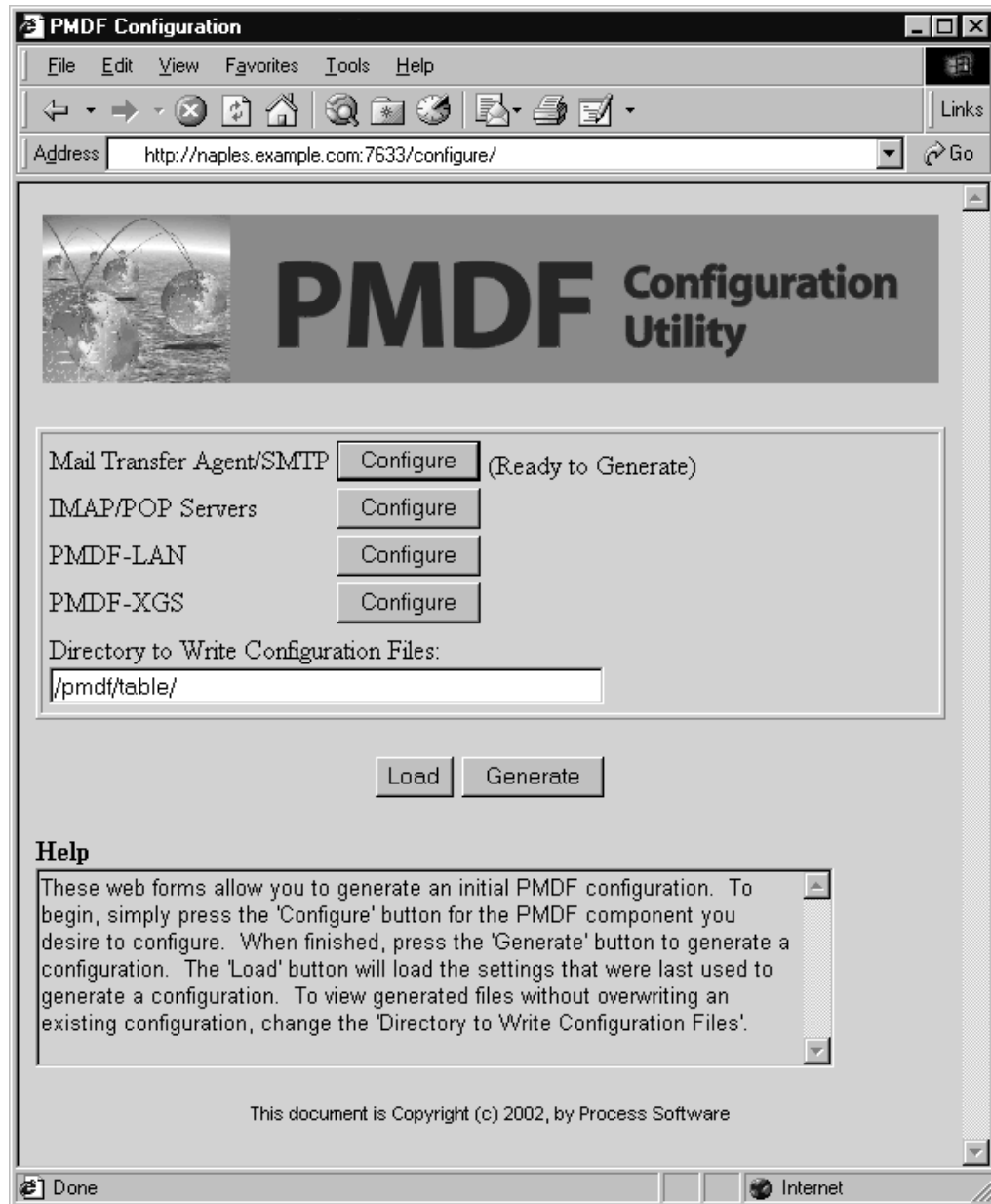


PMDF-MTA and IMAP Example Configuration

MTA/SMTP Configuration

Figure 5–9 shows the configuration utility main menu, after entering configuration information for the MTA/SMTP component. At this point you may either generate just the main MTA configuration files by clicking the “Generate” button, or you may select another component to also configure at this time. For instance, clicking the IMAP/POP Servers “Configure” button will continue the configuration, as shown in Figure 5–10 through Figure 5–15 following.

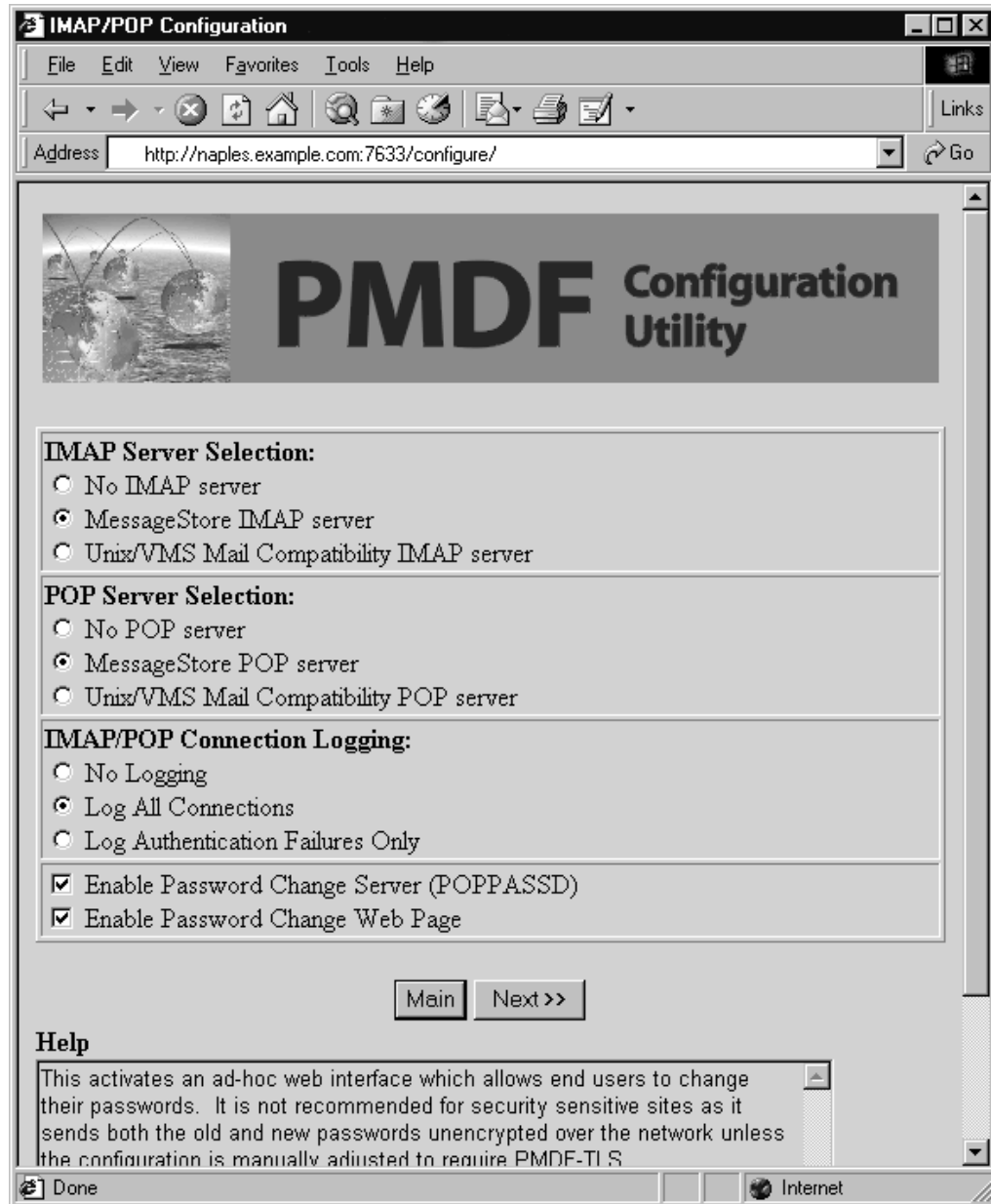
Figure 5–9 Configuration Main Page, MTA Configuration Entered



5.4 IMAP/POP Server Sample Configuration

Figure 5–10 shows the first screen of the IMAP/POP Servers configuration component.

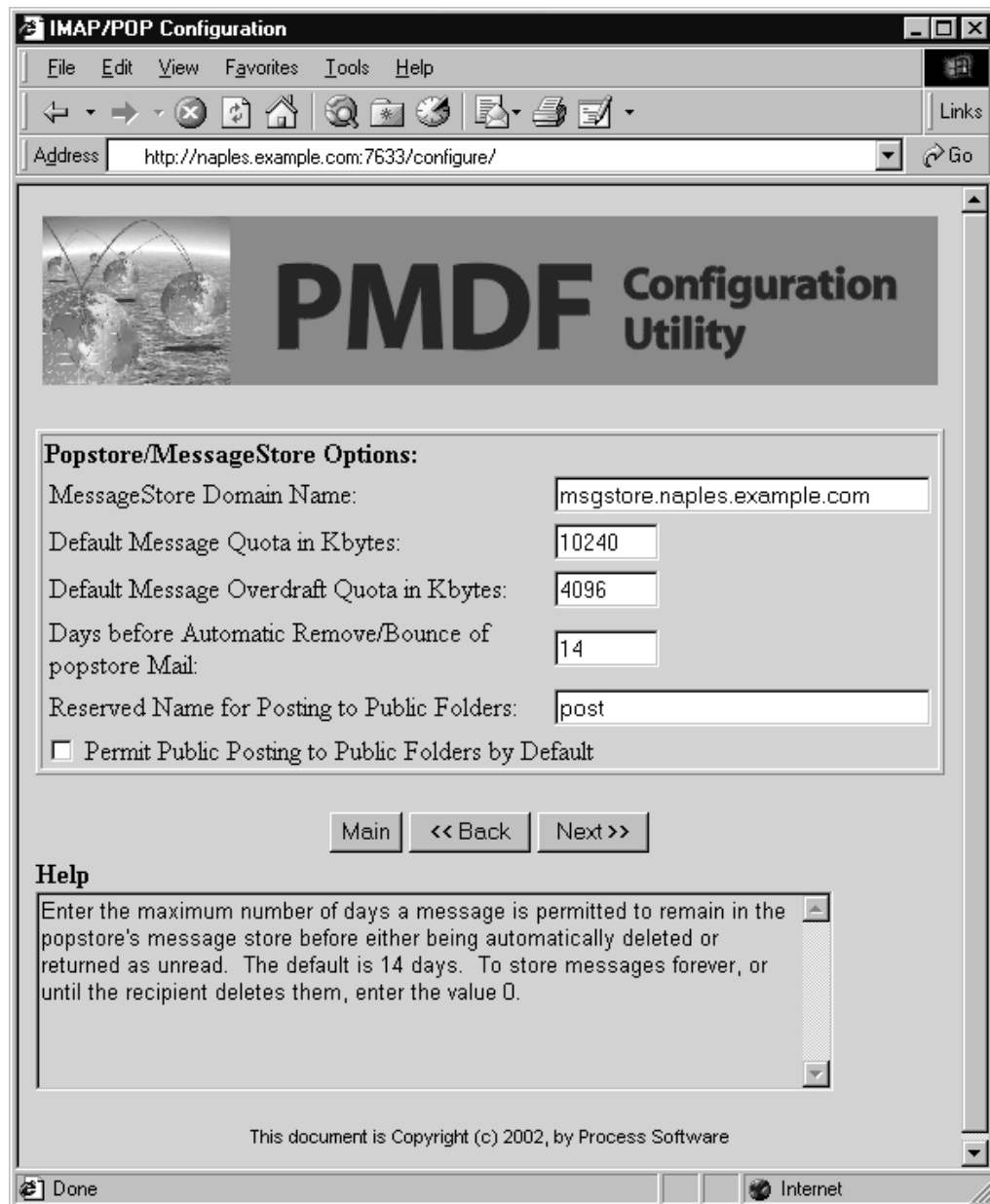
Figure 5–10 IMAP/POP Configuration, Select Servers



PMDF-MTA and IMAP Example Configuration

IMAP/POP Server Sample Configuration

Figure 5–11 IMAP/POP Configuration, popstore/MessageStore Information



The screenshot shows a web browser window titled "IMAP/POP Configuration" with the address bar set to "http://naples.example.com:7633/configure/". The main content area features a banner for "PMDF Configuration Utility" and a configuration form for "Popstore/MessageStore Options".

Popstore/MessageStore Options:

MessageStore Domain Name:	<input type="text" value="msgstore.naples.example.com"/>
Default Message Quota in Kbytes:	<input type="text" value="10240"/>
Default Message Overdraft Quota in Kbytes:	<input type="text" value="4096"/>
Days before Automatic Remove/Bounce of popstore Mail:	<input type="text" value="14"/>
Reserved Name for Posting to Public Folders:	<input type="text" value="post"/>

Permit Public Posting to Public Folders by Default

Navigation buttons: [Main](#) [<< Back](#) [Next >>](#)

Help

Enter the maximum number of days a message is permitted to remain in the popstore's message store before either being automatically deleted or returned as unread. The default is 14 days. To store messages forever, or until the recipient deletes them, enter the value 0.

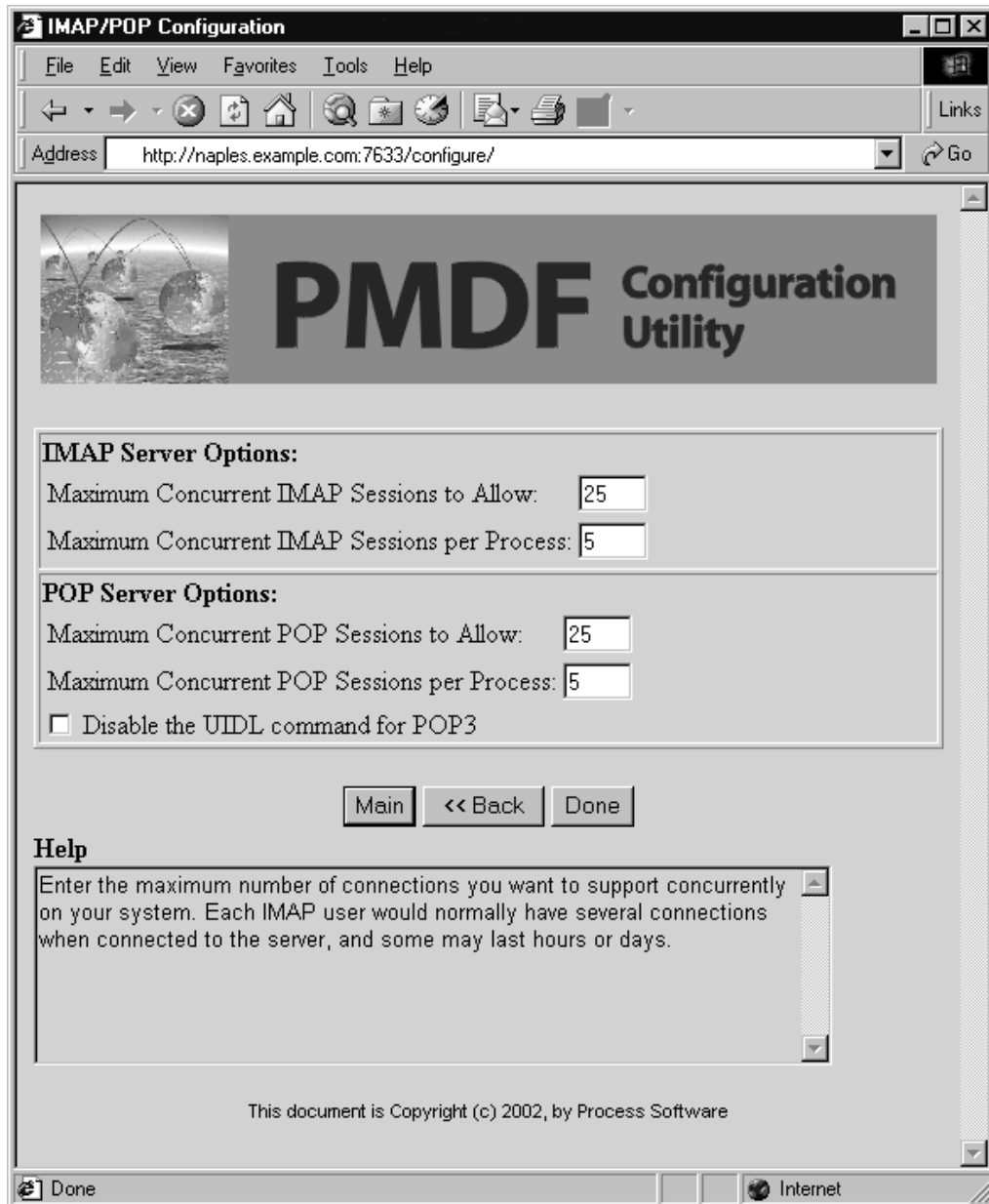
This document is Copyright (c) 2002, by Process Software

Browser status bar: Done Internet

PMDF-MTA and IMAP Example Configuration

IMAP/POP Server Sample Configuration

Figure 5–12 IMAP/POP Configuration, Server Information



The screenshot shows a web browser window titled "IMAP/POP Configuration" with the address bar set to "http://naples.example.com:7633/configure/". The main content area features a banner for "PMDF Configuration Utility" with a background image of a globe. Below the banner, there are two sections for server options:

IMAP Server Options:

- Maximum Concurrent IMAP Sessions to Allow:
- Maximum Concurrent IMAP Sessions per Process:

POP Server Options:

- Maximum Concurrent POP Sessions to Allow:
- Maximum Concurrent POP Sessions per Process:
- Disable the UIDL command for POP3

Navigation buttons include "Main", "<< Back", and "Done". A "Help" section contains a text box with the following text:

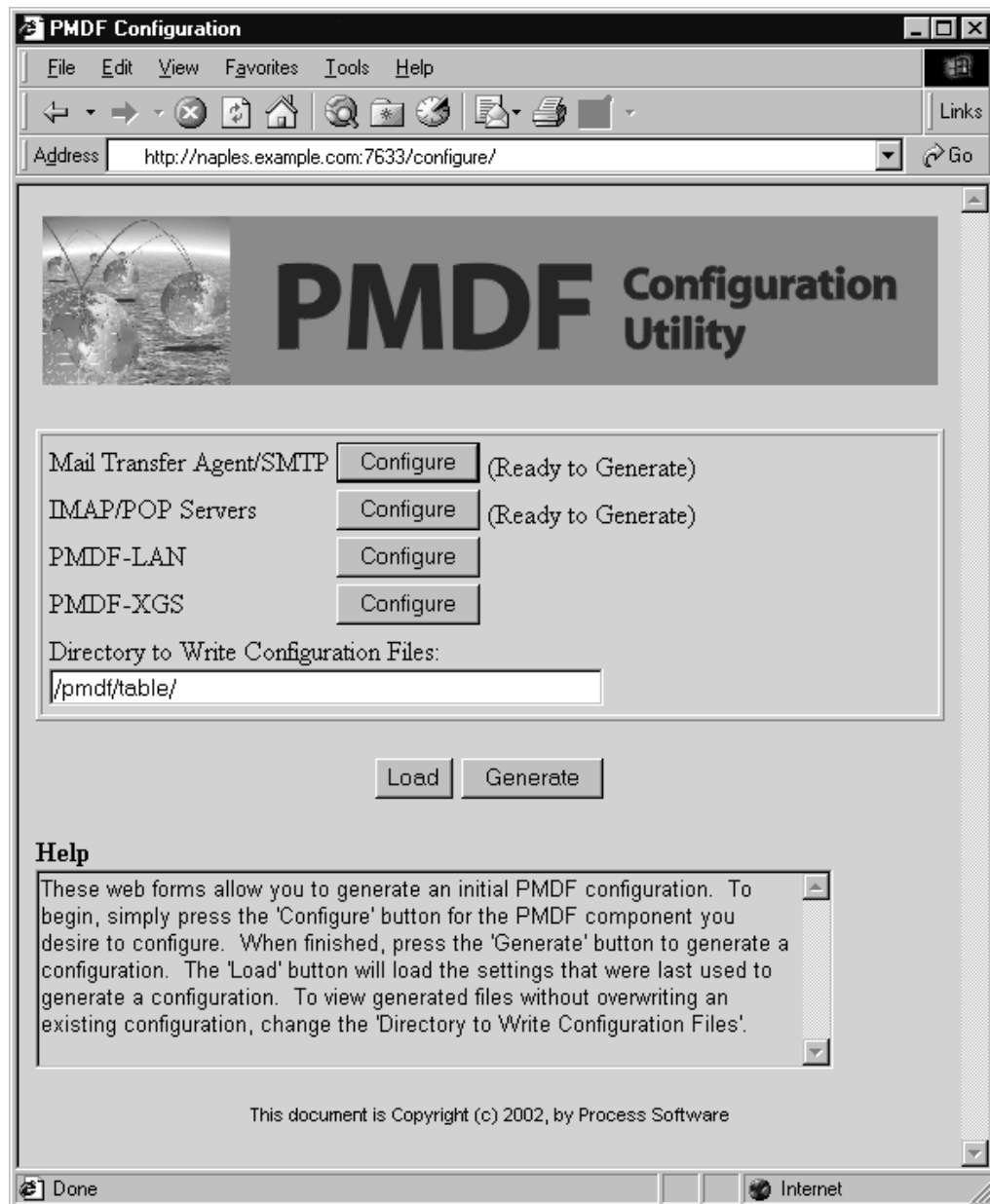
Enter the maximum number of connections you want to support concurrently on your system. Each IMAP user would normally have several connections when connected to the server, and some may last hours or days.

At the bottom of the page, a copyright notice reads: "This document is Copyright (c) 2002, by Process Software". The browser's status bar shows "Done" and "Internet".

PMDF-MTA and IMAP Example Configuration

IMAP/POP Server Sample Configuration

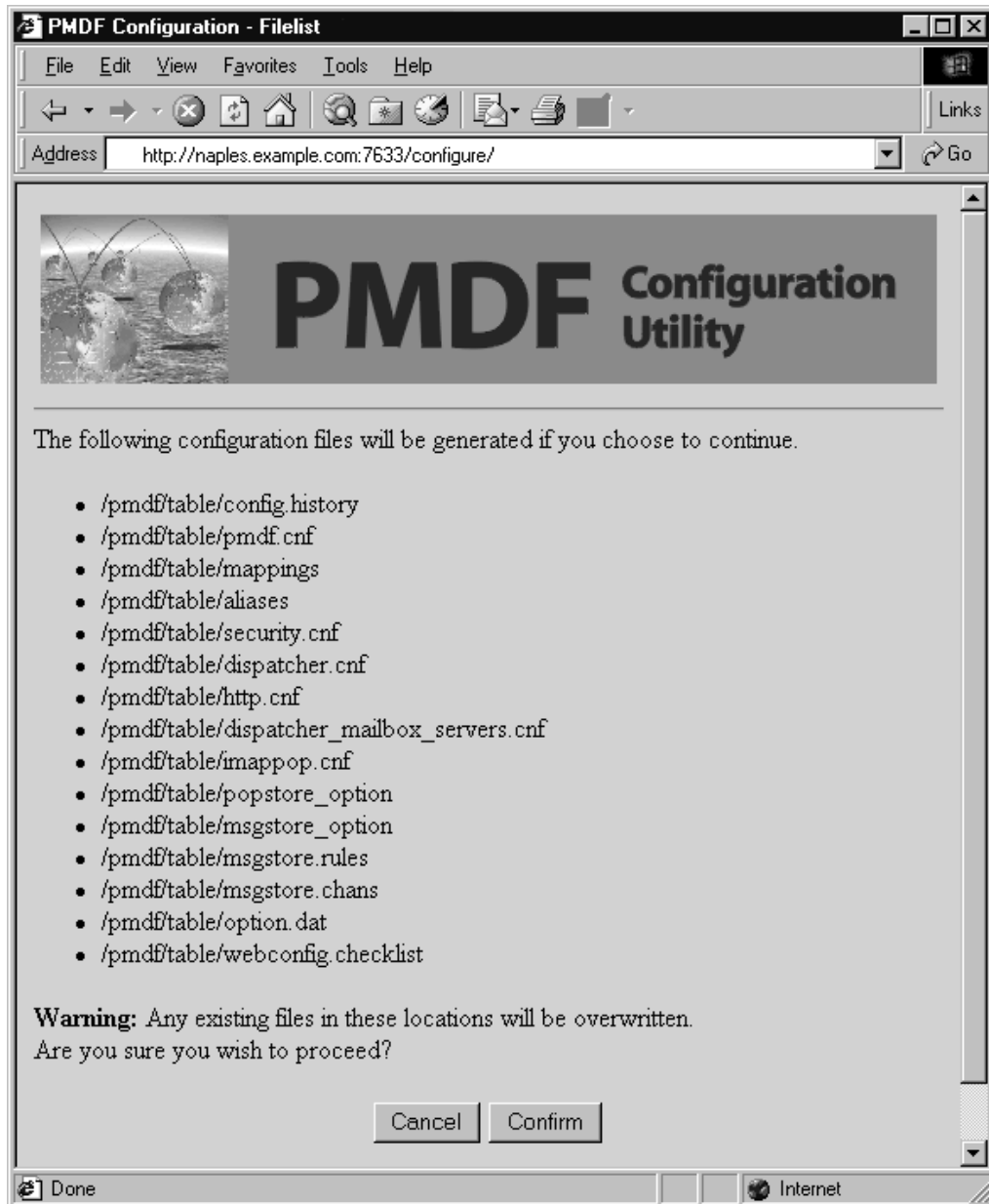
Figure 5–13 Configuration Main Page, MTA and IMAP/POP Configurations Entered



PMDF-MTA and IMAP Example Configuration

IMAP/POP Server Sample Configuration

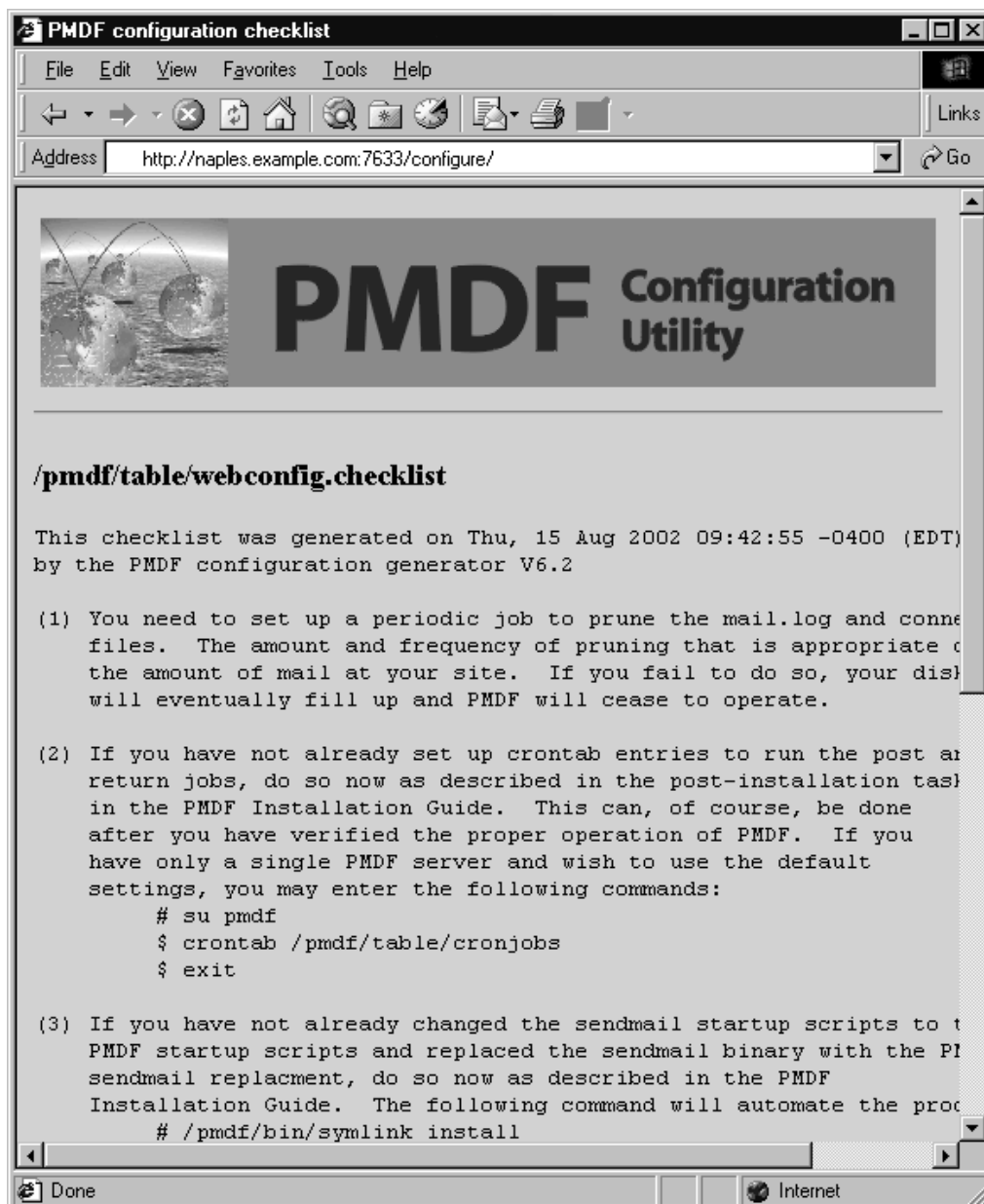
Figure 5–14 Generate Files



PMDF-MTA and IMAP Example Configuration

IMAP/POP Server Sample Configuration

Figure 5-15 MTA and IMAP/POP Checklist File



6 Configuring PMDF-MTA to act as an E-mail Firewall

This chapter describes how to use the `pmdf configure firewall` utility to create an initial configuration for use on an e-mail firewall system. In many cases the configuration created by following these steps will suffice for a firewall system without further modification. Additional customization, for instance, implementing centralized naming on the e-mail firewall, the addition of some channels such as UUCP channels or PhoneNet channels not generated by the utility, implementation of address-specific e-mail access controls, implementation of mail storm or denial or service safeguards, or hooking in a virus scanner via the PMDF conversion channel, will require manual editing of the configuration files.

Manual editing of the configuration files may also be required as your environment evolves. For example, as nodes or networks are added you may need to add rewrite rules or channel blocks to your `pmdf.cnf` file. In many cases you may find it easier to rerun the configuration generator supplying new answers reflecting the changes in your environment.

A history of the configuration run is saved in the file `firewall_configure.history` in the PMDF table directory when you run the `pmdf configure firewall` utility. When you run `pmdf configure firewall` again, you will be prompted as to whether the answers from the history file should be used as default answers. The history file should not be deleted casually, as it could save you from typing the same answers over again, and may prove useful to technical support should you encounter problems.

6.1 Before You Begin

First, before concerning yourself with the setup of e-mail control and restrictions, *i.e.*, an e-mail firewall, you should have a basic Internet firewall setup in place, *i.e.*, TCP/IP level controls in place for functions such as FTP access and remote login access. E-mail is generally much less of an overall security concern than such lower level access issues.

Next, you should consider establishing e-mail policies for your site, taking the next step along the lines of the general security policies you presumably considered and established when setting up your Internet firewall. For instance, depending upon your site, you may want to have explicit policies regarding mail spoofing, the sending of harassing e-mail, list subscriptions, the sending of virus-infected PC executable programs, the use of e-mail for personal business, *etc.*

What is appropriate policy for your site will depend upon your site's goals and needs and what can be reasonably expected from your users. *Your greatest aid in good e-mail security, as in other security, is users who are educated as to your policies and committed to implementing them.* With the tightest security procedures in the world, if your users do not understand the reasons for your policies and practices or find them overly burdensome, sooner or later some users will disregard or circumvent them.

Configuring PMDF-MTA to act as an E-mail Firewall Before You Begin

Then gather any information you will need to provide as input to the firewall configuration utility. Prior to running the automatic configuration generator, you should have a good idea of your network configuration. Note that `pmdf configure firewall` will attempt to provide default values to its prompts. These defaults are picked up, whenever possible, from your system environment.

The *PMDF System Manager's Guide* discusses issues to consider and approaches that can be used to implement an effective e-mail firewall. Either before or after running the firewall configuration utility, you may want to look over the description contained there to better understand the details of your firewall configuration and what additional features beyond those generated automatically by the firewall configuration utility you may want to implement.

In particular, note that in a firewall configuration you usually want the PMDF firewall system to have a good idea of the names or domains and IP numbers of all of your internal systems. In a regular PMDF configuration, PMDF is generally not configured to make much if any distinction between “internal” and “external” addresses and messages; as long as the address is a valid address, PMDF will handle the message. However, one of the fundamental features of a firewall configuration tends to be a desire to distinguish between “internal” and “external” addresses and messages; this requires that you provide PMDF with more information as to just which addresses, system and domain names, and IP numbers are to be considered “internal” versus “external”.

Another issue to consider is how regularly e-mail system maintenance checks will be performed on a firewall system.

For instance, Internet domains are required to have a postmaster address which accepts mail. Therefore you must have a postmaster address “on” (at least apparently) the firewall system. Since a postmaster address is the one address that must always be able to accept mail, it is usually wise to have postmaster mail delivered as simply and directly as possible to some account, without forwarding or additional network or mail system hops that present additional possible points of failure. However, in the case of a firewall which will be operating essentially unattended for long periods of time, some sites may decide to forward postmaster mail to an account on a different system; if you choose to do this, be sure to forward the mail over a reliable connection, not subject to frequent or unexpected failures, and do keep in mind that an interruption in this connection can lead quickly to mail system problems.

Another issue related to maintenance of the firewall system is logging. PMDF has detailed logging which may be enabled. Such logging can be useful in gathering message traffic statistics and in tracking down problems. However, if you enable such logging, you should also have a plan for periodically logging on to the firewall system to check on and truncate, or save to tape, or delete, as you prefer, the PMDF cumulative log file. PMDF never does anything with the `mail.log` itself, other than continue to append to it.

Configuring PMDF-MTA to act as an E-mail Firewall Using the Firewall Configuration Utility

6.2 Using the Firewall Configuration Utility

This section presents a step-by-step procedure for generating your PMDF firewall configuration files using the PMDF firewall configuration utility, `pmdf configure firewall`. Refer to Chapter 7 for a sample configuration dialogue.

1. Configuration of PMDF should be done by `root` to ensure that the necessary privileges are available to create the configuration files. If you are not logged in as `root`, do so now.
2. Begin the configuration procedure by invoking the `pmdf configure firewall` utility as follows, assuming that you have `/usr/bin` in your search path:

```
# cd /pmdf/table
# pmdf configure firewall
```

3. The configuration procedure will optionally print out detailed explanations of each prompt as it proceeds. Unless you are familiar with the procedure, enable the detailed output.
4. Closely examine the example configuration presented in Chapter 7. Parts of the sample site are probably representative of your own network configuration. In addition, the example was run with detailed prompting enabled, and will prepare you for the answers you need to provide for your own site.
5. Once you're completed running the `pmdf configure firewall` utility, type out or print the `/pmdf/table/firewall.checklist` file and complete the configuration by following the steps outlined in the checklist.
6. Test out your configuration initially by sending mail from the firewall system to someone on an internal system. Using the PMDF `pine` utility, send a message to an address of the form

```
username@domain
```

where *username@domain* is a valid address. PMDF should accept the message and send it off the firewall system.

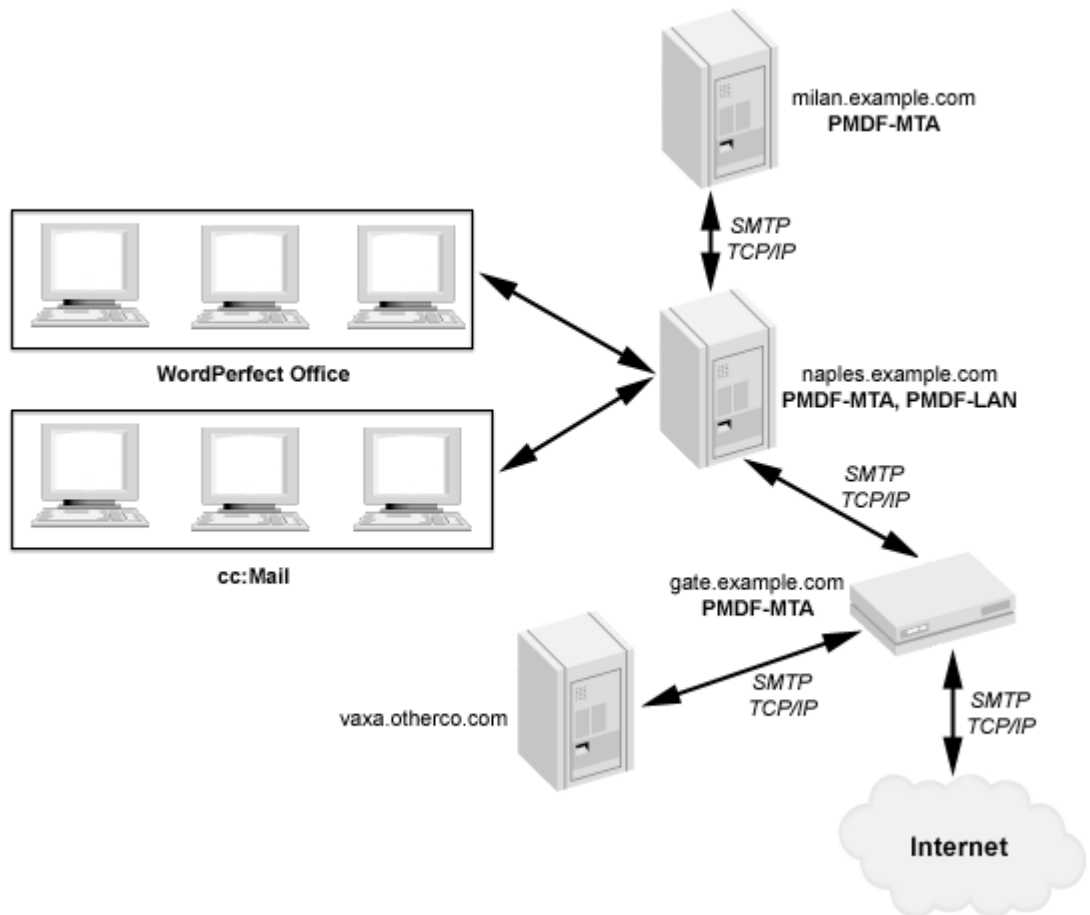
7. If messages do not seem to be getting out, check the subdirectories in the `/pmdf/queue` area or use the `pmdf cache -view` utility to check whether the messages is stuck in the PMDF message queues on your system. Examination of log files in the `/pmdf/log` directory may help isolate network delivery problems. See the section *Maintenance and Troubleshooting* in the *PMDF System Manager's Guide* for additional information on tracking PMDF delivery problems.

Configuring PMDF-MTA to act as an E-mail Firewall Using the Firewall Configuration Utility

8. If everything appears to be functional, and you have completed your configuration for the present, you may want to compile your configuration for increased performance. Use the `pmdf cnbuild` utility. See the *PMDF System Manager's Guide* for more information.

7 E-mail Firewall Example Configuration

Figure 7-1 Sample PMDF Site EXAMPLE.COM



Example 7-1 shows a sample configuration of PMDF-MTA as an e-mail firewall using the `pmdf configure firewall` utility, and Example 7-2 shows a corresponding checklist file. The sample site EXAMPLE.COM, first introduced in Figure 5-1, is now assumed to have added another node, `gate.example.com`, that sits between the PMDF-MTA mailhub system `naples.example.com` and the Internet, as shown in Figure 7-1. The `gate.example.com` system will not have any users, except for the system manager who will log on periodically to check for postmaster messages, *etc.*

E-mail Firewall Example Configuration

The `naples.example.com` system is assumed to have been reconfigured using the `pmdf configure mta` utility to route all messages to the Internet out by way of `gate.example.com`, e.g., by answering:

```
Does this system need to route mail to a firewall [N]? YES  
Domain name for firewall system []? gate.example.com
```

Note that in Example 7–1, the firewall system is informed about the domains and IP addresses of the internal systems with which it may expect to communicate directly, `naples.example.com` (assumed to have IP addresses 192.168.1.1 and 192.168.1.8), `milan.example.com` (assumed to have IP address 192.168.1.2), and more generally is told that any IP number in the subnet 192.168.1.0 should be assumed to be internal. The non-`example.com` domain `otherco.com` (assumed to correspond to the subnet 192.168.50) is also considered here to be behind the firewall.

(Actually, since the `milan.example.com` system is a PMDF-MTA system currently configured to route all of its mail through the PMDF-MTA system `naples.example.com`, the `gate.example.com` system does not need to know about `milan.example.com` for the network setup as pictured. However, it does no harm to inform `gate.example.com` about `milan.example.com` now in case `milan.example.com` were to be reconfigured in the future to direct messages directly to `gate.example.com` itself, instead of by way of `naples.example.com`.)

The firewall configuration utility asks a question about stripping off certain tracking headers. This can be an issue for sites that are concerned about exposing internal system names in those tracking headers. (Note that stripping `Received:` and `Message-ID:` headers should be avoided unless absolutely necessary, since they provide important information used, for instance, in detecting and short-circuiting mail loops, for detecting forged messages, and for correlating messages when questions or problems arise.) In particular, in a setup such as that shown for the sample `example.com` site, which has an internal PMDF mailhub system `naples.example.com` as well as the PMDF firewall system `gate.example.com`, note that there is a much better solution than complete trimming of such headers; configuration options on the PMDF mailhub and PMDF firewall systems can be used to control what names appear in such headers generated by PMDF in the first place. And problematic headers appearing in messages that originated elsewhere but that pass through either PMDF system can often be handled with more fine tuned approaches as they pass through the PMDF system.

Whenever appropriate, each prompt also supplies a default answer which is enclosed within square brackets. Simply pressing return, `[RETURN]`, selects the default answer. You may use the backslash character, `\`, to clear a default answer.

Remember that the values entered in this sample are for purposes of example only. Be sure to use the values appropriate for your system when you perform the actual configuration.

Example 7-1 Example PMDF-MTA configuration as a firewall

```
# cd /pmdf/table
# pmdf configure firewall
```

PMDF Internet Firewall Configuration File Creation Utility, V6.8

This utility creates an initial PMDF configuration file (/pmdf/table/pmdf.cnf), an initial PMDF aliases file (/pmdf/table/aliases), an initial PMDF security configuration file (/pmdf/table/security.cnf), an initial PMDF mappings file (/pmdf/table/mappings), and an initial PMDF option file (/pmdf/table/option.dat) for a system acting as an E-mail firewall on the Internet.

For best results the various network products PMDF is going to be attached to should be installed and operational when this procedure is run. This is by no means required, but the defaults provided by this procedure cannot be selected intelligently without having various software packages available to interrogate.

Important note: No changes are made to existing PMDF configuration information until all questions have been answered. This utility can be aborted at any prompt by entering CTRL/C. The files output by this utility may optionally be redirected to a different location so they will have no impact on the existing PMDF configuration.

Do you wish to continue [Y]? **y**

Do you wish to have a detailed explanation printed before each question [N]? **y**

Part One: Determining local host's name(s).

Enter the 'most official' name for this system. This should be the official domain name in most cases. This is the name that will appear in mail addresses on this system, among other things.

Official local host name of the firewall [gate.example.com]?

gate.example.com

Enter the domain or subdomain your systems are part of, if there is one and it is consistent. For example, if your system's domain name is HMCVAX.EXAMPLE.COM, and in general all your systems are part of the .EXAMPLE.COM domain, enter '.EXAMPLE.COM'. If your system is not part of a domain or if your use of domain name is not consistent, just press CR.

Default domain or subdomain for this system [none]? **.example.com**

Enter any aliases for the local host; these names are rewritten to the official local host name with rewrite rules.

Any other aliases for the local host [RETURN if no more]? **RETURN**

This firewall system either routes all mail addressed to your internal domains to some internal system; or mail addressed to the firewall go to users who logged on the firewall system. Enter Yes if you have users on the firewall system, or No if all mail is routed somewhere else.

Example 7-1 Cont'd on next page

E-mail Firewall Example Configuration

Example 7-1 (Cont.) Example PMDF-MTA configuration as a firewall

Are there mail users on this firewall system [N]? **n**

Enter a valid user@host type of address for the firewall Postmaster. Depending on your needs, this address can be on a system different from the firewall system.

This address will receive notifications of bounced or deferred mail as well as various other types of status and error reports. This address is also the one that will receive user queries about electronic mail.

A user@host style address for the local Postmaster [root@gate.example.com]?

root@gate.example.com

Part Two: The external TCP/IP networking.

This system has one or more names it is known by on TCP/IP.

Enter the most 'official' of these names, preferably a name the system is registered under in the Domain Name System.

Name of this system on TCP/IP [gate.example.com]? **gate.example.com**

PMDF needs to know the IP addresses for all the interfaces used by TCP/IP on this system. These addresses are needed so that PMDF can recognize domain literals references to this system. Such recognition is mandated by RFC1123.

Enter each IP address separately in a.b.c.d format, pressing CR between each one. When you've entered them all just enter a CR by itself to end the list

IP addresses for this system [RETURN if no more]? **192.168.1.1**

IP addresses for this system [RETURN if no more]?

Part Three: Internal TCP/IP connections

PMDF needs to know about internal TCP/IP usage. For instance, this information is used to segregate incoming messages from internal vs. external sources. Your configuration file will automatically contain the rules necessary to reach external Internet domains, so it is not necessary to tell PMDF about external Internet systems.

If your site satisfies any of the following conditions:

- (+) POP or IMAP users,
- (+) other internal TCP/IP systems,
- (+) connect to non-Internet TCP/IP systems,

then you will need to answer YES. If you do answer YES, you will then be asked for the names of these systems or domains so that they can be added to your configuration and mappings files. Answer NO if there is no TCP/IP use behind this firewall.

Are there any internal systems reachable via TCP/IP [Y]? **y**

Is this firewall system set up to lookup the internal systems by:

- (1) Doing host lookups with MX records (name server required)
- (2) Doing host lookups without MX records

Example 7-1 Cont'd on next page

Example 7-1 (Cont.) Example PMDF-MTA configuration as a firewall

MX (Mail eXchange) records are special entries in the TCP/IP Domain Name Service database that redirect mail destined for systems not directly attached to the TCP/IP network to an intermediate gateway system that is directly attached.

If your TCP/IP package is configured to use a name server which includes MX records for your internal systems, you should answer 1; this is the most common case. Otherwise if you have the internal systems in your name server but have a special requirement to ignore MX records for internal systems, then answer 2.

Choose one of the above options [1]? **1**

TCP/IP networks typically provide access to one or more systems or entire domains. This should only include systems or domains that are accessible via TCP/IP inside your firewall.

Enter each system or domain specification (e.g., system names such as 'doofus.company.com' or domains such as '.mycollege.edu') separately, pressing CR between each one. When you've entered them all just enter a CR by itself to end the list.

Internal system or domain reachable via TCP/IP [RETURN if no more]?

naples.example.com

Internal system or domain reachable via TCP/IP [RETURN if no more]?

milan.example.com

Internal system or domain reachable via TCP/IP [RETURN if no more]?

.example.com

Internal system or domain reachable via TCP/IP [RETURN if no more]?

.otherco.com

Internal system or domain reachable via TCP/IP [RETURN if no more]?

PMDF needs to know the IP address of each internal system or subnet.

For instance, this information is used to distinguish between internal and external systems for doing SMTP relay blocking.

Enter each IP address separately in a.b.c.d, or a.b.0.0 or a.b.c.0 format, pressing CR between each one. When you've entered them all just enter a CR by itself to end the list.

IP addresses for your internal system or network [RETURN if no more]?

192.168.1.1

IP addresses for your internal system or network [RETURN if no more]?

192.168.1.7

IP addresses for your internal system or network [RETURN if no more]?

192.168.1.8

IP addresses for your internal system or network [RETURN if no more]?

192.168.0.0

IP addresses for your internal system or network [RETURN if no more]?

192.168.5.0

IP addresses for your internal system or network [RETURN if no more]?

Example 7-1 Cont'd on next page

E-mail Firewall Example Configuration

Example 7-1 (Cont.) Example PMDF-MTA configuration as a firewall

PMDF has the ability to automatically convert shortform names appearing on the right hand side of the at sign in an address into fully qualified domain names. These addresses are then routed to TCP/IP automatically. This convenience is especially appropriate when a system is only connected via TCP/IP and not via other networks. For example, if you were to specify a default domain of CLAREMONT.EDU and the address USER@SIGURD was used, where SIGURD has no other special meaning, this address will be rewritten as USER@SIGURD.CLAREMONT.EDU and routed via TCP/IP. Enter nothing if you don't want to have shortform addresses handled in this way.

Default (internal) domain to attach to shortform host names [none]?
.example.com

Enter YES if all messages to your internal systems are to be routed via a PMDF-MTA system acting as a mailhub. Enter NO otherwise.

Are all internal messages routed to a PMDF-MTA mailhub [N]? **y**

Enter the fully qualified TCP/IP name of the PMDF-MTA system

Enter TCP/IP name of the mailhub []? **naples.example.com**

Part Four: Security Configuration.

Enter YES if you would like to allow external users to submit mail using password and NO if you do not.

Do you want to allow authenticated external users to relay mail [Y]? **y**

Enter YES if you would like to check passwords against LDAP source and NO if you do not.

Do you want to check passwords against LDAP [N]? **n**

Enter YES if you would like to check passwords against MessageStore/popstore user profiles, which is the fastest, and NO if you do not.

Do you want to check passwords against MessageStore/popstore user profiles [Y]? **y**

Enter YES if you would like to check passwords against PMDF password database and NO if you do not.

Do you want to check passwords against PMDF password database [Y]? **y**

Enter YES if you would like to check passwords against the operating system one (e.g. /etc/passwd), and NO if you do not.

Do you want to check passwords against operating system [Y]? **y**

Enter YES if you would like to allow unprotected passwords for internal users and NO if you do not.

Do you want to allow unprotected password for internal users [Y]? **y**

Enter YES if you would like to support for pre-standard unprotected password submission used by Outlook Express and Netscape 4.0x and NO if you do not.

Example 7-1 Cont'd on next page

E-mail Firewall Example Configuration

Example 7-1 (Cont.) Example PMDF-MTA configuration as a firewall

Do you want to support pre-standard password submission used by Outlook Express and Netscape 4.0x [N]? **n**

Part Five: Customizations

If you want to log message traffic through this system, then answer YES. Turning on logging would create log files in your PMDF log directory - mail.log_current, mail.log_yesterday and mail.log. It is your responsibility to archive/delete the mail.log file periodically or these files can consume your disk space.

Do you wish to enable message logging [N]? **n**

As a firewall, you may want to eliminate the names of internal nodes from outgoing mail. PMDF can selectively trim off possible header lines which contain such information. If you choose to trim off the headers, the following will be eliminated from mail outgoing on the external tcp channel:

- Received:
- X400-Received:
- MR-Received:
- Message-id:

Do you wish to get rid of all *received: headers for outgoing mail [Y]? **n**

Part Six: Process and write files

Enter the name of the configuration file you wish to have output. The default action is to produce a real configuration file; you may wish to choose another file name if you are not sure you have properly answered all the questions in the preceding dialogue.

Configuration file to output [/pmdf/table/pmdf.cnf]?

Enter the name of the aliases file you wish to have output. This file contains system-wide local address aliases PMDF will recognize; special aliases are required for proper operation of some channels. The default action is to produce a real alias file; you may wish to choose another file name if you are not sure you have properly answered all the questions in the preceding dialogue, or if you wish to preserve an existing aliases file.

Alias file to output [/pmdf/table/aliases]?

Enter the name of the PMDF option file you wish to have output. The default action is to produce a real PMDF option file; you may wish to choose another file name if you are not sure you have properly answered all the questions in the preceding dialogue.

Option file to output [/pmdf/table/option.dat]?

Example 7-1 Cont'd on next page

E-mail Firewall Example Configuration

Example 7-1 (Cont.) Example PMDF-MTA configuration as a firewall

Enter the name of the mapping file you wish to have output. The default action is to create a real mapping file; you may wish to choose another file name if you are not sure you have properly answered all the questions in the preceding dialogue.

Mapping file to output [/pmdf/table/mappings]?

Enter the name of the security configuration file you wish to have output. The default action is to create a real security.cnf file; you may wish to choose another file name if you are not sure you have properly answered all the questions in the preceding dialogue.

Security configuration file to output [/pmdf/table/security.cnf]?

Enter the name of the option file for the incoming TCP/IP channel. The default action is to create a real channel option file; you may wish to choose another file name if you are not sure you have properly answered all the questions in the preceding dialogue.

(Incoming) tcp channel option file to output [/pmdf/table/tcp_local_option]?

This procedure generates a checklist file that contains the list of steps you must perform in order to complete your PMDF configuration. This procedure does *NOT* perform these steps itself; you must do them manually.

PMDF checklist file name [/pmdf/table/firewall.checklist]?

All configuration questions have been answered.

This question gives you a last chance to change your mind before any files are written. Answer NO if you are not sure you want to generate the configuration you have specified. Answer YES if you do.

Do you wish to generate the configuration files [Y]? **y**

Generating the PMDF configuration file...

Generating /pmdf/table/tcp_local_option

Generating the PMDF mapping file

Generating the PMDF aliases file...

Generating the PMDF option file...

Generating the PMDF security configuration file...

Generating the PMDF firewall configuration checklist file...

Example 7-1 Cont'd on next page

Example 7-1 (Cont.) Example PMDF-MTA configuration as a firewall

```
*****
*
*   To complete your PMDF configuration, carry out the steps
*   detailed in the checklist file /pmdf/table/firewall.checklist.
*
*****

Enter Yes if you want to see the checklist now. You can still type
the file out later if you say No.

Do you want to see the checklist now [Y]? n

Enter YES if you would now like to configure the PMDF Dispatcher.
If you answer NO, then you may configure it later with the command

    # pmdf configure dispatcher

Configure the PMDF Dispatcher [Y]? n
```

Example 7-2 Example checklist file for firewall configuration

```
# cat /pmdf/table/firewall.checklist
Checklist for completing the setup of the PMDF firewall configuration.
Written by root, Oct 15 12:55:48 EST 2012
This file was created by the PMDF configuration generator V6.8

(1) Be sure to configure the PMDF Dispatcher, using the
    command:

        pmdf configure dispatcher

(2) Make sure to perform the remaining post-installation
    tasks as described in the PMDF Installation Guide &
    Release Notes.
```

Index

/pmdf/bin/sendmail
 Replacing sendmail • 1–10
/pmdf/bin/symlink script
 Replacing sendmail startup script • 1–9
/pmdf directory location • 1–6

C

Configuration
 Dispatcher • 3–3
 Firewall
 See Configuration, PMDF-MTA, As firewall
 IMAP server • 4–1
 Mailbox servers • 4–1
 PMDF-MTA • 1–8, 3–1 to 4–4
 As firewall • 6–1
 Example • 7–1
 Example • 5–1 to 5–22
 POP3 server • 4–1
configure utility
 See Utilities, configure
cron
 Scheduling PMDF periodic jobs • 1–9
cronjobs shell script
 Scheduling PMDF periodic jobs • 1–9
crontab
 Scheduling PMDF periodic jobs • 1–9

D

Databases
 Converting After Upgrade • 1–6, 1–7
 Defragment Database • 1–6
 Personal Alias Databases • 1–6
Deinstallation
 Necessary before reinstallation or upgrade • 1–4
 Site-generated files not removed • 1–12
df
 Checking disk space • 1–2
Disk space
 Required for PMDF • 1–2
Dispatcher
 Configuration • 3–3
 Shutdown before upgrade • 1–4
 Starting • 1–7, 1–11
Distribution media
 PMDF • 1–1

Documentation
 Location on CD-ROM • 1–2
 Online
 Accessing • 1–11
 Installation
 Example • 2–1

F

Files
 *.license • 1–4, 1–8
 cronjobs • 1–9
 firewall_configure.history • 6–1
 mail.log
 Firewall system • 6–2
 PMDF-MTA-LINUX.license • 1–4, 1–8
 pmdf_lg_purge shell script • 1–9
 post.sh shell script • 1–9
 return.sh shell script • 1–9
 symlink shell script • 1–9
Firewall
 See PMDF-MTA, Configuration as e-mail firewall

H

HTML documentation for PMDF
 See Documentation, Online
HTTP server
 Configured during Dispatcher configuration • 3–3
 Starting up in standalone mode • 3–2

I

IMAP server
 Configuration • 4–1
 Multithreaded • 1–10
Installation
 PMDF licenses • 1–4 to 1–5, 1–8
 PMDF-MSGSTORE • 1–1 to 1–11
 PMDF-MTA • 1–1 to 1–11
 Example • 2–1
 PMDF online documentation • 1–1 to 1–11
 Example • 2–1

Index

J

Job Controller

- Shutdown before upgrade • 1–4
- Starting • 1–7, 1–11

L

License for PMDF

- Installation • 1–4 to 1–5, 1–8
- Release date • 1–5, 1–8
- Validity period • 1–5

Linux

- Versions supported by PMDF • 1–1

Log files

- periodic jobs • 1–9

M

Mailbox servers

- Configuration • 4–1
- IMAP server
 - Disabling old • 4–1
- POP server
 - Disabling old • 4–1

msgstore

- x-build-user-db • 1–6

O

Official local host name • 3–1

Operating system upgrade

- Effect on PMDF • 1–13

P

Periodic PMDF jobs

- log files • 1–9
- Scheduling with cron • 1–9

PMDF

- Configuration
 - See *specific-product-name*, Configuration
- Configuration as e-mail firewall
 - See PMDF-MTA, Configuration as e-mail firewall

PMDF (cont'd)

- Deinstallation
 - Site-generated files not removed • 1–12
- Directory location • 1–6
- Installation
 - See Installation
- Kit location • 1–2
- Reinstallation
 - Reconfiguration not necessary • 1–12
- pmdf configure
 - See Utilities, configure
- /pmdf directory location • 1–6
- PMDF firewall
 - See PMDF-MTA, Configuration as e-mail firewall
- PMDF license
 - Distribution of • 1–1
 - Release date • 1–5
 - Validity period • 1–5, 1–8
- PMDF-MSGSTORE
 - Installation • 1–1 to 1–11
- PMDF-MTA
 - Configuration • 1–8, 3–1 to 4–4
 - Example • 5–1 to 5–22
 - Configuration as e-mail firewall • 6–1
 - Example • 7–1
 - Installation • 1–1 to 1–11
 - Example • 2–1
- pmdf startup script
 - Replacing sendmail startup script • 1–9
- pmdf user account • 1–2
- pmdfuser user account • 1–2
- pmdf_lg_purge shell script
 - Scheduling execution of • 1–9
- POP3 server
 - Configuration • 4–1
 - Multithreaded • 1–10
- post.sh shell script
 - Scheduling execution of • 1–9
- Privileges
 - Required for PMDF configuration • 3–3, 4–4
 - Required for PMDF deinstallation • 1–12
 - Required for PMDF firewall configuration • 6–3
 - Required for PMDF installation • 1–4

R

Reinstallation

- Reconfiguration not necessary • 1–12
- return.sh shell script
 - Scheduling execution of • 1–9
- rpm
 - Check installed PMDF packages • 1–12
 - Deinstall PMDF package • 1–12

RPM • 1-2, 1-5 to 1-6, 2-1

S

sendmail

 Killing old, pre-PMDf processes • 1-10

 Replacing by /pmdf/bin/sendmail • 1-10

sendmail startup script

 Replacing by pmdf startup script • 1-9

Service Dispatcher

 See Dispatcher

shutdown utility

 Use before upgrading • 1-4

SleepyCat

 Converting To New Format • 1-6, 1-7

 Environment Files • 1-6

startup utility • 1-7, 1-11

symlink script

 Replacing sendmail startup script • 1-9

U

Upgrade

 Operating system

 Effect on PMDF • 1-13

upgrade_all_dbs.sh • 1-6

User accounts for PMDF • 1-2

Utilities

 cnbuild

 After upgrade of PMDF • 1-6

 command-line configuration

 Default values • 5-1

 configure

 access • 4-4

 Default values • 3-1

 dispatcher • 3-3

 firewall • 6-1

 mailbox_servers • 3-4, 4-3, 4-4

 mta • 3-3 to 4-4

 Default values • 3-1, 3-3

 configure

 mailbox_servers • 4-1

 convertdb • 1-6, 1-7

 license -verify • 1-5

 shutdown

 Use before upgrading • 1-4

 startup • 1-7, 1-11

 upgrade_all_dbs.sh • 1-6

 web-based configuration

 Default values • 5-1

 Web-based configuration

Utilities

 Web-based configuration (cont'd)

 Using • 3-2

W

Web-based configure utility

 See Utilities, Web-based configuration

