Sendmail 8.9.3 Release Notes

First Edition

Manufacturing Part Number: <5969-4321>
<E0901>

U.S.A.

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication or disclosure by the U.S. 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 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs, in their present form or with alterations, is expressly

prohibited.

Copyright Notices

Trademark Notices

Contents

Contents

1 New and Changed Features

A new version of sendmail, sendmail 8.9.3, is now available on HP-UX platform as the following patches:

- on HP-UX 10.20 as patch PHNE_18979

- on HP-UX 11.00 as patch PHNE_18546

This version of sendmail includes fixes for the defects found in the sendmail 8.8.6 version and some new features.

The above patches will supersede the sendmail-8.8.6 patch released last year. The delta training document for the same is available in the KMINE database. It is also available at the Internet Services Support Information web page available at the URL:

http://snsltm.cup.hp.com/dir_IntServ/sendmail.txt

New Features

The following are the new features in Sendmail 8.9.3:

Sendmail using LDAP

Sendmail-8.9.3 supports the use of the LDAP protocol for address lookup. The ldapx class (database) is used to lookup items in the ldap directory service.

The syntax of this directive in the sendmail configuration file, sendmail.cf file is as shown:

```
Kldap ldapx -k"uid=%s" -v"mail" -h"ldap_server_name"
-b"o=organization, c=US"
```

Lookups via LDAP are entirely defined by the switches specified. There are four switches that are widely used by most applications. The four switches are:

Table 1-1

Switch	Definition	Description
-b	ldap search base	"Directory" in the ldap "tree" where searching begins.
-h	ldap servers	Space separated string of servers that support ldap at your site.
-k	ldap search string (key)	String that defines how the ldap map takes it's input value and constructs an ldap search.
-v	ldap attribute	The value that replaces the origin string in the map. In most cases this will be the rfc822 email address.

NOTE Any `ldap-style` options must be double-quoted and must follow immediately after the option (i.e. no spaces between the option and the quote).

To lookup a login name in this database and have the official email address for that user returned, you might use a declaration like this:

example: Kldap

```
ldapx -k"uid=%s" -v"mail" -h"test1.india.hp.com"
-b"o=organization, c=US"
```

For the above query to work, you need to comment out the ruleset mentioned below in the sendmail.cf configuration file along with the above `kldap` directive.

```
#LDAP support
#R< > $-       $: < > $(ldap $1 $: $1 $)       Local users only
#R< > $+ $=O $+       $@ $>97 $1 $2 $3       try again
```

If you want the LDAP alias to take precedence over the other system aliases i.e, the `/etc/mail/aliases` or nis alias, the `AliasFile` option must be set with the value "sequence:ldap" as shown:

```
O AliasFile = sequence:ldap, /etc/mail/aliases,
nis:mail.aliases
```

LDAP Support using the sendmail.cf file

The following steps describe how to enable LDAP support using the sendmail-8.8.6 sendmail.cf file:

- Add the following `kldap` directive in the sendmail.cf file in the options section.

  ```
  Kldap ldapx -k"uid=%s" -v"mail" -hldap_server_name
  -b"o=organization, c=US"
  ```

- Add the following LDAP rules in ruleset5 in the sendmail.cf file. These rules have to be added above the rule which has the comment "see if we have a relay or a hub".

  ```
  #LDAP support  ( This is a comment and needs to be
  commented)
  ```

```
#R< > $-      $: < > $(ldap $1 $: $1 $)      Local users only
#R< > $+ $=O $+      $@ $>97 $1 $2 $3        try again
```

Generating the Configuration File

A shell script "gen_cf" is distributed along with the sendmail-8.9.3 patch. When the patch is installed, the script will be installed in the directory /usr/newconfig/etc/mail/cf/cf. This script has to be executed as root and in the /usr/newconfig/etc/mail/cf/cf directory. This script cannot be copied to a different directory and executed as this script will use the macros defined in the /usr/newconfig/etc/mail/cf directory to generate the sendmail.cf file.

This script gives the user several options. Each of these options will turn ON a specific anti-spamming ruleset. The input file for this script will be the *.m4 files defined in the /usr/newconfig/etc/mail/cf directory. An output file of your choice can be specified. Later if there are any site-specific changes, they can be incorporated into the output file generated by this script. This file can be later copied or moved to /etc/mail/sendmail.cf file.

The usage of this script is:

```
$ cd /usr/newconfig/etc/mail/cf/cf
```

```
$ ./gen_cf test.cf
```

The test.cf is the resultant file. This can be later copied into the /etc/mail/sendmail.cf file. This is not a must as the user can start sendmail specifying the sendmail.cf file that is located in /usr/newconfig/etc/mail/cf/cf directory as:

```
/usr/sbin/sendmail -C/usr/newconfig/etc/mail/cf/cf/test.cf
```

The options that can be enabled using this script are:

sendmail.cf with relay ON
sendmail.cf with relay OFF
sendmail.cf with relay_entire_domain
sendmail.cf with relay_based_on_MX
sendmail.cf with relay_hosts_only
sendmail.cf with access_db
sendmail.cf with relay_local_from
sendmail.cf with blacklist_recipients
sendmail.cf with accept_unresolvable_domains
sendmail.cf with accept_unqualified_senders
sendmail.cf with Realtime_Blackhole_list

sendmail.cf with loose_relay_check
sendmail.cf with promiscuous_relay

The sendmail.cf file generated using this script will differ from the default sendmail.cf file provided in the `/usr/newconfig/etc/mail` directory with respect to the check_* rulesets(check_mail, check_relay, check_rcpt) only. All the other options are identical.

New Configuration File Options

Described below are the new configuration file (sendmail.cf) options added in sendmail-8.9.3.

- MaxHeadersLength

  This option will limit the maximum length of a mail header. If the maximum length exceeds the limit, it will send an error message "552 Headers too large #MaxHeadersLength" to the sender of the mail. The default maximum length is 32768.

  This option is set using,

  ```
  O MaxHeadersLength=32768
  ```

  This option is commented out in the default sendmail.cf file.

- MaxRecipientsPerMessage

  This option will limit the number of recipients for a single mail message (a common feature of spam messages) if the recipients of the mail message are having their mailboxes on the same mail server. For example, if users Tom, Dick and Harry have their mailboxes on machine `test` and if the `MaxRecipientsPerMessage` is set to 2 on machine `test` then, if a message is sent to Tom, Dick and Harry then the message will be delivered only to Tom and Dick while it will be discarded for Harry.

  The maximum value for this option is 100. It can be changed depending on your network. After the maximum number is reached, sendmail returns error message "452 Too many recipients" to all RCPT commands. This feature can be used to discourage the use of the mail server for spamming.

  This option is set using,

  ```
  O MaxRecipientsPerMessage=100
  ```

  This option is commented in the default sendmail.cf file.

- DontBlameSendmail

  This option is used to enforce security check on the mode of files on which sendmail operates (reads/writes). For example, by default sendmail will refuse to read most files that are group writable on the grounds that they might have been tampered with by someone other than the owner. It will even refuse to read files in group-writable directories if the above option is set. However, if the user is sure that his configuration is safe and wants sendmail to avoid the security checks, he can do so by unsetting the above option.

  The default value of this option is "safe", wherein sendmail will check modes and permissions of all the files that it operates on. This is hard coded in the binaries. If this value is not reset in the sendmail.cf with any of the values mentioned below even if this option is commented in the sendmail.cf file sendmail will check the modes and permissions of the files it accesses. The values set in the sendmail.cf file take precedence over the default hard coded "safe" value.

  This option is set using:

  ```
  O DontBlameSendmail=option1, option2 ......
  ```

  Listed below are the various values with which the above option can be set. Depending on the option(s) with which the above option is set, Sendmail performs those security checks while avoiding all others.

  The above option can be set with more than one of the values listed below. The values have to be separated with commas as shown below:

  ```
  ODontBlameSendmail=AssumeSafeChown,ClassFileInUnsafeDirPath
  ```

  List of values and their function is listed below.

Table 1-2

Value	Description
`Safe`	Allow the files only in safe directory
`AssumeSafeChown`	Assumes that the "chown" system call is restricted to root.
`ClassFileInUnsafeDirPath`	Allow class file that are in unsafe directories.

Table 1-2

Value	Description
`ErrorHeaderInUnsafeDirPath`	Allow the file named in the ErrorHeader option to be in an unsafe directory.
`GroupWritableDirPathSafe`	Consider group-writable directories to be safe.
`GroupWritableForwardFileSafe`	Accept group-writable.forward files.
`GroupWritableIncludeFile`	Accept group-writable :include: files.
`GroupWritableAliasFile`	Allow group-writable alias files.
`HelpFileinUnsafeDirPath`	Allow Help file to be in unsafe directory.
`WorldWritableAliasFile`	Accept world-writable alias files.
`ForwardFileInGroupWritableDirPath`	Allow .forward files in group writable directories.
`IncludeFileInGroupWritableDirPath`	Allow :include: files in group writable directories.
`ForwardFileInUnsafeDirPath`	Allow .forward files in unsafe directories.
`IncludeFileInUnsafeDirPath`	Allow :include: files in unsafe directories.
`ForwardFileInUnsafeDirPathsafe`	Allow a .forward file that is in an unsafe directory to include references to program and files.

Table 1-2

Value	Description
`IncludeFileInUnsafeDirPathSafe`	Allow a :include: file that is in an unsafe directory to include references to program and files.
`MapInUnsafeDirPath`	Allow maps (e.g., hash, btree, and dbm files) in unsafe directories.
`LinkedAliasFileInWritableDir`	Allow an alias file that is a link in a writable directory.
`LinkedClassFileInWritableDir`	Allow class files that are links in writable directory.
`LinkedForwardFileInWritableDir`	Allow .forward files that are links in writable directory.
`LinkedIncludeFileInWritableDir`	Allow :include: files that are links in writable directories.
`LinkedMapInWritableDir`	Allow map files that are links in writable directories.
`LinkedServiceSwitchFileInWritableDir`	Allow the service switch file to be a link even if the directory is writable.
`FileDeliveryToHardLink`	Allow delivery to files that are hard links.
`FileDeliveryToSymLink`	Allow delivery to files that are symbolic links.
`WriteMapToHardLink`	Allow writes to maps that are hard links.
`WriteMapToSymLink`	Allow writes to maps that are symbolic links.
`WriteStatsToHardLink`	Allow the status file to be a hard link.

Table 1-2

Value	Description
`WriteStatsToSymLink`	Allow the status file to be a symbolic link.
`RunProgramInUnsafeDirPath`	Go ahead and run programs that are in writable directory.
`RunWritableProgram`	Go ahead and run programs that are group or world writable.

- DontProbeInterfaces

  This option will turn OFF the addition of all the interface names into the `$=w` macro on start-up. If users have lots of virtual interfaces, this option will speed up start-up. However, mail messages addressed to those interfaces will bounce.

  This option is set using,

  ```
  O DontProbeInterface
  ```

  This option is commented in the default sendmail.cf file.

- Additional flags to the PrivacyOptions

  Two additional flags have been added to the existing `PrivacyOptions`. The two flags are:

  ```
  O PrivacyOptions=noetrn
  ```

  The `noetrn` flag will disable the `SMTP ETRN` command which forces sendmail to process its queue asynchronously.

  ```
  O  PrivacyOptions=noverb
  ```

  The `noverb` flag will disable the `SMTP VERB` command which causes sendmail to enter the verbose mode and the deliver mode to become interactive.

- QueueSortOrder

  This option exists in the earlier version of sendmail, sendmail 8.8.6. It is not case-sensitive.

- EightBitHeader

This option will allow eight bit header when set to TRUE. This option is mainly used to allow eight bit characters in the header line of a mail message.

This option is set using:

```
O EightBitHeader = TRUE
```

This option is commented in the default sendmail.cf file.

Support for New Mailer Delivery Agent and Map

Sendmail 8.9.3 supports the following:

- Discard

  A special internal delivery agent named `discard` is now defined for use with check_* rulesets and header checking rulesets.

  If a mail address resolves to the `$#discard` mailer then, all the SMTP commands (`MAIL FROM` and `RCPT TO`) will be accepted but the message will be completely discarded. Therefore, if only one of the recipient address resolves to the `$#discard` mailer, all the other recipients will not receive the mail since the entire mail envelope will be discarded.

- Regular Expressions

  Sendmail-8.9.3 supports regular expressions using the new map class `regex`. The `regex` map can be used to see if an address matches a certain regular expression. By using such a map in a check_* ruleset, you can block a certain range of addresses that would otherwise be considered valid.

  For example: If you want to block all senders with all numerics usernames (i.e. 2312343@bigisp.com), you would use Local_check_mail and the new regex map. An example is shown below.

  ```
  LOCAL_CONFIG
  Kallnumbers regex -a@MATCH ^[0-9]+$

  LOCAL_RULESETS

  SLocal_check_mail    # check address against various regex
  checks
  ```

- Class R

$=R macro is used to define the hosts that are allowed to relay. The default file sendmail uses to read the values for the $=R macro is /etc/mail/relay-domains.

It is set in the sendmail.cf file using,

```
FR -o /etc/mail/relay-domains
```

The above line is commented out by default in the default sendmail.cf file provided. The default file from where the $=R macro receives its input is /etc/mail/relay-domains. This can be replaced by a file of user's choice. They will have to edit the sendmail.cf file accordingly.

This file will be a text file. Each line of this file is either an IP address, a domain name or a hostname.

Anti-spam Configuration Control

The primary anti-spam features available in sendmail-8.9.3 are:

- Access database

  Access database is a user-defined file to decide the domains from which the user wants to receive/reject mail messages. The entries in the access db file are either domain names, IP addresses, hosts names or e-mail addresses. The access db file has to be created manually. Every line of the access db file has a key and a value pair.

  — The key can be an IP address, a domain name, a hostname or an e-mail address.

  — The value part of the database can be:

  Table 1-3

Value	Meaning
OK	Accept mail even if other rules in the running ruleset would reject it, for example, if the domain name is unresolvable.
RELAY	Accept mail addressed to the indicated domain or received from the indicated domain for relaying through your SMTP server. RELAY also serves as an implicit OK for the other checks.

Table 1-3

Value	Meaning
REJECT	Reject the sender or recipient with a general purpose message.
DISCARD	Discard the message completely using the $#discard mailer. This only works for sender addresses (i.e., it indicates that you should discard anything received from the indicated domain).
### any text	where ### is an RFC 821 compliant error code and "any text" is a message to return for the command.

To enable the use of this feature use the script "gen_cf" distributed along with the sendmail-8.9.3 patch. The default access db file is /etc/mail/access. This can be replaced by a file of user's choice in the sendmail.cf file.

A sample access db file /etc/mail/access is as shown below:

```
spammer@aol.com        REJECT
192.168.212            DISCARD
cyberspammer.com       550 We don't accept mail from spammers
128.32                 RELAY
okay.cyberspammer.com  OK
```

With the above access db file you would reject all mail messages from spammer@aol.com. You would discard all mail messages from the 192.168.212 domain. You would reject all mail messages from the cyberspammer.com domain with an error message. You will canonical to Relay all those messages originating from the 128.32 domain.You would accept all mail messages from the okay.cyberspammer.com domain.

NOTE

Since /etc/mail/access is a database, after creating the text file, you must use makemap to create the database map. The command to make the database is as shown:

```
makemap dbm /etc/mail/access < /etc/mail/access
```

Refer to makemap(1M) manpage for details on makemap utility.

- Relaying

  Transmission of messages from a site outside your domain to another site outside your domain (relaying) is denied by default when using a sendmail-8.9.3 sendmail.cf file. Previous versions of sendmail allowed relaying by default.

  There are a lot of new features (rulesets) introduced in sendmail-8.9.3 that can revert back to the old behaviour completely or partially. Following are the new features.

  — Promiscuous relay

    Setting this option, will let your site to allow mail relaying. This feature is commented in the default sendmail.cf file. To set this feature you must use the gen_cf script distributed with the sendmail-8.9.3 patch.

    In general, relaying can be more precisely controlled using the access db file and the 'R' class ($=R) macro.

  — Relay entire domain

    Setting this option, will allow any host in your domain as defined by the 'm' class macro ($=m) to relay. By default only hosts listed as RELAY in the access db file will be allowed to relay.

    This feature is commented in the default sendmail.cf file. To enable this features must use the gen_cf script distributed with the sendmail-8.9.3 patch.

  — Relay hosts only

    This feature will change the behaviour of the access_db and class 'R' macro to lookup individual host names only. By default, names that are listed as RELAY in the access db file and class 'R' ($=R) macro are domain names, not host names.

    This feature is commented in the default sendmail.cf file. To enable this feature use the gen_cf script distributed along with the sendmail-8.9.3 patch.

  — Relay local from only

Setting this option, will allow relaying of all those mail messages where the sender of the mail messages is a valid user on that machine. For example, if abc is a valid user on host 1 then, user cbz on host 2 can telnet to host 1 as user abc and then send mail to user xyz on host 3 i.e. host 1 is now relaying.

This should only be used if absolutely necessary as it opens a window for spammers. Specifically, they can send mail to your mail server that claims to be from your domain (either directly or via a routed address), and you can then go ahead and relay it out to arbitrary hosts on the Internet.

This feature is commented in the default sendmail.cf file. To enable this feature use the `gen_cf` script distributed with the sendmail-8.9.3 patch.

— Relay base on MX records

Setting this option, will turn ON the ability to allow relaying based on the MX records of the host portion of an incoming recipient; that is, if an MX record for host foo.com points to your site, you will accept and relay mail addressed to foo.com.

This feature is commented in the default sendmail.cf file. To enable this feature use the `gen_cf` script distributed with the sendmail-8.9.3 patch.

— Loose relay checking

Setting this option, will turn OFF the default behaviour of rechecking all those recipients using % addressing.

For example if the recipient address is user%site@othersite then, the default behaviour without the above feature ON is that Sendmail will check if other site is an allowed relay host specified in either class 'R' macro or access db file. If yes then, the check_rcpt ruleset will strip @othersite and recheck user@site for relaying. This rechecking will not be done if this feature is turned ON. This should not be needed for most installations.

This feature is commented in the default sendmail.cf file. To enable this feature use the `gen_cf` script distributed along with the sendmail-8.9.3 patch.

- Better checking on sender information

  As of version 8.9, sendmail will refuse mail if the MAIL FROM: parameter has an unresolvable domain. If you want to continue to

accept such domains, use the features discussed below.

— Accept unresolvable domains

Setting this option, will allow accepting of all those MAIL FROM: parameters that are not fully qualified i.e, if the host part of the argument to `MAIL FROM:` command cannot be located in the host name service (e.g, DNS).

This feature is commented in the default sendmail.cf file. To enable this feature, use the `gen_cf` script distributed along with the sendmail-8.9.3 patch.

— Accept unqualified senders

Setting this option, will allow accepting of all those MAIL FROM: parameters where the sender's mail address does not include a domain name.

Normally, `MAIL FROM:` commands in the SMTP session will be refused if the connection is a network connection and the sender address does not include a domain name.

This feature is commented in the default sendmail.cf file. To enable this feature, use the `gen_cf` script distributed along with the sendmail-8.9.3 patch.

— Black list recipients

Setting this option, will turn ON the ability to block incoming mail messages destined for certain recipient usernames, hostnames, or addresses. This feature needs the access db file to be included. Enabling this feature will also restrict you from sending mail messages to all those addresses that have an error message or REJECT as value part in the access db file.

For example, if you have the following entry in the access database file:

```
badlocaluser       550 Mailbox disabled for this username

host.mydomain.com  550 That host does not accept mail

user@otherhost.mydomain.com  550 Mailbox disabled for
this recipient
```

This would prevent a recipient of badlocaluser@mydomain.com, any user at host.mydomain.com, and the single address user@otherhost.mydomain.com from receiving mail.

```
spammer@aol.com     REJECT
cyberspammer.com    REJECT
```

Mail can't be sent to spammer@aol.com or anyone at cyberspammer.com.

To enable this feature use the `gen_cf` script distributed along with the sendmail-8.9.3 patch.

— Realtime Blackhole List

Setting this option, will turn ON rejection of hosts found in the Realtime Blackhole List. The default list is maintained on the server rbl.maps.vix.com. To use the default list maintained on the server rbl.maps.vix the below mentioned directive has to be added to the DNS database.

```
1.5.5.192.rbl.maps.vix.com IN A 127.0.0.2
```

You could use a local server by replacing the default server name in the sendmail.cf. Before doing so you need to copy the entire database from the server rbl.maps.vix.com. The data maintained locally has to be updated as and when data on the primary server i.e, rbl.maps.vix.com is updated.

This feature is commented in the default sendmail.cf file. To enable this feature use the `gen_cf` script distributed along with the sendmail-8.9.3 patch.

- Header checks

  New syntax to do limited checking of header syntax is available. A config line of the form: HHeader: $>Ruleset causes the indicated Ruleset to be invoked on the Header when read. This ruleset works like the check_* rulesets -- that is, it can reject mail on the basis of the contents.

  For example:

  Validity of a Message-ID: header

```
#LOCAL_RULESETS
HMessage-Id: $>CheckMessageId

SCheckMessageId

R< $+ @ $+ >    $@ OK

R$*             $#error $: 553 Header Error
```

If the above lines are included in the sendmail.cf file then, all header messages of the form "Message-Id:" will result in the ruleset SCheckMessageID to be called which will check the validity of the Message-Id header.

Turning on this feature will increase the time sendmail takes to deliver a message as sendmail will now perform header checking.It will also check sender and recipient addresses by default (feature of sendmail-8.9.3).

An exhaustive list of the various HHeader format headers are described in the sendmail O'Reilly book.

Other New Features

The following are the additional features introduced in this release of Sendmail:

- Allow multiple -qI, -qR, or -qS queue run limiters.

  example: sendmail -qRfoo -qRbar which would deliver mail to recipients with foo or bar in their address.

- New map flag -"Tx" appends "x" to lookups that return temporary failure. This is similar to "-ax" flag which appends "x" to lookups that return success.

2 Installation Information

Read this chapter before installing Sendmail 8.9.3 on your system.

Compatibility with Previous Versions

Customers currently using any 8.x version of Sendmail do not need to modify their configuration file. It is compatible with this release of Sendmail. However, HP recommends using the Sendmail 8.9.3 configuration file (`/usr/newconfig/etc/mail`) delivered with this release in order to effectively use the new features and changes incorporated in this version. Site-specific changes can be made as required.

Before using the sendmail 8.9.3 sendmail.cf file, consider that by default sendmail 8.9.3 does not relay to provide increased security and prevent spammers from spamming. While sendmail 8.x relays by default. However, many new rulesets have been provided to revert back to the old behaviour completely or partially.

Also, in this version a number of rulesets have been added to check the sender and recipient address. Thus, sendmail-8.9.3 will not accept invalid sender and recipient addresses.

Anti-spamming Rulesets

The anti-spamming rulesets that were provided in sendmail-8.8.6 are not supported in sendmail-8.9.3. The files that were provided to specify the domain, hostanames, IP addresses of the spammers are no longer supported. (`/etc/Mail/Spammer`, `/etc/Mail/SpamDomains`, `/etc/Mail/LocalIP`, `/etc/Mail/LocalNames`, `/etc/Mail/RelayTo`, `/etc/Mail/DeniedIP`, `/etc/Mail/DeniedNames`). This has been replaced by the Access database provided. The default access database being `/etc/mail/access.db`.

A number of rulesets have been added to achieve the same functionality as sendmail-8.8.6. However, there is no one-to-one mapping of the rulesets. Thus it is strongly recommended that customers use the sendmail-8.9.3 sendmail.cf file as it provides more security and many more rulesets to avoid spamming.

To enable some of the new anti-spamming rulesets provided in sendmail-8.9.3, a shell script "`gen_cf`" is distributed along with the patch.

Database Changes

The version of the DB included in this patch is 3.0.55. The file format of the database files has changed considerably when compared to the previous versions. If the customers are using any db files it is required that they re-build all the maps using makemap utility and rebuild all the aliases using newaliases.

System Requirements

The following are the system requirements to install Sendmail 8.9.3:

- Hewlett-Packard 9000 Computer
- HP-UX operating system version 10.20/11.00 as applicable

Installing Sendmail 8.9.3

The following are the Sendmail 8.9.3 patches:

- on HP-UX 10.20 as patch PHNE_18979
- on HP-UX 11.00 as patch PHNE_18546

Install the appropriate patch as per the following steps:

1. Run the following command on the command line.

   `swinstall -s <destination path>`

   Where `<destination path>` is the absolute path where you downloaded the Sendmail 8.9.3 patch to.

   A GUI screen appears.

2. Select the Sendmail 8.9.3 product in the GUI screen.
3. Go to `Action` menu and choose `Install` option.

   Sendmail 8.9.3 is now available for your use.

3 Documentation

The following product documentation is available with Sendmail 8.9.3 release:

Man Pages

The following man pages are distributed with Sendmail 8.9.3 release:

- mailstats.1
- idlookup.1
- mailq.1
- praliases.1
- sendmail.1m
- makemap.1m
- mtail.1m
- newaliases.1m
- killsm.1m
- smrsh.1m
- convert_awk.1m
- identd.1m
- owners.1m
- aliases.5

4 Known Problems and Limitations

This chapter discusses the known problems and limitations in this release of Sendmail.

Known Problems

If LDAP is used for address lookup and if the LDAP lookup fails due to either network or server errors then the mail messages will be queued including those messages addressed to root. This is not acceptable as mail messsages addresssed to root need to be delivered immediately as they could be messages about system panics.

A work-around solution to this problem will be to comment out the "CL" class macro in the sendmail.cf file as follows:

```
CL root
```

By using the above directive only mail messages that are queued up for user "root" will be delivered when there is an LDAP look-up failure. However, if you wish that mail messages addressed to some of the other local users on the server be deliverd too, you can do so by using the "CL" macro. For example:

```
CL root bill
```

Limitations

There are no limitations in Sendmail 8.9.3.