Postfix Basic Configuration

Introduction

Postfix has several hundred configuration parameters that are controlled via the main.cf file. Fortunately, all parameters have sensible default values. In many cases, you need to configure only two or three parameters before you can start to play with the mail system. Here's a quick introduction to the syntax:

- Postfix configuration files

The text below assumes that you already have Postfix installed on the system, either by compiling the source code yourself (as described in the INSTALL file) or by installing an already compiled version.

This document covers basic Postfix configuration. Information about how to configure Postfix for specific applications such as mailhub, firewall or dial-up client can be found in the STANDARD_CONFIGURATION_README file. But don't go there until you already have covered the material presented below.

The first parameters of interest specify the machine's identity and role in the network.

- What domain name to use in outbound mail
- What domains to receive mail for
- What clients to relay mail from
- What destinations to relay mail to
- What delivery method: direct or indirect

The default values for many other configuration parameters are derived from just these.

The next parameter of interest controls the amount of mail sent to the local postmaster:

- What trouble to report to the postmaster

Be sure to set the following correctly if you're behind a proxy or network address translator, and you are running a backup MX host for some other domain:

- Proxy/NAT external network addresses

Postfix daemon processes run in the background, and log problems and normal activity to the syslog daemon. Here are a few things that you need to be aware of:

- What you need to know about Postfix logging

If your machine has unusual security requirements you may want to run Postfix daemon processes inside a chroot environment.

- Running Postfix daemon processes chrooted

If you run Postfix on a virtual network interface, or if your machine runs other mailers on virtual interfaces, you'll have to look at the other parameters listed here as well:

- My own hostname
- My own domain name
- My own network addresses

Postfix configuration files

By default, Postfix configuration files are in /etc/postfix. The two most important files are main.cf and master.cf; these files must be owned by root. Giving someone else write permission to main.cf or master.cf (or to their parent directories) means giving root privileges to that person.

In /etc/postfix/main.cf you will have to set up a minimal number of configuration parameters. Postfix configuration parameters resemble shell variables, with two important differences: the first one is that Postfix does not know about quotes like the UNIX shell does.

You specify a configuration parameter as:

```
/etc/postfix/main.cf:
    parameter = value
```

and you use it by putting a "$" character in front of its name:

```
/etc/postfix/main.cf:
    other_parameter = $parameter
```

You can use $parameter before it is given a value (that is the second main difference with UNIX shell variables). The Postfix configuration language uses lazy evaluation, and does not look at a parameter value until it is needed at runtime.

Postfix uses database files for access control, address rewriting and other purposes. The DATABASE_README file gives an introduction to how Postfix works with Berkeley DB, LDAP or SQL and other types. Here is a common example of how Postfix invokes a database:

```
/etc/postfix/main.cf:
    virtual_alias_maps = hash:/etc/postfix/virtual
```

Whenever you make a change to the main.cf or master.cf file, execute the following command as root in order to refresh a running mail system:

```
# postfix reload
```

What domain name to use in outbound mail

The myorigin parameter specifies the domain that appears in mail that is posted on this machine. The default is to use the local machine name, $myhostname, which defaults to the name of the machine. Unless you are running a really small site, you probably want to change that into $mydomain, which defaults to the parent domain of the machine name.

For the sake of consistency between sender and recipient addresses, myorigin also specifies the domain name that is appended to an unqualified recipient address.

Examples (specify only one of the following):

```
/etc/postfix/main.cf:
    myorigin = $myhostname (default: send mail as "user@$myhostname")
    myorigin = $mydomain   (probably desirable: "user@$mydomain")
```

What domains to receive mail for

The mydestination parameter specifies what domains this machine will deliver locally, instead of forwarding to another machine. The default is to receive mail for the machine itself. See the VIRTUAL_README file for how to configure Postfix for hosted domains.

You can specify zero or more domain names, "/file/name" patterns and/or "type:table" lookup tables (such as hash:, btree:, nis:, ldap:, or mysql:), separated by whitespace and/or commas. A "/file/name" pattern is replaced by its contents; "type:table" requests that a table lookup is done and merely tests for existence: the lookup result is ignored.

IMPORTANT: If your machine is a mail server for its entire domain, you must list $mydomain as well.

Example 1: default setting.

```
/etc/postfix/main.cf:
    mydestination = $myhostname localhost.$mydomain localhost
```

Example 2: domain-wide mail server.

```
/etc/postfix/main.cf:
    mydestination = $myhostname localhost.$mydomain localhost $mydomain
```

Example 3: host with multiple DNS A records.

```
/etc/postfix/main.cf:
    mydestination = $myhostname localhost.$mydomain localhost
        www.$mydomain ftp.$mydomain
```

Caution: in order to avoid mail delivery loops, you must list all hostnames of the machine, including $myhostname, and localhost.$mydomain.

What clients to relay mail from

By default, Postfix will forward mail from clients in authorized network blocks to any destination. Authorized networks are defined with the mynetworks configuration parameter. The current default is to authorize the local machine only. Prior to Postfix 3.0, the default was to authorize all clients in the IP subnetworks that the local machine is attached to.

Postfix can also be configured to relay mail from "mobile" clients that send mail from outside an authorized network block. This is explained in the SASL_README and TLS_README documents.

IMPORTANT: If your machine is connected to a wide area network then your default mynetworks setting may be too friendly.

Examples (specify only one of the following):

```
/etc/postfix/main.cf:
    mynetworks_style = subnet  (default: authorize subnetworks)
    mynetworks_style = host    (safe: authorize local machine only)
    mynetworks = 127.0.0.0/8   (safe: authorize local machine only)
    mynetworks = 127.0.0.0/8 168.100.189.2/32 (authorize local machine)
```

You can specify the trusted networks in the main.cf file, or you can let Postfix do the work for you. The default is to let Postfix do the work. The result depends on the mynetworks_style parameter value.

- Specify "mynetworks_style = host" when Postfix should forward mail from only the local machine.
- Specify "mynetworks_style = subnet" (the default) when Postfix should forward mail from SMTP clients in the same IP subnetworks as the local machine. On Linux, this works correctly only with

interfaces specified with the "ifconfig" command.

- Specify "mynetworks_style = class" when Postfix should forward mail from SMTP clients in the same IP class A/B/C networks as the local machine. Don't do this with a dialup site - it would cause Postfix to "trust" your entire provider's network. Instead, specify an explicit mynetworks list by hand, as described below.

Alternatively, you can specify the mynetworks list by hand, in which case Postfix ignores the mynetworks_style setting. To specify the list of trusted networks by hand, specify network blocks in CIDR (network/mask) notation, for example:

```
/etc/postfix/main.cf:
    mynetworks = 168.100.189.0/28, 127.0.0.0/8
```

You can also specify the absolute pathname of a pattern file instead of listing the patterns in the main.cf file.

What destinations to relay mail to

By default, Postfix will forward mail from strangers (clients outside authorized networks) to authorized remote destinations only. Authorized remote destinations are defined with the relay_domains configuration parameter. The default is to authorize all domains (and subdomains) of the domains listed with the mydestination parameter.

Examples (specify only one of the following):

```
/etc/postfix/main.cf:
    relay_domains = $mydestination (default)
    relay_domains =           (safe: never forward mail from strangers)
    relay_domains = $mydomain (forward mail to my domain and subdomains)
```

What delivery method: direct or indirect

By default, Postfix tries to deliver mail directly to the Internet. Depending on your local conditions this may not be possible or desirable. For example, your system may be turned off outside office hours, it may be behind a firewall, or it may be connected via a provider who does not allow direct mail to the Internet. In those cases you need to configure Postfix to deliver mail indirectly via a relay host.

Examples (specify only one of the following):

```
/etc/postfix/main.cf:
    relayhost =                 (default: direct delivery to Internet)
    relayhost = $mydomain       (deliver via local mailhub)
    relayhost = [mail.$mydomain] (deliver via local mailhub)
    relayhost = [mail.isp.tld]  (deliver via provider mailhub)
```

The form enclosed with [] eliminates DNS MX lookups. Don't worry if you don't know what that means. Just be sure to specify the [] around the mailhub hostname that your ISP gave to you, otherwise mail may be mis-delivered.

The STANDARD_CONFIGURATION_README file has more hints and tips for firewalled and/or dial-up networks.

What trouble to report to the postmaster

You should set up a postmaster alias in the aliases(5) table that directs mail to a human person. The postmaster address is required to exist, so that people can report mail delivery problems. While you're updating the aliases(5) table, be sure to direct mail for the super-user to a human person too.

```
/etc/aliases:
    postmaster: you
    root: you
```

Execute the command "newaliases" after changing the aliases file. Instead of /etc/aliases, your alias file may be located elsewhere. Use the command "postconf alias_maps" to find out.

The Postfix system reports problems to the postmaster alias. You may not be interested in all types of trouble reports, so this reporting mechanism is configurable. The default is to report only serious problems (resource, software) to postmaster:

Default setting:

```
/etc/postfix/main.cf:
    notify_classes = resource, software
```

The meaning of the classes is as follows:

bounce
: Inform the postmaster of undeliverable mail. Either send the postmaster a copy of undeliverable mail that is returned to the sender, or send a transcript of the SMTP session when Postfix rejected mail. For privacy reasons, the postmaster copy of undeliverable mail is truncated after the original message headers. This implies "2bounce" (see below). See also the luser_relay feature. The notification is sent to the address specified with the bounce_notice_recipient configuration parameter (default: postmaster).

2bounce
: When Postfix is unable to return undeliverable mail to the sender, send it to the postmaster instead (without truncating the message after the primary headers). The notification is sent to the address specified with the 2bounce_notice_recipient configuration parameter (default: postmaster).

delay
: Inform the postmaster of delayed mail. In this case, the postmaster receives message headers only. The notification is sent to the address specified with the delay_notice_recipient configuration parameter (default: postmaster).

policy
: Inform the postmaster of client requests that were rejected because of (UCE) policy restrictions. The postmaster receives a transcript of the SMTP session. The notification is sent to the address specified with the error_notice_recipient configuration parameter (default: postmaster).

protocol
: Inform the postmaster of protocol errors (client or server side) or attempts by a client to execute unimplemented commands. The postmaster receives a transcript of the SMTP session. The notification is sent to the address specified with the error_notice_recipient configuration parameter (default: postmaster).

resource
: Inform the postmaster of mail not delivered due to resource problems (for example, queue file write errors). The notification is sent to the address specified with the error_notice_recipient configuration parameter (default: postmaster).

software
: Inform the postmaster of mail not delivered due to software problems. The notification is sent to the address specified with the error_notice_recipient configuration parameter (default: postmaster).

Proxy/NAT external network addresses

Some mail servers are connected to the Internet via a network address translator (NAT) or proxy. This means that systems on the Internet connect to the address of the NAT or proxy, instead of connecting to the network

address of the mail server. The NAT or proxy forwards the connection to the network address of the mail server, but Postfix does not know this.

If you run a Postfix server behind a proxy or NAT, you need to configure the proxy_interfaces parameter and specify all the external proxy or NAT addresses that Postfix receives mail on. You may specify symbolic hostnames instead of network addresses.

IMPORTANT: You must specify your proxy/NAT external addresses when your system is a backup MX host for other domains, otherwise mail delivery loops will happen when the primary MX host is down.

Example: host behind NAT box running a backup MX host.

```
/etc/postfix/main.cf:
    proxy_interfaces = 1.2.3.4 (the proxy/NAT external network address)
```

What you need to know about Postfix logging

Postfix daemon processes run in the background, and log problems and normal activity to the syslog daemon. The syslogd process sorts events by class and severity, and appends them to logfiles. The logging classes, levels and logfile names are usually specified in /etc/syslog.conf. At the very least you need something like:

```
/etc/syslog.conf:
    mail.err                                    /dev/console
    mail.debug                                  /var/log/maillog
```

After changing the syslog.conf file, send a "HUP" signal to the syslogd process.

IMPORTANT: many syslogd implementations will not create files. You must create files before (re)starting syslogd.

IMPORTANT: on Linux you need to put a "-" character before the pathname, e.g., -/var/log/maillog, otherwise the syslogd process will use more system resources than Postfix.

Hopefully, the number of problems will be small, but it is a good idea to run every night before the syslog files are rotated:

```
# postfix check
# egrep '(reject|warning|error|fatal|panic):' /some/log/file
```

- The first line (postfix check) causes Postfix to report file permission/ownership discrepancies.
- The second line looks for problem reports from the mail software, and reports how effective the relay and junk mail access blocks are. This may produce a lot of output. You will want to apply some postprocessing to eliminate uninteresting information.

The DEBUG_README document describes the meaning of the "warning" etc. labels in Postfix logging.

Running Postfix daemon processes chrooted

Postfix daemon processes can be configured (via the master.cf file) to run in a chroot jail. The processes run at a fixed low privilege and with file system access limited to the Postfix queue directories (/var/spool/postfix). This provides a significant barrier against intrusion. The barrier is not impenetrable (chroot limits file system access only), but every little bit helps.

With the exception of Postfix daemons that deliver mail locally and/or that execute non-Postfix commands, every Postfix daemon can run chrooted.

Sites with high security requirements should consider to chroot all daemons that talk to the network: the smtp(8) and smtpd(8) processes, and perhaps also the lmtp(8) client. The author's own porcupine.org mail server runs all daemons chrooted that can be chrooted.

The default /etc/postfix/master.cf file specifies that no Postfix daemon runs chrooted. In order to enable chroot operation, edit the file /etc/postfix/master.cf, and follow instructions in the file. When you're finished, execute "postfix reload" to make the change effective.

Note that a chrooted daemon resolves all filenames relative to the Postfix queue directory (/var/spool/postfix). For successful use of a chroot jail, most UNIX systems require you to bring in some files or device nodes. The examples/chroot-setup directory in the source code distribution has a collection of scripts that help you set up Postfix chroot environments on different operating systems.

Additionally, you almost certainly need to configure syslogd so that it listens on a socket inside the Postfix queue directory. Examples of syslogd command line options that achieve this for specific systems:

FreeBSD: `syslogd -l /var/spool/postfix/var/run/log`

Linux, OpenBSD: `syslogd -a /var/spool/postfix/dev/log`

My own hostname

The myhostname parameter specifies the fully-qualified domain name of the machine running the Postfix system. $myhostname appears as the default value in many other Postfix configuration parameters.

By default, myhostname is set to the local machine name. If your local machine name is not in fully-qualified domain name form, or if you run Postfix on a virtual interface, you will have to specify the fully-qualified domain name that the mail system should use.

Alternatively, if you specify mydomain in main.cf, then Postfix will use its value to generate a fully-qualified default value for the myhostname parameter.

Examples (specify only one of the following):

```
/etc/postfix/main.cf:
    myhostname = host.local.domain (machine name is not FQDN)
    myhostname = host.virtual.domain (virtual interface)
    myhostname = virtual.domain (virtual interface)
```

My own domain name

The mydomain parameter specifies the parent domain of $myhostname. By default, it is derived from $myhostname by stripping off the first part (unless the result would be a top-level domain).

Conversely, if you specify mydomain in main.cf, then Postfix will use its value to generate a fully-qualified default value for the myhostname parameter.

Examples (specify only one of the following):

```
/etc/postfix/main.cf:
    mydomain = local.domain
    mydomain = virtual.domain (virtual interface)
```

My own network addresses

The inet_interfaces parameter specifies all network interface addresses that the Postfix system should listen on; mail addressed to "user@[network address]" will be delivered locally, as if it is addressed to a domain listed in $mydestination.

You can override the inet_interfaces setting in the Postfix master.cf file by prepending an IP address to a server name.

The default is to listen on all active interfaces. If you run mailers on virtual interfaces, you will have to specify what interfaces to listen on.

IMPORTANT: If you run MTAs on virtual interfaces you must specify explicit inet_interfaces values for the MTA that receives mail for the machine itself: this MTA should never listen on the virtual interfaces or you would have a mailer loop when a virtual MTA is down.

Example: default setting.

```
/etc/postfix/main.cf:
    inet_interfaces = all
```

Example: host running one or more virtual mailers. For each Postfix instance, specify only one of the following.

```
/etc/postfix/main.cf:
    inet_interfaces = virtual.host.tld         (virtual Postfix)
    inet_interfaces = $myhostname localhost... (non-virtual Postfix)
```

Note: you need to stop and start Postfix after changing this parameter.