Postfix Standard Configuration Examples

Purpose of this document

This document presents a number of typical Postfix configurations. This document should be reviewed after you have followed the basic configuration steps as described in the BASIC_CONFIGURATION_README[1] document. In particular, do not proceed here if you don't already have Postfix working for local mail submission and for local mail delivery.

The first part of this document presents standard configurations that each solve one specific problem.

The second part of this document presents additional configurations for hosts in specific environments.

Postfix on a stand-alone Internet host

Postfix should work out of the box without change on a stand-alone machine that has direct Internet access. At least, that is how Postfix installs when you download the Postfix source code via http://www.postfix.org/[2].

You can use the command "**postconf -n**" to find out what settings are overruled by your main.cf[3]. Besides a few pathname settings, few parameters should be set on a stand-alone box, beyond what is covered in the BASIC_CONFIGURATION_README[4] document:

```
/etc/postfix/main.cf[5]:
    # Optional: send mail as user@domainname instead of user@hostname.
    #myorigin = $mydomain

    # Optional: specify NAT/proxy external address.
    #proxy_interfaces = 1.2.3.4

    # Alternative 1: don't relay mail from other hosts.
    mynetworks_style = host
    relay_domains =

    # Alternative 2: relay mail from local clients only.
    # mynetworks = 192.168.1.0/28
    # relay_domains =
```

See also the section "Postfix on hosts without a real Internet hostname" if this is applicable to your configuration.

Postfix on a null client

A null client is a machine that can only send mail. It receives no mail from the network, and it does not deliver any mail locally. A null client typically uses POP, IMAP or NFS for mailbox access.

In this example we assume that the Internet domain name is "example.com" and that the machine is named "hostname.example.com". As usual, the examples show only parameters that are not left at their default settings.

```
/etc/postfix/main.cf[6]:
    myhostname = hostname.example.com
    myorigin = $mydomain
    relayhost = $mydomain
    inet_interfaces = loopback-only
    mydestination =
```

Translation:

- Line 2: Set myhostname to hostname.example.com, in case the machine name isn't set to a fully-qualified domain name (use the command "postconf -d myhostname" to find out what the machine name is).
- Line 2: The myhostname value also provides the default value for the mydomain parameter (here, "mydomain = example.com").
- Line 3: Send mail as "user@example.com" (instead of "user@hostname.example.com"), so that nothing ever has a reason to send mail to "user@hostname.example.com".
- Line 4: Forward all mail to the mail server that is responsible for the "example.com" domain. This prevents mail from getting stuck on the null client if it is turned off while some remote destination is unreachable. Specify a real hostname here if your "example.com" domain has no MX record.
- Line 5: Do not accept mail from the network.
- Line 6: Disable local mail delivery. All mail goes to the mail server as specified in line 4.

Postfix on a local network

This section describes a local area network environment of one main server and multiple other systems that send and receive email. As usual we assume that the Internet domain name is "example.com". All systems are configured to send mail as "user@example.com", and all systems receive mail for "user@hostname.example.com". The main server also receives mail for "user@example.com". We call this machine by the name of mailhost.example.com.

A drawback of sending mail as "user@example.com" is that mail for "root" and other system accounts is also sent to the central mailhost. See the section "Delivering some but not all accounts locally" below for possible solutions.

As usual, the examples show only parameters that are not left at their default settings.

First we present the non-mailhost configuration, because it is the simpler one. This machine sends mail as "user@example.com" and is final destination for "user@hostname.example.com".

```
 1 /etc/postfix/main.cf[7]:
 2     myorigin = $mydomain
 3     mynetworks = 127.0.0.0/8 10.0.0.0/24
 4     relay_domains =
 5     # Optional: forward all non-local mail to mailhost
 6     #relayhost = $mydomain
```

Translation:

- Line 2: Send mail as "user@example.com".
- Line 3: Specify the trusted networks.
- Line 4: This host does not relay mail from untrusted networks.
- Line 6: This is needed if no direct Internet access is available. See also below, "Postfix behind a firewall".

Next we present the mailhost configuration. This machine sends mail as "user@example.com" and is final destination for "user@hostname.example.com" as well as "user@example.com".

```
 1 DNS:
 2     example.com    IN    MX  10 mailhost.example.com.
 3
 4 /etc/postfix/main.cf[8]:
 5     myorigin = $mydomain
 6     mydestination = $myhostname localhost.$mydomain localhost $mydomain
 7     mynetworks = 127.0.0.0/8 10.0.0.0/24
 8     relay_domains =
 9     # Optional: forward all non-local mail to firewall
10     #relayhost = [firewall.example.com]
```

Translation:

- Line 2: Send mail for the domain "example.com" to the machine mailhost.example.com. Remember to specify the "." at the end of the line.
- Line 5: Send mail as "user@example.com".
- Line 6: This host is the final mail destination for the "example.com" domain, in addition to the names of the machine itself.
- Line 7: Specify the trusted networks.
- Line 8: This host does not relay mail from untrusted networks.

- Line 10: This is needed only when the mailhost has to forward non-local mail via a mail server on a firewall. The [] forces Postfix to do no MX record lookups.

In an environment like this, users access their mailbox in one or more of the following ways:

- Mailbox access via NFS or equivalent.
- Mailbox access via POP or IMAP.
- Mailbox on the user's preferred machine.

In the latter case, each user has an alias on the mailhost that forwards mail to her preferred machine:

```
/etc/aliases:
    joe:    joe@joes.preferred.machine
    jane:   jane@janes.preferred.machine
```

On some systems the alias database is not in /etc/aliases. To find out the location for your system, execute the command "**postconf alias_maps**".

Execute the command "**newaliases**" whenever you change the aliases file.

Postfix email firewall/gateway

The idea is to set up a Postfix email firewall/gateway that forwards mail for "example.com" to an inside gateway machine but rejects mail for "anything.example.com". There is only one problem: with "relay_domains = example.com", the firewall normally also accepts mail for "anything.example.com". That would not be right.

Note: this example requires Postfix version 2.0 and later. To find out what Postfix version you have, execute the command "**postconf mail_version**".

The solution is presented in multiple parts. This first part gets rid of local mail delivery on the firewall, making the firewall harder to break.

```
1 /etc/postfix/main.cf[9]:
```

```
2     myorigin = example.com
3     mydestination =
4     local_recipient_maps =
5     local_transport = error[10]:local mail delivery is disabled
6
7 /etc/postfix/master.cf[11]:
8     Comment out the local delivery agent
```

Translation:

- Line 2: Send mail from this machine as "user@example.com", so that no reason exists to send mail to "user@firewall.example.com".
- Lines 3-8: Disable local mail delivery on the firewall machine.

For the sake of technical correctness the firewall must be able to receive mail for postmaster@[firewall ip address]. Reportedly, some things actually expect this ability to exist. The second part of the solution therefore adds support for postmaster@[firewall ip address], and as a bonus we do abuse@[firewall ip address] as well. All the mail to these two accounts is forwarded to an inside address.

```
/etc/postfix/main.cf[12]:
    virtual_alias_maps = hash:/etc/postfix/virtual

/etc/postfix/virtual:
    postmaster      postmaster@example.com
    abuse           abuse@example.com
```

Translation:

- Because mydestination is empty (see the previous example), only address literals matching $inet_interfaces or $proxy_interfaces are deemed local. So "localpart@[a.d.d.r]" can be matched as simply "localpart" in canonical(5)[13] and virtual(5)[14]. This avoids the need to specify firewall IP addresses into Postfix configuration files.

The last part of the solution does the email forwarding, which is the real purpose of the firewall email function.

```
1 /etc/postfix/main.cf[15]:
2     mynetworks = 127.0.0.0/8 12.34.56.0/24
3     relay_domains = example.com
4     parent_domain_matches_subdomains =
5         debug_peer_list smtpd_access_maps


6a    # Postfix 2.10 and later support separate relay control and
7a    # spam control.
8a    smtpd_relay_restrictions =
9a        permit_mynetworks reject_unauth_destination
10a   smtpd_recipient_restrictions = ...spam blocking rules....


6b    # Older configurations combine relay control and spam control. To
7b    # use this with Postfix ≥ 2.10 specify "smtpd_relay_restrictions=".
8b    smtpd_recipient_restrictions =
9b        permit_mynetworks reject_unauth_destination
10b       ...spam blocking rules....


11    relay_recipient_maps = hash:/etc/postfix/relay_recipients
12    transport_maps = hash:/etc/postfix/transport
13
14 /etc/postfix/relay_recipients:
15    user1@example.com   x
16    user2@example.com   x
17     . . .
18
19 /etc/postfix/transport:
20    example.com   smtp[16]:[inside-gateway.example.com]
```

Translation:

- Lines 1-10: Accept mail from local systems in $mynetworks, and accept mail from outside for "user@example.com" but not for "user@anything.example.com". The magic is in lines 4-5.
- Lines 11, 13-16: Define the list of valid addresses in the "example.com" domain that can receive mail from the Internet. This prevents the mail queue from filling up with

undeliverable MAILER-DAEMON messages. If you can't maintain a list of valid recipients then you must specify "relay_recipient_maps =" (that is, an empty value), or you must specify an "@example.com x" wild-card in the relay_recipients table.

- Lines 12, 19-20: Route mail for "example.com" to the inside gateway machine. The [] forces Postfix to do no MX lookup.

Specify **dbm** instead of **hash** if your system uses **dbm** files instead of **db** files. To find out what lookup tables Postfix supports, use the command "**postconf -m**".

Execute the command "**postmap /etc/postfix/relay_recipients**" whenever you change the relay_recipients table.

Execute the command "**postmap /etc/postfix/transport**" whenever you change the transport table.

In some installations, there may be separate instances of Postfix processing inbound and outbound mail on a multi-homed firewall. The inbound Postfix instance has an SMTP server listening on the external firewall interface, and the outbound Postfix instance has an SMTP server listening on the internal interface. In such a configuration is it is tempting to configure $inet_interfaces in each instance with just the corresponding interface address.

In most cases, using inet_interfaces in this way will not work, because as documented in the $inet_interfaces reference manual, the smtp(8)[17] delivery agent will also use the specified interface address as the source address for outbound connections and will be unable to reach hosts on "the other side" of the firewall. The symptoms are that the firewall is unable to connect to hosts that are in fact up. See the inet_interfaces parameter documentation for suggested work-arounds.

Delivering some but not all accounts locally

A drawback of sending mail as "user@example.com" (instead of "user@hostname.example.com") is that mail for "root" and other system accounts is also sent to the central mailhost. In order to deliver such accounts locally, you can set up virtual aliases as follows:

```
1 /etc/postfix/main.cf[18]:
2     virtual_alias_maps = hash:/etc/postfix/virtual
3 
4 /etc/postfix/virtual:
5     root     root@localhost
6     . . .
```

Translation:

- Line 5: As described in the virtual(5)[19] manual page, the bare name "root" matches "root@site" when "site" is equal to $myorigin, when "site" is listed in $mydestination, or when it matches $inet_interfaces or $proxy_interfaces.

Execute the command "**postmap /etc/postfix/virtual**" after editing the file.

Running Postfix behind a firewall

The simplest way to set up Postfix on a host behind a firewalled network is to send all mail to a gateway host, and to let that mail host take care of internal and external forwarding. Examples of that are shown in the local area network section above. A more sophisticated approach is to send only external mail to the gateway host, and to send intranet mail directly.

Note: this example requires Postfix version 2.0 and later. To find out what Postfix version you have, execute the command "**postconf mail_version**".

The following example presents additional configuration. You need to combine this with basic configuration information as discussed the first half of this document.

```
/etc/postfix/main.cf[20]:
    transport_maps = hash:/etc/postfix/transport
    relayhost =
    # Optional for a machine that isn't "always on"
    #fallback_relay = [gateway.example.com]

/etc/postfix/transport:
    # Internal delivery.
```

```
 9     example.com      :
10     .example.com     :
11     # External delivery.
12     *                smtp[21]:[gateway.example.com]
```

Translation:

- Lines 2, 7-12: Request that intranet mail is delivered directly, and that external mail is given to a gateway. Obviously, this example assumes that the organization uses DNS MX records internally. The [] forces Postfix to do no MX lookup.
- Line 3: IMPORTANT: do not specify a relayhost in main.cf[22].
- Line 5: This prevents mail from being stuck in the queue when the machine is turned off. Postfix tries to deliver mail directly, and gives undeliverable mail to a gateway.

Specify **dbm** instead of **hash** if your system uses **dbm** files instead of **db** files. To find out what lookup tables Postfix supports, use the command "**postconf -m**".

Execute the command "**postmap /etc/postfix/transport**" whenever you edit the transport table.

Configuring Postfix as primary or backup MX host for a remote site

This section presents additional configuration. You need to combine this with basic configuration information as discussed the first half of this document.

When your system is SECONDARY MX host for a remote site this is all you need:

```
1 DNS:
2     the.backed-up.domain.tld        IN      MX 100 your.machine.tld.
3
4 /etc/postfix/main.cf[23]:
5     relay_domains = . . . the.backed-up.domain.tld



6a    # Postfix 2.10 and later support separate relay control and
```

```
 7a    # spam control.
 8a    smtpd_relay_restrictions =
 9a        permit_mynetworks reject_unauth_destination
10a    smtpd_recipient_restrictions = ...spam blocking rules....



 6b    # Older configurations combine relay control and spam control. To
 7b    # use this with Postfix ≥ 2.10 specify "smtpd_relay_restrictions=".
 8b    smtpd_recipient_restrictions =
 9b        permit_mynetworks reject_unauth_destination
10b        ...spam blocking rules....



11     # You must specify your NAT/proxy external address.
12     #proxy_interfaces = 1.2.3.4
13
14     relay_recipient_maps = hash:/etc/postfix/relay_recipients
15
16 /etc/postfix/relay_recipients:
17     user1@the.backed-up.domain.tld   x
18     user2@the.backed-up.domain.tld   x
19      . . .
```

When your system is PRIMARY MX host for a remote site you need the above, plus:

```
20 /etc/postfix/main.cf[24]:
21     transport_maps = hash:/etc/postfix/transport
22
23 /etc/postfix/transport:
24     the.backed-up.domain.tld       relay:[their.mail.host.tld]
```

Important notes:

- Do not list the.backed-up.domain.tld in mydestination.
- Do not list the.backed-up.domain.tld in virtual_alias_domains.
- Do not list the.backed-up.domain.tld in virtual_mailbox_domains.
- Lines 1-9: Forward mail from the Internet for "the.backed-up.domain.tld" to the primary MX host for that domain.
- Line 12: This is a must if Postfix receives mail via a NAT relay or proxy that presents

a different IP address to the world than the local machine.

- Lines 14-18: Define the list of valid addresses in the "the.backed-up.domain.tld" domain. This prevents your mail queue from filling up with undeliverable MAILER-DAEMON messages. If you can't maintain a list of valid recipients then you must specify "relay_recipient_maps =" (that is, an empty value), or you must specify an "@the.backed-up.domain.tld x" wild-card in the relay_recipients table.
- Line 24: The [] forces Postfix to do no MX lookup.

Specify **dbm** instead of **hash** if your system uses **dbm** files instead of **db** files. To find out what lookup tables Postfix supports, use the command "**postconf -m**".

Execute the command "**postmap /etc/postfix/transport**" whenever you change the transport table.

NOTE for Postfix < 2.2: Do not use the fallback_relay feature when relaying mail for a backup or primary MX domain. Mail would loop between the Postfix MX host and the fallback_relay host when the final destination is unavailable.

- In main.cf[25] specify "relay_transport = relay",
- In master.cf[26] specify "-o fallback_relay =" at the end of the relay entry.
- In transport maps, specify "relay:*nexthop...*" as the right-hand side for backup or primary MX domain entries.

These are default settings in Postfix version 2.2 and later.

Postfix on a dialup machine

This section applies to dialup connections that are down most of the time. For dialup connections that are up 24x7, see the local area network section above.

This section presents additional configuration. You need to combine this with basic configuration information as discussed the first half of this document.

If you do not have your own hostname and IP address (usually with dialup, cable TV or DSL connections) then you should also study the section on "Postfix on hosts without a real Internet hostname".

- Route all outgoing mail to your network provider.
  If your machine is disconnected most of the time, there isn't a lot of opportunity for Postfix to deliver mail to hard-to-reach corners of the Internet. It's better to give the mail to a machine that is connected all the time. In the example below, the [] prevents Postfix from trying to look up DNS MX records.

  ```
  /etc/postfix/main.cf[27]:
      relayhost = [smtprelay.someprovider.com]
  ```
- Disable spontaneous SMTP mail delivery (if using on-demand dialup IP only).

  Normally, Postfix attempts to deliver outbound mail at its convenience. If your machine uses on-demand dialup IP, this causes your system to place a telephone call whenever you submit new mail, and whenever Postfix retries to deliver delayed mail. To prevent such telephone calls from being placed, disable spontaneous SMTP mail deliveries.

  ```
  /etc/postfix/main.cf[28]:
      defer_transports = smtp (Only for on-demand dialup IP hosts)
  ```
- Disable SMTP client DNS lookups (dialup LAN only).

  ```
  /etc/postfix/main.cf[29]:
      disable_dns_lookups = yes (Only for on-demand dialup IP hosts)
  ```
- Flush the mail queue whenever the Internet link is established.
  Put the following command into your PPP or SLIP dialup scripts:

  ```
  /usr/sbin/sendmail -q (whenever the Internet link is up)
  ```
  The exact location of the Postfix sendmail command is system-specific. Use the command "**postconf sendmail_path**" to find out where the Postfix sendmail command is located on your machine.

  In order to find out if the mail queue is flushed, use something like:

  ```
  #!/bin/sh

  # Start mail deliveries.
  /usr/sbin/sendmail -q
  ```

```
# Allow deliveries to start.
sleep 10

# Loop until all messages have been tried at least once.
while mailq | grep '^[^ ]*\*' >/dev/null
do
    sleep 10
done
```

If you have disabled spontaneous SMTP mail delivery, you also need to run the "**sendmail -q**" command every now and then while the dialup link is up, so that newly-posted mail is flushed from the queue.

Postfix on hosts without a real Internet hostname

This section is for hosts that don't have their own Internet hostname. Typically these are systems that get a dynamic IP address via DHCP or via dialup. Postfix will let you send and receive mail just fine between accounts on a machine with a fantasy name. However, you cannot use a fantasy hostname in your email address when sending mail into the Internet, because no-one would be able to reply to your mail. In fact, more and more sites refuse mail addresses with non-existent domain names.

Note: the following information is Postfix version dependent. To find out what Postfix version you have, execute the command "**postconf mail_version**".

Solution 1: Postfix version 2.2 and later

Postfix 2.2 uses the generic(5)[30] address mapping to replace local fantasy email addresses by valid Internet addresses. This mapping happens ONLY when mail leaves the machine; not when you send mail between users on the same machine.

The following example presents additional configuration. You need to combine this with basic configuration information as discussed the first half of this document.

```
/etc/postfix/main.cf[31]:
    smtp_generic_maps = hash:/etc/postfix/generic

```

```
4 /etc/postfix/generic:
5     his@localdomain.local             hisaccount@hisisp.example
6     her@localdomain.local             heraccount@herisp.example
7     @localdomain.local                hisaccount+local@hisisp.example
```

When mail is sent to a remote host via SMTP:

- Line 5 replaces *his@localdomain.local* by his ISP mail address,
- Line 6 replaces *her@localdomain.local* by her ISP mail address, and
- Line 7 replaces other local addresses by his ISP account, with an address extension of +*local* (this example assumes that the ISP supports "+" style address extensions).

Specify **dbm** instead of **hash** if your system uses **dbm** files instead of **db** files. To find out what lookup tables Postfix supports, use the command "**postconf -m**".

Execute the command "**postmap /etc/postfix/generic**" whenever you change the generic table.

Solution 2: Postfix version 2.1 and earlier

The solution with older Postfix systems is to use valid Internet addresses where possible, and to let Postfix map valid Internet addresses to local fantasy addresses. With this, you can send mail to the Internet and to local fantasy addresses, including mail to local fantasy addresses that don't have a valid Internet address of their own.

The following example presents additional configuration. You need to combine this with basic configuration information as discussed the first half of this document.

```
/etc/postfix/main.cf[32]:
    myhostname = hostname.localdomain
    mydomain = localdomain

    canonical_maps = hash:/etc/postfix/canonical

    virtual_alias_maps = hash:/etc/postfix/virtual

/etc/postfix/canonical:
    your-login-name    your-account@your-isp.com
```

```
11
12 /etc/postfix/virtual:
13     your-account@your-isp.com       your-login-name
```

Translation:

- Lines 2-3: Substitute your fantasy hostname here. Do not use a domain name that is already in use by real organizations on the Internet. See RFC 2606[33] for examples of domain names that are guaranteed not to be owned by anyone.
- Lines 5, 9, 10: This provides the mapping from "your-login-name@hostname.localdomain" to "your-account@your-isp.com". This part is required.
- Lines 7, 12, 13: Deliver mail for "your-account@your-isp.com" locally, instead of sending it to the ISP. This part is not required but is convenient.

Specify **dbm** instead of **hash** if your system uses **dbm** files instead of **db** files. To find out what lookup tables Postfix supports, use the command "**postconf -m**".

Execute the command "**postmap /etc/postfix/canonical**" whenever you change the canonical table.

Execute the command "**postmap /etc/postfix/virtual**" whenever you change the virtual table.

1. http://www.postfix.org/BASIC_CONFIGURATION_README.html
2. http://www.postfix.org/
3. http://www.postfix.org/postconf.5.html
4. http://www.postfix.org/BASIC_CONFIGURATION_README.html
5. http://www.postfix.org/postconf.5.html
6. http://www.postfix.org/postconf.5.html
7. http://www.postfix.org/postconf.5.html
8. http://www.postfix.org/postconf.5.html
9. http://www.postfix.org/postconf.5.html
10. http://www.postfix.org/error.8.html
11. http://www.postfix.org/master.5.html

12. http://www.postfix.org/postconf.5.html
13. http://www.postfix.org/canonical.5.html
14. http://www.postfix.org/virtual.5.html
15. http://www.postfix.org/postconf.5.html
16. http://www.postfix.org/smtp.8.html
17. http://www.postfix.org/smtp.8.html
18. http://www.postfix.org/postconf.5.html
19. http://www.postfix.org/virtual.5.html
20. http://www.postfix.org/postconf.5.html
21. http://www.postfix.org/smtp.8.html
22. http://www.postfix.org/postconf.5.html
23. http://www.postfix.org/postconf.5.html
24. http://www.postfix.org/postconf.5.html
25. http://www.postfix.org/postconf.5.html
26. http://www.postfix.org/master.5.html
27. http://www.postfix.org/postconf.5.html
28. http://www.postfix.org/postconf.5.html
29. http://www.postfix.org/postconf.5.html
30. http://www.postfix.org/generic.5.html
31. http://www.postfix.org/postconf.5.html
32. http://www.postfix.org/postconf.5.html
33. http://tools.ietf.org/html/rfc2606