

Jason Meers - Getting started with EXIM

Notes for Debian-based distributions

The examples all use a Red Hat/CentOS/Fedora style configuration.

Users of Debian-based distributions will need to substitute the following paths and filenames in all of their configurations and configuration files.

`/etc/exim` becomes `/etc/exim4`

`/etc/exim/exim.conf` becomes `/etc/exim4/exim4.conf`

Adding mailboxes to the server

The examples expect the following user accounts and mailboxes to be present on the system:

```
admin
alice
bob
carol
pa
hired
jsmith
```

Set up an account and a password for each of these users on your Exim server machine.

(If you don't, Exim will be unable to deliver messages to them.)

To add a user or change passwords you must have root privileges. You can use the same password for each user if your server is *not* publicly accessible and is for testing or training purposes only.

Your distribution will have its own user configuration tools for adding accounts and setting passwords. You should try these first.

Adding mailboxes to the server manually

If you have problems setting up these accounts and passwords, the following commands are available on all most Linux/UNIX systems:

To create a new user account:

```
# useradd alice          enter
```

To set a password for a user account you've already created:

```
# passwd alice          enter
```

Changing password for alice

New UNIX password:

Retype new UNIX password:

passwd: all authentication tokens updated successfully.

Repeat for each user, before moving on. Otherwise you may receive an “Unknown User” messages from your mail client when Exim trying to send mail messages to users mailboxes that don't exist yet.

Sending and receiving messages from local users.

Sending and receiving messages to and from local users will usually not require access to any external computers or services if SMTP, POP3 and IMAP are all installed on the same server as the users home directories and mailboxes. For this reason local deliveries will almost always work correctly without requiring access to external DNS servers, MX records, gateways or firewalls.

Sending messages to external servers.

When sending messages to external servers Exim will usually require a working Internet connection through a gateway or firewall to query DNS servers to retrieve MX records and resolve hostnames to Ip addresses. Failure to retrieve MX records or resolve hostnames can lead to undeliverable messages that remain in the queue until they are bounced/failed. Building a server from a non-routable or private range of IP addresses that **does not** have a gateway configured will lead to almost all external deliveries being held in the queue.

If you are new to building SMTP mail servers it would be wise to build your first few servers on a private network that is not connected to the Internet until you become more comfortable with the software. Obviously having no Internet connection or access to DNS servers will mean that the exim mail queue will soon fill up with undeliverable messages, but this is quite normal behaviour for a mail server and is exactly what happens in reality when sites unexpectedly encounter connection issues, DNS issues or problems with MX records.

Receiving messages from external servers

In order to receive messages from external servers we need to have a registered domain name, with valid MX records that point to a host or hosts with fixed IP addresses. If you don't have a fixed IP address to use it is still possible to use a dynamic DNS service such as DynDNS.org, however the domain name and MX record are still required for inbound SMTP deliveries to function correctly. If we don't have these we can only send messages externally and will only be able to receive messages from other local users with mailboxes on the same server as we do.

Public IP ranges

If you are a seasoned IT professional with a good knowledge of server security and Internet security you may want to connect your server directly to the Internet on a public IP address. Again this allows us to exchange messages with other email servers but having our server on a public IP address could make it much more visible and open to attack from malicious hackers.

Security

It is also important to remember that our servers have other services running on them in addition to SMTP, POP3 and IMAP and serious consideration should be given to removing, restricting and firewalling these services from anyone who does not need to use them. Most security professionals would recommend removing all unnecessary software and services from any server accessible from the Internet. This includes any graphical desktops, browsers, and unnecessary programs and utilities that may have been installed or used in earlier examples.

It is not recommended that you use a sever you have been learning on as a final email solution, wherever possible format the disks and start again completely from scratch and pay particular attention to security tools such as SELinux, App Armour, firewalls, strong passwords and any unnecessary services which may be running.

POP3 & IMAP

In order to access, send, receive and access messages stored in a local mailbox on our server we will need to provide a POP3 service, IMAP service, or both. The simplest way of doing this is to install a POP3/IMAP server such as Dovecot. Courier, Cyrus and UW-IMAP are also popular alternatives.

Overview of the configs

With the exception of C2 (which provides exactly the same functionality as C1 but in a different way), each config includes all the features of the preceding one.

Configuration C1

- A very simple configuration to introduce Exim.
- A mail server that can be used to send e-mails to other people locally (within your site), or externally (sent out over the Internet).

Configuration C2

- This works in exactly the same as C1, but all of the “scary” settings are hidden away in a master config file, and everything else is kept in two easy-to-understand files. Normally you will only have to edit these subsidiary files, leaving the master untouched.

Configuration C3

- This configuration can be used to automatically redirect messages sent to one person e-mail address to somebody else's e-mail address. This is useful if someone is on holiday, maternity or leaves the organization.
- Our redirect facility does not require any special permissions to read or modify the system “aliases” file.
- We also includes some changes that make it easy to re-use the same set of configuration files for many e-mail servers without having to duplicate work – for example if you are setting up another site with a similar type of mail server.

Configuration C4

- In this configuration we are more specific about what Exim should do if an e-mail can't be delivered the first time, and how often to keep trying to send e-mails before finally giving up on the message.
- We also check that nobody is trying to deliberately send “rogue” emails that are designed to crash computers and e-mail clients.

Configuration C5

- The mail server now becomes a “mail-relay”. A “mail-relay” is often used to reduce the load on other mail servers, or to allow other mail servers containing sensitive information to be “hidden” behind them on private networks.
- We also begin to start using our own custom error messages that make it easier to identify what went wrong should our server encounter delivery problems with certain e-mails.

Configuration C6

- The mail server now becomes a “mail-hub”. A “mail-hub” is often used to centralize sending, receiving and scanning e-mail messages in organizations with multiple mail servers.
- We also add a facility to send a warning e-mail to users who send messages over a certain size limit.
- Several new custom error messages and replies are added.
- For local destination addresses, we also now check that the users mailbox exists before trying to deliver an e-mail to it.

Configuration C7

- Support is added for third party mail scanning services and security appliances.
- Workarounds are shown for users with on “home” broadband Internet connections that block SMTP services running on port 25.
- Simple e-mail address lists are also covered. An address list allows a single e-mail address to be used to send a message to several people at once.
- This configuration provides a good base platform for building secure, high throughput mail servers with Anti-Virus, Anti-Spam and LDAP facilities.

Getting the configuration files

All of the configuration files mentioned in this document are available from the “Getting started with EXIM” section of the authors website:

<http://www.exim-new-users.co.uk>

Contact the author

Please send any comments, corrections and suggestions to:

jason @ exim-new-users . co . uk

It's a lonely job creating documentation, but receiving feedback, praise, criticism or even just an email to say “I got it working!” makes all the difference during late nights and weekends when it's tempting to just give up and go out for a beer instead. So if you found this useful, please find the time to send me an email from your new e-mail system.

(No viruses or spam please, just messages about the guides, tutorials or the site)

Professional services

If you require professional services, consultancy or hands-on training please contact me at the following address. If I can't help personally, I will try and find somebody else who can. Please include information regarding the actual country you are based in and the dates you require assistance.

jason @ rocksan . co . uk

My book

My book “Exim by Example” will be available in mid 2008.

ISBN-10: 0954452984

ISBN-13: 978-0954452988

NO WARRANTY – NO LIABILITY

The author accepts no liability for any damage or loss caused by the use of information contained in these documents. While every effort has been made in the creation of these documents, the author does not guarantee the accuracy of any of the information contained in them. It is the readers responsibility to decide for themselves if the information contained is accurate when deciding to follow this guide. A test system that does not contain any important information or correspondence is recommended for following these guides. The author also recommends that anyone wishing to follow these guides should first purchase a new, separate domain name for the purpose of testing, to ensure that no business critical systems are affected.