Email with Postfix, Dovecot, and MySQL

Updated Wednesday, April 29th, 2015 by Phil Zona

Contribute on GitHub View Project | View File | Edit File

In this guide, you'll learn how to set up a secure mail server with Postfix, Dovecot, and MySQL o Debian or Ubuntu. Specifically, we'll explain how to create new user mailboxes and send or rece email to and from configured domains.

For a different Linux distribution or different mail server, review our email tutorials.

Before You Begin

1. Set up the Linode as specified in the Getting Started and Securing Your Server guides.

2. Ensure that the iptables firewall is not blocking any of the standard mail ports (`25`, `465`, `587`, `110`, `995`, `143`, and `993`). If using a different form of firewall, confirm that not blocking any of the needed ports either.

Configure DNS

When ready to update the DNS and to start sending mail to the server, edit the domain's MX rec so that it points to the Linode's domain or IP address, similar to the example below:

```
1 ex
2 ex
3 ma
```

Ensure that the MX record is changed for all domains and subdomains that might receive email. setting up a brand new domain, these steps can be performed prior to configuring the mail serve When using Linode's DNS Manager, create an MX record that points to the desired domain or subdomain, and then create an A record for that domain or subdomain, which points to the corre IP address.

Installing an SSL Certificate

Dovecot offers a default self-signed certificate for free. This certificate encrypts the mail connecti similar to a purchased certificate. However, the email users receive warnings about the certificat when they attempt to set up their email accounts. Optionally, you can purchase and configure a commercial SSL certificate to avoid the warnings. For information about SSL certificates, see Linode's SSL Certificate guides.

> As of version 2.2.13-7, Dovecot no longer provides a default SSL certificate. This affects Debian 8 users, and means that if you wish to use SSL encryption (recommended), you must generate your ow self-signed certificate or use a trusted certificate from a Certificate Authority.
>
> Many email service providers such as Gmail will only accept commercial SSL certificates for secure IMAP/POP3 connections. To communicate with these providers, follow our guide for obtaining a commercial SSL certificate for Debian and Ubuntu or CentOS and Fedora.

Installing Packages

The next steps are to install the required packages on the Linode.

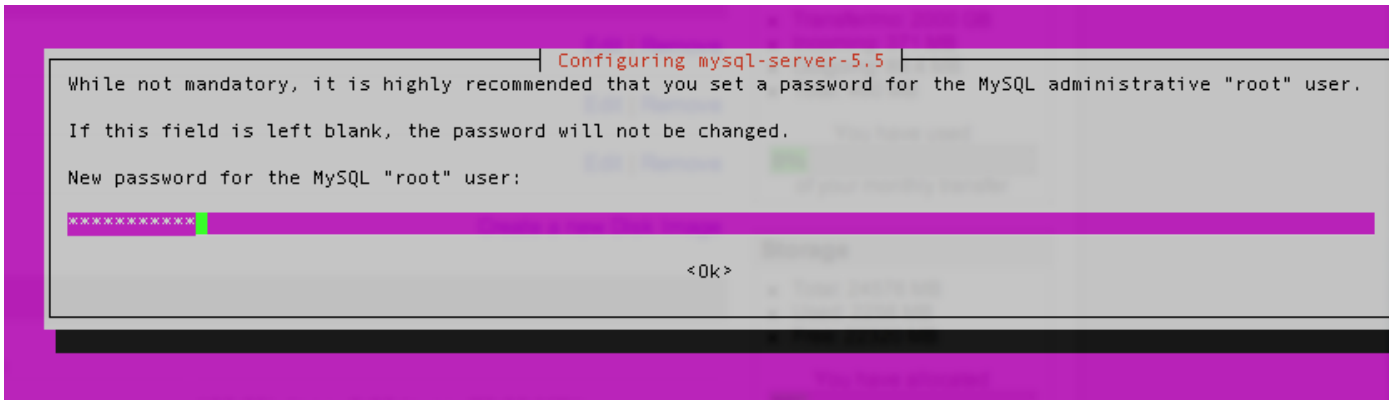
1. Log in as the root user via SSH. Replace `example` with your domain name or IP address:

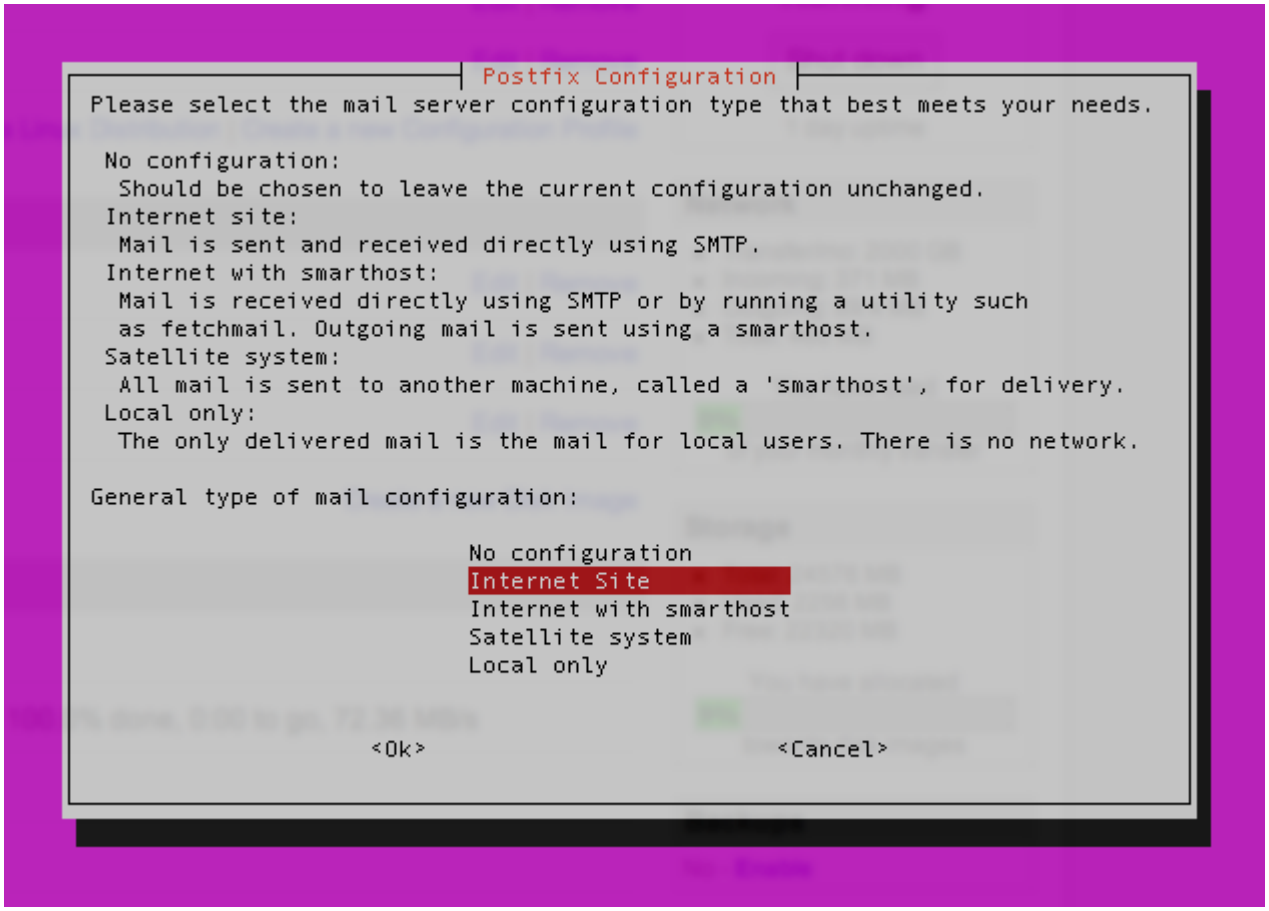
```
ss
```

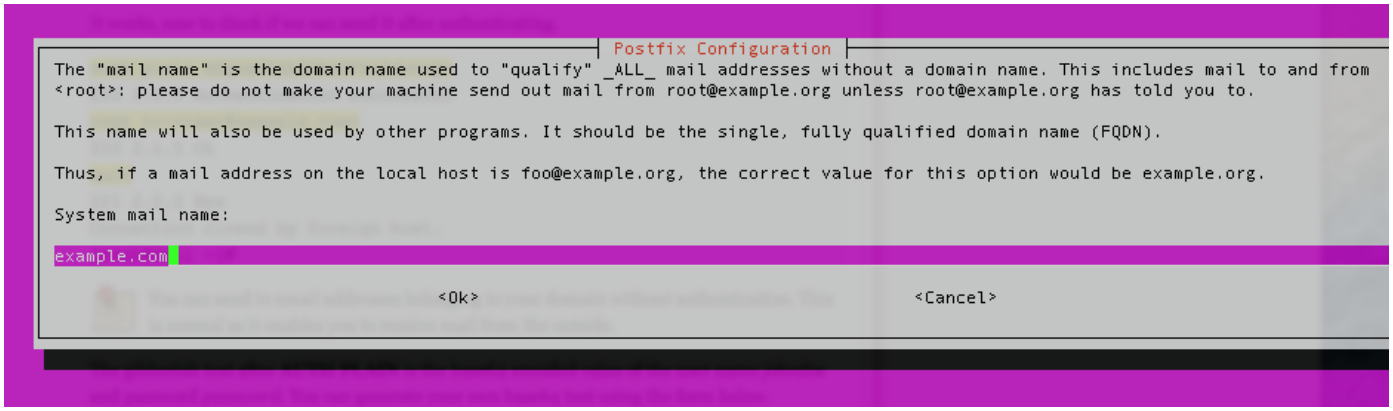
2. Install the required packages:

```
ap
```

   Follow the prompt to type in a secure MySQL password and to select the type of mail serve you wish to configure. Select **Internet Site**. The *System Mail Name* should be the FQDN.







MySQL

1. Create a new database:

```
1  my
```

2. Enter the MySQL root password.
3. Log in to MySQL:

```
my
```

4. Create the MySQL user and grant the new user permissions over the database. Replace `mailuserpass` with a secure password:

```
GR
```

5. Flush the MySQL privileges to apply the change:

```
FL
```

6. Create a table for the domains that will receive mail on the Linode:

```
CR

)
```

7. Create a table for all of the email addresses and passwords:

```
CR

)
```

8. Create a table for the email aliases:

```
CR

)
```

Adding Data

Now that the database and tables have been created, add some data to MySQL.

1. Add the domains to the `virtual_domains` table. Replace the values for `example.com` and `hostname` with your own settings.

```
IN

VA
```

> Note which `id` goes with which domain, the `id` is necessary for the next two steps.

2. Add email addresses to the `virtual_users` table. Replace the email address values with the addresses that you wish to configure on the mailserver. Replace the `password` values with strong passwords.

```
IN

VA
```

3. To set up an email alias, add it to the `virtual_aliases` table.

```
IN

VA
```

That’s it! Now you’re ready to verify that the data was successfully added to MySQL.

Testing

Since all of the information has been entered into MySQL, check that the data is there.

1. Check the contents of the `virtual_domains` table:

```
SE
```

2. Verify that you see the following output:

```
+-
|
+-
|
|
|
|
+-
4
```

3. Check the `virtual_users` table:

```
SE
```

4. Verify the following output, the hashed passwords are longer than they appear below:

```
+-
```

```
|
+-
|
|
+-
2
```

5. Check the `virtual_aliases` table:

```
SE
```

6. Verify the following output:

```
+-
|
+-
|
+-
1
```

7. If everything outputs correctly, you’re done with MySQL! Exit MySQL:

```
ex
```

Postfix

Next, set up Postfix so the server can accept incoming messages for the domains.

1. Before making any changes, make a copy of the default Postfix configuration file in case yo need to revert to the default configuration:

```
cp
```

2. Edit the `/etc/postfix/main.cf` file to match the following. Ensure that occurrences of `example.com` are replaced with the domain name. Also, replace `hostname` with the systen hostname on line 44.

/etc/postfix/main.cf

```
1  #
2
3  #
4  #
5  #
6  #r
7
8  sr
9  bi
10
11 #
12 ap
13
14 #
15 #c
16
17 re
18
19 #
20 #s
21 #s
22 #s
23 #s
24 #s
25
26 sr
27 sr
28 sr
29 sr
30
31 #E
32 sr
33 sr
34 sr
35
36 sr
37
38
39
40
```

```
#
#

my
al
al
my
#r
my
re
my
ma
re
in

#h
vi

#V
vi
vi
vi

```

3. Create the file for virtual domains. Ensure that you change the password for the `mailuser` account. If you used a different user, database name, or table name, change those settings as well.

/etc/postfix/mysql-virtual-mailbox-domains.cf

```
us
pa
ho
db
qu
```

4. Create the `/etc/postfix/mysql-virtual-mailbox-maps.cf` file, and enter the following values. Make sure you use the `mailuser`'s password and make any other changes as needed.

/etc/postfix/mysql-virtual-mailbox-maps.cf

```
us
pa
```

```
ho
db
qu
```

5. Create the `/etc/postfix/mysql-virtual-alias-maps.cf` file and enter the following values. Ag make sure you use the mailuser's password, and make any other changes as necessary.

/etc/postfix/mysql-virtual-alias-maps.cf

```
us
pa
ho
db
qu
```

6. Create the `/etc/postfix/mysql-virtual-email2email.cf` file and enter the following values. Again, make sure you use the mailuser's password, and make any other changes as necessary.

/etc/postfix/mysql-virtual-email2email.cf

```
us
pa
ho
db
qu
```

7. Save the changes you've made to the `/etc/postfix/mysql-virtual-email2email.cf` file, and restart Postfix:

```
su
```

8. Enter the following command to ensure that Postfix can find the first domain. Be sure to replace `example.com` with the first virtual domain. The command should return `1` if it is successful.

```
po
```

9. Test Postfix to verify that it can find the first email address in the MySQL table. Enter the following command, replacing `email1@example.com` with the first email address in the MySQL table. You should again receive `1` as the output:

```
po
```

10. Test Postfix to verify that it can find the aliases by entering the following command. Be sure replace `alias@example.com` with the actual alias you entered:

```
po
```

This should return the email address to which the alias forwards, which is `email1@example.com` in this example.

11. Make a copy of the `/etc/postfix/master.cf` file:

```
cp
```

12. Open the configuration file for editing and uncomment the two lines starting with `submission` and `smtps` and the block of lines starting with `-o` after each. The first sect of the `/etc/postfix/master.cf` file should resemble the following:

`/etc/postfix/master.cf`

```
#
#
#
#
#
#
#
#
#
#
sr
#s
#s
#c
```

```
#t
su
sr
```

13. Change the permissions on the `/etc/postfix` directory to restrict permissions to allow only owner and the corresponding group:

```
ch
```

14. Restart Postfix:

```
se
```

Congratulations! You have successfully configured Postfix.

Dovecot

Dovecot allows users to log in and check their email using POP3 and IMAP. In this section, configure Dovecot to force users to use SSL when they connect so that their passwords are nev sent to the server in plain text.

1. Copy all of the configuration files so that you can easily revert back to them if needed:

```
cp
cp
cp
cp
```

```
cp
cp
```

2. Open the main configuration file and edit the contents to match the following. Specifically, a
the line beginning with `protocols` under the section beginning with “Enable installed protoc

`/etc/dovecot/dovecot.conf`

```
#!

#

#
#

#
#
#

#
#
#
#
#
#

#
!:
pr

#
#
#
#
#:

#
#b

#
#:

#
#:

```

```
#
#
#
#
#l

#
#l

#
#
#
#v

#
#
#
#
#s

#
#
#c
#
#c

#
#
#
#i

##
##
##

#
#
#
#
#

di


}

#
```

```
#
#
!:

#
#
!:
```

3. Save the changes to the `/etc/dovecot/dovecot.conf` file.
4. Open the `/etc/dovecot/conf.d/10-mail.conf` file. This file controls how Dovecot interacts wit the server's file system to store and retrieve messages.

> Click this link to see the final, complete version of `10-mail.conf` example file. This is a long file, so you may need to use your text editor's search feature to find the values you need to edit.

Modify the following variables within the configuration file:

`/etc/dovecot/conf.d/10-mail.conf`

```
ma
.
ma
```

Save your changes and exit.

5. Enter the following command to verify the permissions for `/var/mail`:

```
ls
```

6. Verify that the permissions for `/var/mail` are as follows. The date and time will likely be different in your output:

```
dr
```

If your permissions do not match the above, go back and ensure you've completed the abo steps correctly.

7. Create the `/var/mail/vhosts/` directory and a subdirectory for your domain, replacing `example.com`:

```
mk
```

This directory will serve as storage for mail sent to your domain.

8. Create the `vmail` user with a user and group id of 5000 by entering the following commanc one by one. This user will be in charge of reading mail from the server.

```
gr
us
```

9. Change the owner of the `/var/mail/` folder and its contents to belong to `vmail`:

```
ch
```

10. Open the user authentication file, located in `/etc/dovecot/conf.d/10-auth.conf` and disable plain-text authentication by uncommenting this line:

`/etc/dovecot/conf.d/10-auth.conf`

```
di
```

Set the `auth_mechanisms` by modifying the following line:

`/etc/dovecot/conf.d/10-auth.conf`

```
au
```

Comment out the system user login line:

/etc/dovecot/conf.d/10-auth.conf

```
#
```

Enable MySQL authentication by uncommenting the `auth-sql.conf.ext` line:

/etc/dovecot/conf.d/10-auth.conf

```
#
!
#
#
#
#
#
```

> Click here to see the final, complete version of `10-auth.conf`.

Save the changes to the `/etc/dovecot/conf.d/10-auth.conf` file.

11. Edit the `/etc/dovecot/conf.d/auth-sql.conf.ext` file with the authentication information. Ens your file contains the following lines and that they are uncommented:

/etc/dovecot/conf.d/auth-sql.conf.ext

```
pa


}
us
```

Save the changes to the `/etc/dovecot/conf.d/auth-sql.conf.ext` file.

12. Update the `/etc/dovecot/dovecot-sql.conf.ext` file with our custom MySQL connection information.

Uncomment and set the `driver` line as shown below:

/etc/dovecot/dovecot-sql.conf.ext

```
dr
```

Uncomment the `connect` line and set the MySQL connection information. Use the `mailuser` password and any other custom settings:

/etc/dovecot/dovecot-sql.conf.ext

```
co
```

Uncomment the `default_pass_scheme` line and set it to `SHA512-CRYPT`:

/etc/dovecot/dovecot-sql.conf.ext

```
de
```

Uncomment the `password_query` line and set it to the following:

/etc/dovecot/dovecot-sql.conf.ext

```
pa
```

> This password query lets you use an email address listed in the `virtual_users` table as the username credential for an email account. If you want to be able to use the alias as the username instead (listed in the `virtual_aliases` table), first add every primary email address t the `virtual_aliases` table (directing to themselves) and then use the following line in `/etc/dovecot/dovecot-sql.conf.ext` instead:
>
> ```
> pa
> ```

> Click the link to see the final, complete version of dovecot-sql.conf.ext.

Save the changes to the `/etc/dovecot/dovecot-sql.conf.ext` file.

13. Change the owner and group of the `/etc/dovecot/` directory to `vmail` and `dovecot`:

```
ch
```

14. Change the permissions on the `/etc/dovecot/` directory:

```
ch
```

15. Open the sockets configuration file, located at `/etc/dovecot/conf.d/10-master.conf`

> Click this link to see the final version of 10-master.conf. There are many nested blocks of code i this file, so please pay close attention to the brackets. It's probably better if you edit line by line, rather than copying large chunks of code. If there's a syntax error, Dovecot will crash silently, bu you can check `/var/log/upstart/dovecot.log` to help you find the error.

16. Disable unencrypted IMAP and POP3 by setting the protocols' ports to 0, as shown below. Ensure that the entries for port and ssl below the IMAPS and pop3s entries are uncommen

`/etc/dovecot/conf.d/10-master.conf`

```

in

}

po
ss
}



in
```

```
}
```

> Leave the secure versions unedited, specifically the `imaps` and `pop3s`, so that their ports still work. The default settings for `imaps` and `pop3s` are fine. Optionally, leave the `port` lines commented out, as the default ports are the standard 993 and 995.

Find the `service lmtp` section and use the configuration shown below:

/etc/dovecot/conf.d/10-master.conf

```
```

Locate the `service auth` section and configure it as shown below:

/etc/dovecot/conf.d/10-master.conf

```
se
```

```
}
```

In the `service auth-worker` section, uncomment the `user` line and set it to `vmail` as shown below:

`/etc/dovecot/conf.d/10-master.conf`

```
se
}
```

Save the changes to the `/etc/dovecot/conf.d/10-master.conf` file.

17. Verify that the default Dovecot SSL certificate and key exist:

```
ls
ls
```

> As noted above, these files are not provided in Dovecot 2.2.13-7 and above, and will not be present on Debian 8 and other newer systems, as well as some older ones.
>
> If using a different SSL certificate, upload the certificate to the server and make a note of its location and the key's location.

18. Open `/etc/dovecot/conf.d/10-ssl.conf`.

> Click the link to see the final, complete version of 10-ssl.conf.

19. Verify that the `ssl_cert` setting has the correct path to the certificate, and that the `ssl_key` setting has the correct path to the key. The default setting displayed uses Dovecot's built-in certificate, so you can leave this as-is if using the Dovecot certificate. Up the paths accordingly if you are using a different certificate and key.

`/etc/dovecot/conf.d/10-ssl.conf`

```
ss
ss
```

Force the clients to use SSL encryption by uncommenting the `ssl` line and setting it to `required`:

`/etc/dovecot/conf.d/10-ssl.conf`

```
ss
```

Save the changes to the `/etc/dovecot/conf.d/10-ssl.conf` file.

20. Finally, restart Dovecot:

```
se
```

Test Email

1. Set up a test account in an email client to ensure that everything is working. Many clients detect server settings automatically. However, manual configuration requires the following parameters:

    - the full email address, including the `@example.com` part, is the username.
    - the password should be the one you added to the MySQL table for this email address
    - The incoming and outgoing server names must be a domain that resolves to the Linoc
    - Both the incoming and outgoing servers require authentication and SSL encryption.
    - You should use Port 993 for secure IMAP, Port 995 for secure POP3, and Port 587 wi SSL for SMTP.

2. Try sending an email to this account from an outside email account and then reply to it. Ch the mail log file in */var/log/mail.log* for the following output (the first block is for an incoming message, and the second block for an outgoing message):

/var/log/mail.log

```
1  Ma
2  Ma
3  Ma
4  Ma
5  Ma
6  Ma
7  Ma
8  Ma
9  Ma
10 Ma
```

/var/log/mail.log

```
1  Ma
2  Ma
3  Ma
4  Ma
5  Ma
6  Ma
7  Ma
```

You now have a functioning mail server that can securely send and receive email. If things are n working smoothly, try consulting the Troubleshooting Problems with Postfix, Dovecot, and MySQL guide. At this point, consider adding spam and virus filtering and a webmail client. If DNS records have not been created for the mail server yet, do so now. Once the DNS records have propagated, email will be delivered via the new mail server.

> If errors are encountered in the /var/log/syslog stating “Invalid settings: postmaster_address setting n given”, you may need to append the following line to the /etc/dovecot/dovecot.conf file, replacing domain with the domain name.
>
> ```
> 1 p
> ```

Adding New Domains, Email Addresses, and Aliases

Although the mail server is up and running, eventually you’ll probably need to add new domains, email addresses, and aliases for the users. To do this, simply add a new line to the appropriate MySQL table. These instructions are for command-line MySQL, but you can also use phpMyAdmin to add new entries to the tables.

Domains

1. To add a new domain, open a terminal window and log in to the Linode via SSH.
2. Log in to the MySQL server with an appropriately privileged user. For this example, use the `root` user:

   ```
   1 my
   ```

3. Enter the root MySQL password when prompted.
4. Always view the contents of the table before adding new entries. Enter the following comma to view the current contents of any table, replacing `virtual_domains` with the table:

```
SE
```

5. The output should resemble the following:

```
+-
|
+-
|
|
|
|
+-
```

6. To add another domain, enter the following command, replacing `newdomain.com` with the domain name:

```
IN

VA
```

7. Verify that the new domain has been added. The output should display the new domain nai

```
SE
```

8. Exit MySQL:

```
qu
```

You have successfully added the new domain to the Postfix and Dovecot setup.

Email Addresses

1. To add a new email address, enter the following command in MySQL, replacing `newpassword` with the user's password, and `email3@newdomain.com` with the user's

email address:

```
IN

VA
```

> Be sure to use the correct number for the `domain_id`. In this case, we are using `5`, because w
> want to make an email address for `newdomain.com`, and `newdomain.com` has an `id` of `5` in the `virtual_domains` table.

2. Verify that the new email address has been added. The new email address should be displayed in the output.

```
SE
```

3. Exit MySQL:

```
qu
```

You have successfully added the new email address to the Postfix and Dovecot setup.

Aliases

1. To add a new alias, enter the following command in MySQL, replacing `alias@newdomain.com` with the address from which you want to forward email, and `myemail@gmail.com` with the address that you want to forward the mail to. The `alias@newdomain.com` needs to be an email address that already exists on the server.

```
IN

VA
```

> Ensure that the correct number is entered for the `domain_id` value. Use the `id` of the domain f
> this email address. For an explanation of `id` us, see the email users section above.

You can also add a “catch-all” alias which will forward all emails sent to a domain which do have matching aliases or users by specifying `@newdomain.com` as the source of the alias.

```
IN

VA
```

2. Verify that the new alias has been added. The new alias will be displayed in the output.

```
SE
```

3. Exit MySQL:

```
qu
```

You have now successfully added the new alias to the Postfix and Dovecot setup.