Hardening Postfix For ISPConfig 3

Author: Jesús Córdoba
Email: j.cordoba [at] gmx [dot] net
Forum user: pititis

Version: 1.2

On this page

The goal of this tutorial is to harden the mail server postfix used by ISPConfig for internet mail servers where authenticated users are trusted. With this setup you will reject a great amount of spam before it passes into your mail queue, saving a lot of system resources and making your mail server strong against spammers and spam botnets. Let's go.

Reverse DNS, (DNS PTR Record)

To set up rdns you will find two situations:

- Your ISP allows to you change it yourself. Take a look in your control panel.

- Your ISP doesn't allow to you change it. Just send an email with your request.

Ask or point your rdns record to your server. i.e *server.example.com* You can check your rdns with the command host:

```
root@server / #  host 149.20.4.69
```

```
  69.64-27.4.20.149.in-addr.arpa domain name pointer pub2.
kernel.org.
```

Remember dns must propagate the changes.

SPF For Your Domain (DNS TXT Record)

SPF is an email validation system designed to prevent email spam by detecting email spoofing, a common vulnerability, by verifying sender IP addresses.

To set up spf you will need to add a TXT record to your dns zone but first you can generate your record here: http://www.mailradar.com/spf/

Copy the spf result, then go to ISPConfig -> dns -> zones ->click on your domain name -> click on records tab -> and click on *TXT*

Hostname -> *example.com.* (**with dot at the end!**)

Text -> Paste here the spf result (without " ").

Example: *v=spf1 a mx ptr ip4:11.222.333.444 -all* ...and click on *Save*.

Remember dns must propagate the changes.

Postfix main.cf

Let's add/change something to */etc/postfix/main.cf*

Helo restrictions:

```
smtpd_helo_required = yes
smtpd_helo_restrictions = permit_mynetworks, permit_sasl_a
uthenticated, reject_non_fqdn_helo_hostname, reject_invali
d_helo_hostname
```

Helo restrinctions in action:

```
Jan 12 01:57:08 server postfix/smtpd[4687]: NOQUEUE: rejec
t: RCPT from unknown[186.43.77.153]: 450 4.7.1 Client host
rejected: cannot find your hostname, [186.43.77.153]; from
=
<pamela_nathan@ixxxxxs.com.au> to=<boricua@domain.com> pro
```

```
to=ESMTP helo=<[186.43.77.153]>
Jan  8 00:32:22 server postfix/smtpd[17504]: NOQUEUE: reje
ct: RCPT from 201-93-87-2.dial-up.telesp.net.br[201.93.87.
2]: 504 5.5.2 <lan-32204df3031>: Helo command rejected: ne
ed fully-qualified hostname; from=<nils-allan.lindgren@dex
xxxxe.ca> to=<boricua@domain.com> proto=ESMTP helo=<lan-32
204df3031>
```

Strict rfc:

```
strict_rfc821_envelopes = yes
```

Clients restrictions:

```
smtpd_client_restrictions = permit_mynetworks, permit_sasl
_authenticated, reject_unknown_client_hostname, check_clie
nt_access mysql:/etc/postfix/mysql-virtual_client.cf
```

Recipient restrictions:

```
smtpd_recipient_restrictions = permit_mynetworks, permit_s
asl_authenticated, reject_unauth_destination, check_recipi
ent_access mysql:/etc/postfix/mysql-virtual_recipient.cf,
reject_unknown_recipient_domain
```

Data restrictions:

```
smtpd_data_restrictions = reject_unauth_pipelining
```

Smtpd delay:


```
smtpd_delay_reject = yes
```

Don't forget reload postfix:

```
/etc/init.d/postfix reload
```

SPF Check For Postfix (Debian And Ubuntu)

Intstall spf package:

```
apt-get install postfix-policyd-spf-python
```

or

```
apt-get install postfix-policyd-spf-perl
```

Add this to `/etc/postfix/main.cf` :

```
policy-spf_time_limit = 3600s
```

and add *check_policy_service unix:private/policy-spf* at the end of *smtpd_recipient_restrictions*:

```
smtpd_recipient_restrictions = permit_mynetworks, permit_s
asl_authenticated, check_recipient_access mysql:/etc/postf
ix/mysql-virtual_recipient.cf, reject_unauth_destination,
reject_unknown_recipient_domain, check_policy_service uni
x:private/policy-spf
```

Now edit *master.cf* and add at the end this (for the python version):

```
policy-spf  unix  -       n       n       -       -
spawn
     user=nobody argv=/usr/bin/policyd-spf
```

or this for the perl version:

```
policy-spf  unix  -       n       n       -       -
spawn
     user=nobody argv=/usr/sbin/postfix-policyd-spf-perl
```

…reload postfix.

```
/etc/init.d/postfix reload
```

Spf check in action:

```
Jan  4 15:50:11 server postfix/smtpd[19096]: NOQUEUE: reje
ct: RCPT from g230068165.adsl.alicedsl.de[92.230.68.165]:
550 5.7.1 <william@domain.org>: Recipient address rejecte
d: Message rejected due to: SPF fail - not authorized. Ple
ase see http://www.openspf.org/Why?s=helo;id=paxxxxxn.com;
ip=92.230.68.165;r=william@domain.com; from=<opaquenesszv9
1@paxxxxxn.com> to=<william@domain.com> proto=ESMTP helo=
<paxxxxxn.com>
```

Greylist

Greylisting is a method of defending email users against spam. A mail transfer agent (MTA) using greylisting will "temporarily reject" any email from a sender it does not recognize. If the mail is legitimate the originating server

will, after a delay, try again and, if sufficient time has elapsed, the email will be accepted.

Installing *postgrey* (Debian, Ubuntu):

```
apt-get install postgrey
```

The configuration options are in */etc/default/postgrey* (default delay is 5 min).

Edit *main.cf* and add *check_policy_service inet:127.0.0.1:10023* to the end of *smtpd_recipient_restrictions*:

```
smtpd_recipient_restrictions = permit_mynetworks, permit_s
asl_authenticated, check_recipient_access mysql:/etc/postf
ix/mysql-virtual_recipient.cf, reject_unauth_destination,
reject_unknown_recipient_domain, check_policy_service uni
x:private/policy-spf,check_policy_service inet:127.0.0.1:1
0023
```

…reload postfix:

```
/etc/init.d/postfix reload
```

Greylist in action:

```
Jan 10 17:38:57 server postfix/smtpd[21302]: NOQUEUE: reje
ct: RCPT from mailout-de.gmx.net[213.165.64.22]: 451 4.7.1
<admin@domain.com>: Recipient address rejected: Greylistin
g in effect, please come back later; from=<joe@gmx.net> to
=<admin@domain.com> proto=SMTP helo=<mailout-de.gmx.net>
```

DNSBL (DNS Based Blacklist/Blocklist)

A DNSBL is a list of ip addresses published through the Internet Domain Name Service (DNS) either as a zone file that can be used by DNS server software, or as a live DNS zone that can be queried in real-time. DNSBLs are most often used to publish the addresses of computers or networks linked to spamming; most mail server software can be configured to reject or flag

messages which have been sent from a site listed on one or more such lists. These may include listing the addresses of zombie computers or other machines being used to send spam, listing the addresses of ISPs who willingly host spammers, or listing addresses which have sent spam to a honeypot system. To use dnsbl with postix we use reject_rbl_client. Just add some live dns zone for queries into the *main.cf* file.

In my example I will use two lists with very good reputation (added to the end of *smtpd_client_restrictions*):

```
smtpd_client_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_unknown_client_hostname, check_client_access mysql:/etc/postfix/mysql-virtual_client.cf,  reject_rbl_client cbl.abuseat.org,  reject_rbl_client b.barracudacentral.org
```

rbl in action:

```
Jan 12 01:52:42 server postfix/smtpd[4616]: NOQUEUE: reject: RCPT from 89.pool85-49-26.dynamic.orange.es[85.49.26.89]: 554 5.7.1 Service unavailable; Client host [85.49.26.89] blocked using cbl.abuseat.org; Blocked - see http://cbl.abuseat.org/lookup.cgi?ip=85.49.26.89; from=<dresschirp@fxxxxx.com> to=<william@domain.com> proto=SMTP helo=<colossus.home>
Jan 11 20:13:58 server postfix/smtpd[29591]: NOQUEUE: reject: RCPT from 93-87-122-56.dynamic.isp.telekom.rs[93.87.122.56]: 554 5.7.1 Service unavailable; Client host [93.87.122.56] blocked using b.barracudacentral.org; http://www.barracudanetworks.com/reputation/?pr=1&ip=93.87.122.56; from=
<trundlesd@ukxxxxx.edu> to=<infoo@domain.com> proto=ESMTP helo=
```

Postscreen

Note: This feature is available in Postfix 2.8 and up

The Postfix postscreen daemon provides additional protection against mail server overload. One postscreen process handles multiple inbound SMTP connections, and decides which clients may talk to a Postfix SMTP server process. By keeping spambots away, postscreen leaves more SMTP server processes available for legitimate clients, and delays the onset of server overload conditions.

The main challenge for postscreen is to make an is-it-a-zombie decision based on a single measurement. This is necessary because many zombies

try to fly under the radar and avoid spamming the same site repeatedly. Once postscreen decides that a client is not-a-zombie, it whitelists the client temporarily to avoid further delays for legitimate mail.

We will use for this tutorial the default settings with an exception. These settings are fine for the most situations

First, we add a line to main.cf with the command:

```
postscreen_greet_action = enforce
```

Second we add postscreen and some new services to master.cf Note: These settings can already exists, just uncomment. Also be sure that the line "smtp inet ... smtpd", including any parameter is commented out (if any, parameters must be moved to the new smtpd service).

```
# Postfix master process configuration file.  For details
on the format
# of the file, see the master(5) manual page (command: "ma
n 5 master").
#
# Do not forget to execute "postfix reload" after editing
this file.
#
# ==========================================================
==================
# service type  private unpriv  chroot  wakeup  maxproc co
mmand + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================
==================
#smtp      inet  n       -       -       -       -       s
mtpd
#          -o ...
smtpd     pass  -       -       n       -       -       sm
tpd
     -o ... # Parameters moved from smtp service to the ne
w smtpd service.(if any)
smtp      inet  n       -       n       -       1       po
stscreen
tlsproxy  unix  -       -       n       -       0       tl
sproxy
dnsblog   unix  -       -       n       -       0       dn
sblog
```

Now, we reload postfix:

```
/etc/init.d/postfix reload
```


Suggested articles

28 Comment(s)

Add comment

Name *

Email *

p

I'm not a robot

reCAPTCHA
Privacy - Terms

Submit comment

Comments

By: Reply

Very useful, thank you - especially because there's a big lack of tutorials for mailserver hardening otherwise.

By: Reply

This tutorial helped me get rid of all spam my clients were receiving, thank you very much! Great tutotiral!

By: Reply

I Implemented all these nice features in my mailserver now.
Now I also want postscreen to work properly but it just won't work for me. I followed the instructions on postfix.org (postscreen README) but as soon as I change the line:
smtp inet n - - - - smtpd
to:
smtp inet n - n - 1 postscreen
I can't send any emails from my POP3 email client anymore.
Sure hope that you can shine more light on postscreen for ISPConfig3 too.

By: Anonymous Reply

You need to send email through port 587 (submission) and not anymore through port 25.

By: Reply

Added postscreen to the tutorial.

By: Reply

Spam was really a problem, this has really solved the prob. Thanx loads

By: Reply

Removed **reject_unknown_helo_hostname** from helo restrictions. It causes several false positives from legitimate clients with dns problems/misconfiguration.

By: Reply

I think is reject_invalid_helo_hostname right? thanks! great tutorial.

By: Reply

They are two different directives:
reject_invalid_helo_hostname (with Postfix < 2.3: reject_invalid_hostname)
Reject the request when the HELO or EHLO hostname is malformed. Note: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip reject_invalid_helo_hostname by not sending HELO or EHLO).
The invalid_hostname_reject_code specifies the response code for rejected requests (default: 501).
reject_unknown_helo_hostname (with Postfix < 2.3: reject_unknown_hostname)
Reject the request when the HELO or EHLO hostname has no DNS A or MX record.

The unknown_hostname_reject_code parameter specifies the numerical response code for rejected requests (default: 450).
The unknown_helo_hostname_tempfail_action parameter specifies the action after a temporary DNS error (default: defer_if_permit). Note: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip reject_unknown_helo_hostname by not sending HELO or EHLO).

By: Reply

Thanks, pititis! Just about every Postfix user should benefit from this How-To. The default configuration is hardly suitable for most real-world scenarios (and I understand why the Postfix authors have set the defaults as they have; I'm not blaming them).
While perhaps outside the scope of this How-To, another measure I have taken that has cut-down on spam-related activity considerably is switching-on fail2ban's Postfix filter, which essentially bans IP addresses (via iptables) whenever they elicit a 554 response code. (Actually, I added banning for 504 responses, too, as no legitimate user should experience one in my particular environment.) This measure ensures that the same remote hosts do not hammer on Postfix with illegitimate garbage for extended periods of time.
Thanks again!

By: Reply

Regarding the smtpd_recipient_restrictions list that is recommended in the How-To, the Postfix author himself (Wietse Venema) states very clearly that reject_unauth_destination should always come before check_recipient_access in order to prevent unexpected open-relay problems. The order should be:

smtpd_recipient_restrictions =
permit_mynetworks,
permit_sasl_authenticated,
reject_unauth_destination,
check_recipient_access mysql:/etc/postfix/mysql-virtual_recipient.cf

For the original discussion, see http://archives.neohapsis.com/archives/postfix/2013-06/0053.html .

By: Reply

This is soooooo important! Thank you very much, it solved my problem with many many fake senders.

By: Reply

You're very welcome! I reported this critical issue, and the ISPConfig team fixed it in version 3.0.5.4.p2. Link to the bug report: http://bugtracker.ispconfig.org/index.php?do=details&task_id=3478

By: Reply

In the postscreen section, isn't this line erroneous?

postconf -e postscreen_greet_action = enforce

You state to place this line in main.cf, but you seem to have prepended the directive with "postconf -e", which is not valid syntax in the context of main.cf.
The line should be:

postscreen_greet_action = enforce

By: Reply

Yes, it is. Thank you

By: Raeco Reply

E-mails with the error 450 4.7.1 Client host rejected: cannot find your hostname
Do is possible configure some sort of exception to get around this rule just for specific ip?

By: thctlo Reply

@Raeco.. RFC stats.. CLIENT Must have A and RR (PTR) in the DNS.HELO Must have A in the DNS.
Any server connecting not having these, block them, they are the main problem why spam exist. Most are crappy providers. I reject them with and 550 message, that they dont RFC compliance.

By: Feby Reply

After a lot of headache and research online about policyd, I've managed to get it working but in it's "easy" webui way on a Ubuntu server 12.10 (yea I know not supported) but it works on other versions as well.
What I did and from where and why:
There is a module that can be downloaded from apt-get but I hadn't seemed to see it working with a DB.
So, first get policyd.org I've got 2.0.17 and untar.gz it
wget http://download.policyd.org/v2.0.14/cluebringer-v2.0.14.tar.gz
tar -xzf cluebringer-v2.0.14.tar.gz
cd cluebringer-v2.0.14 and start reading the INSTALLATION file, which is a little ambiguous but what you need to do next is complete the decencies. for those (like myself) sho didn't get what net::server meant or Mail::SPF, I had to research it. These are modules requested by Pearl, so you need pearl installed... I've had it from the tutorials of howtoforge.com
next step is to install the deps. of pearl to do this start pearl in shell mode
perl -MCPAN -e shell

and after the initial config (if you hand't ran it ever it will ask different things just go with the defaults)
after start writing in this shell (it doesn't support copy paste so you'll have to do it by hand and take notice it is CASE SENSITIVE so ...)
Module::Build
q -> this options quits, you have to go again in
perl -MCPAN -e shell
install Net::Server
install Net::CIDR
(this can be installed via apt-get, I didn't know of the pearl installation so I got them via apt-get, apt-get install libconfig-inifiles-perl and apt-get install libcache-fastmmap-perl) if you use this method disregard the next 2 lines
install Config::IniFiles
install Cache::FastMmap
install NetAddr::IP
install Net::DNS::Resolver::Programmable
install NetAddr::IP
install Mail::SPF
the mail::spf if it return
Writing /usr/local/lib/perl/5.8.8/auto/Mail/SPF/.packlist
  /usr/bin/make install -- OK
then it's ok
hit q and enter and that's that for now.
The php needs to be at version 5 so you should have it up and running.
Now let's continue with the installation
cd database
mcedit runcmd and put in it (I use mcedit you can use vi or any other editor)
#!/bin/bash
for i in core.tsql access_control.tsql quotas.tsql amavis.tsql checkhelo.tsql checkspf.tsql greylisting.tsql
do
./convert-tsql mysql $i
done > policyd.mysql
save it and make it executable
chmod +x runcmd
./runcmd
and you get that sql file.
Now for security reasons I didn't allow it to run with my root of the sql so I went on and created a user and a database...
MySQL -uroot -p
(input your pass)
now create a db and a user and grant privileges so, I choosed as the db policyd policyddb the user and policydpassword for the password, you can change these to any other login info :
CREATE DATABASE policyd;
CREATE USER 'policyddb'@'localhost' IDENTIFIED BY 'policydpassword'
GRANT ALL PRIVILEGES ON policyd.* TO 'policyddb'@localhost;
FLUSH PRIVILEGES;

EXIT;
Done now you can continue with the tutorial:
so type MySQL -upolicyddb -p policyd < policyd.mysql
insert the pass,so you have to insert the pass of the policyddb user for me it was policydpassword
but,for me it gave an error as I have MySQL ver 5.5 and I had to change the MySQL file.
at each table you need to change at the end from TYPE=InnoDB to ENGINE=InnoDB and then run again the sql command
MySQL -upolicyddb -p policyd < policyd.mysql
this should work now,so you have to insert the pass of the policyddb user for me it was policydpassword
copy the conf file
cd..
cp cluebringer.conf /etc/
mkdir /usr/local/lib/policyd-2.0
cp -r cbp /usr/local/lib/policyd-2.0/
cp cbpadmin /usr/local/bin/
cp cbpolicyd /usr/local/sbin/
install the webui meaning copy the contents of the webui to a new folder in /var/www/ for example and go to /etc/apache2/ and change the .conf file accordingly to point to that new folder and now configure the file /var/www/policyd/webui/includes/config.php and set the user and the pass for the newly created user in sql
do the same in /etc/cluebringer.conf
and in here the following adjustments:
uncomment pidfile
set the log_level to 4 if you want to see everything else leave it at 2
uncomment log_file, host,port
host=* I use local postfix so I set it to
host=127.0.0.1
port=10031
in [database]
complete the user and pass and uncomment them
now in the next part this is the config I had tried with what I found on the net but it didn't work so I made it to work
[AccessControl]
enable=1
[Accounting]
enable=1
# Greylisting module
[Greylisting]
enable=0
#[Whitelisting]
#enable=0
#[Senderthrottle]
#enable=1
CheckHelo module
[CheckHelo]
enable=1

CheckSPF module
[CheckSPF]
enable=0
#SENDERMSGLIMIT=1
#SENDERRCPTLIMIT=360000
Quotas module
[Quotas]
enable=1
and now you should save the file and start cbpolicyd if everything is ok it should not give any error at launch and you can see the log file with tail -f /var/log/cbpolicyd.log
Now go to postfix config main.cf and this is very important to do in this order !!!
at smtpd_recipient_restrictions add the first field to be the ruleset to send it to policyd. The order is very important so I have like it to work
smtpd_recipient_restrictions =
    check_policy_service inet:127.0.0.1:10031,
    permit_mynetworks,
...
after this add the next line
smtpd_end_of_data_restrictions = check_policy_service inet:127.0.0.1:10031
after that continue with the regular main.cf config. you do not need to modify anything in the master.cf
Now the next step is a pickle and it gave me headaches to try to make it work... so...
go the to webbrowser and set the rules for policyd.
www.domain.com/policyd/webui/
there is no login info now the access control you can activate to create special rules of not sending from one domain to another you need to make it enable in cluebringer.conf
Now to set the limits you need to do the following:
go to Policies-> main -> action -> add
set a name, a priority (you can go with 50)and a description
go with submit query
back to policies (up button) select the added policy action change change disabled to no save it go back
Select again the policy action -> members
here you add the members that are added in the policies groups, you can go with source with %internal_domains and destination !%internal_domains meaning the you can send from your domains to anywere and the policy to count.
next go to policies -> groups -> and change %internal_domains and add the domains that are on your server with the @domain.com format. add as many as you want.
Next go to quotas -> action -> add
give a name, track I set sender user@domain (so it logs a user of a domain and this is policy to be used)
period in seconds (I think, need further testing, on the main site there a few versions with different versions but I think it's seconds), link policy choose the policy you've created earlier, verdict, reject, data, input a text to give at the access denied and a comment if you like, save it and now select the quota -> action -> change -> activate it (disable set it to no)
go back select it again -> action -> limits -> action -> add

here you add the number of messager to be sent in that specific time period provided earlier. To test it out you can set the message counter to 1 and play with your domains. If it gives an error after the first send it is ok and you've completed it successfully.
The tutorial provided online by policyd are a little bit confusing but after a time you will understand them better to create a more complex settings, but this is for those users who just want to limit the amount of emails to be sent and prevent blacklisting a domain cause of a stupid user that hasn't got a antivirus and goes on strange sites and gets infected with a spam bot...
Cheers and I hope you find usefull my tutorial...

By: edge Reply

No clue how old this post from you @Feby is, and I hope that you can help me with creating some rules.
Are you still active here?

By: corpus Reply

The correct parameter is "policy-spf_time_limit", not "spf-policyd_time_limit".

By: brody Reply

I am having a problem on Centos 7

Jul 14 23:52:50 hydrogen postfix/smtpd[2989]: warning: connect to private/policy-spf: Connection refusedJul 14 23:52:50 hydrogen postfix/smtpd[2989]: warning: problem talking to server private/policy-spf: Connection refusedJul 14 23:52:51 hydrogen postfix/smtpd[2989]: warning: connect to private/policy-spf: Connection refusedJul 14 23:52:51 hydrogen postfix/smtpd[2989]: warning: problem talking to server private/policy-spf: Connection refusedJul 14 23:52:51 hydrogen postfix/smtpd[2989]: NOQUEUE: reject: RCPT from nm37-vm4.bullet.mail.ne1.yahoo.com[98.138.119.132]: 451 4.3.5 Server configuration problem;

By: Slug Reply

For me the reject_invalid_helo_hostname did not stop the spammers at all, however i changed it to just reject_invalid_hostname, and now everything works perfectly!NOQUEUE: reject: RCPT from unknown[14.183.111.153]: 450 4.7.1 Client host rejected: cannot find your hostname, [14.183.111.153]; from=<Mayer.60@static.vnpt.vn> to=<***> proto=ESMTP helo=<static.vnpt.vn>NOQUEUE: reject: RCPT from unknown[103.53.164.66]: 450 4.7.1 Client host rejected: cannot find your hostname, [103.53.164.66]; from=<Dunn.20@extremeweatherproductions.com> to=<***> proto=ESMTP helo=<[103.53.164.66]>NOQUEUE: reject: RCPT from unknown[182.64.250.245]: 450 4.7.1 Client host rejected: cannot find your hostname, [182.64.250.245]; from=<Mcbride.756@airtelbroadband.in> to=<***> proto=ESMTP helo=<abts-north-dynamic-147.21.162.122.airtelbroadband.in>

By: brody Reply

Are these techniques added in ispcinfig 3.1 or do I still noeed to add them?

By: Gwyneth Llewelyn Reply

You need to add them.

By: icemaker Reply

after adding the postscreen configurations as suggested below,
the smtp server is always timing out and we are unable to send emails.
any suggestions?

By: David Bucknell Reply

Problems after hardening: tail /var/log/mail.log (debian, postfix, ispconfig,
1. insecure message: Today 02:04:26 host opendkim[1472]: domain: key data is not secure: /etc/opendkim/keys/domain.private is in group 127 which has multiple users (e.g., "postfix")
2. Error loading key: Today 02:04:26 host opendkim[1472]: 8CC6820CE5: error loading key 'domain'
3. Can't send mail via client (e.g. Thunderbird): Today 02:04:26 host postfix/cleanup[17148]: 8CC6820CE5: milter-reject: END-OF-MESSAGE from localhost[127.0.0.1]: 4.7.1 Service unavailable - try again later; from=<getmail@host.domain> to=<user@domain>
Sorry to ask, but any ideas from these log errors?

By: Tastiger Reply

Can someone confirm that this tutorial is still valid as I have problems with my mail after applying the changes on my Ubuntu Perfect Server 16.04? The tutorial worked fine with 14.04.
My mail server just stops working if all changes are implimented - also I have extra entries in my Helo restrictions:
smtpd_helo_restrictions = permit_sasl_authenticated, permit_mynetworks, check_helo_access regexp:/etc/postfix/helo_access, reject_invalid_hostname, reject_non_fqdn_hostname, check_helo_access regexp:/etc/postfix/blacklist_helo
Should these entries be replaced or retained?
Does it matter what line in main.cf the following is placed? - then I can continue the tutortorial and see at what stage the mail server stops working.
strict_rfc821_envelopes = yes

By: Airbag888 Reply

Did you find out?

Tutorial Info

Author: pititis

Tags: linux, postfix, anti-spam/virus, control panels, email, ispconfig

How do I edit files on the command line?

How to use the Linux ftp command to up- and download files on the shell

The Perfect Server - Debian 10 (Buster) with Apache, BIND, Dovecot, PureFTPD and ISPConfig 3.2

How to Install and Use Snap Package Manager on Ubuntu 20.04

Install and Use Guacamole Remote Desktop on CentOS 8

How to Install Shopware 6 with NGINX and Let's Encrypt on CentOS 8

How to Install a Debian 10 (Buster) Minimal Server

How to Install GoAccess Web Log Analyzer on Ubuntu 20.04

How to Install and Use PowerShell on Ubuntu 20.04