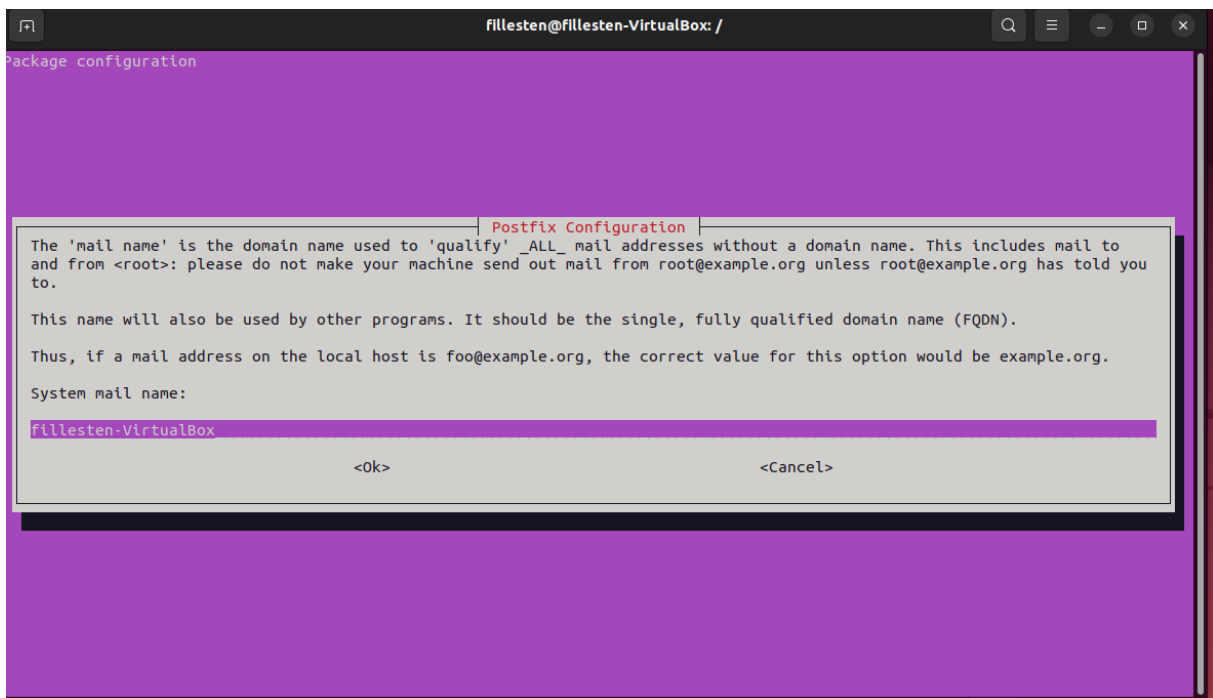
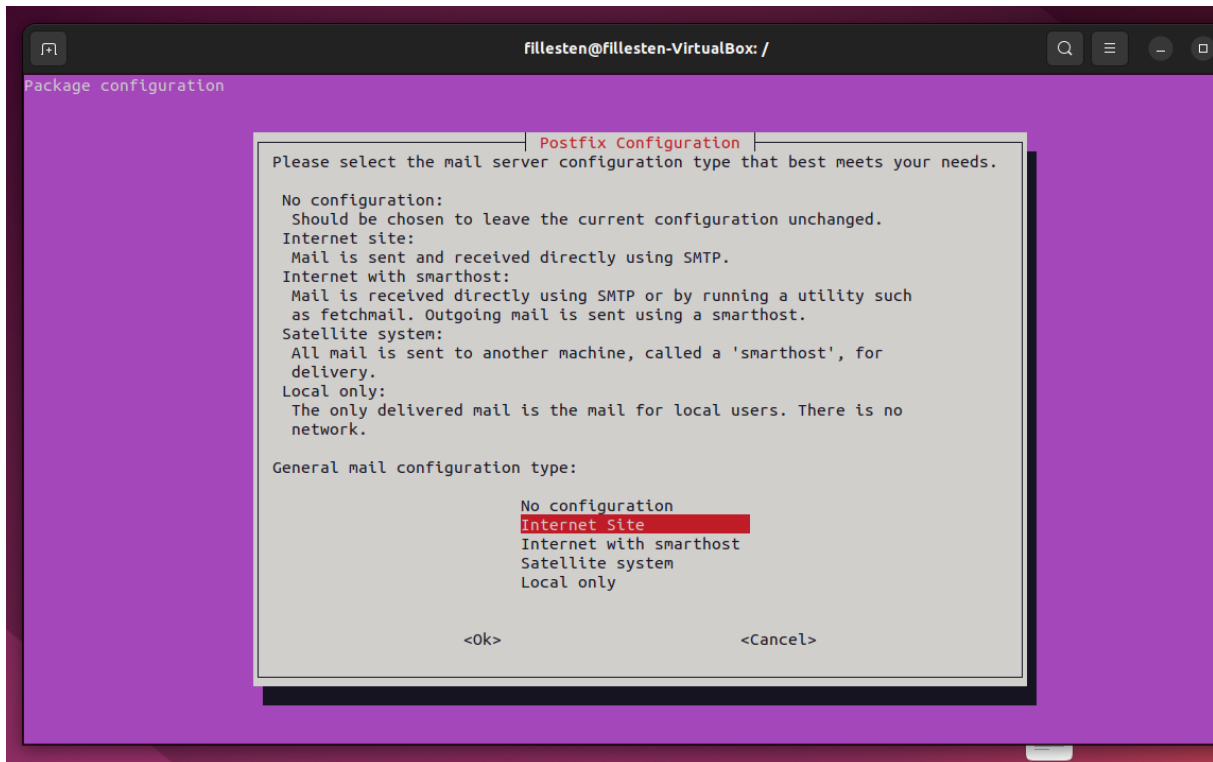


# UNIX LAB 5

## 4.1 MTA/MDA

Sudo apt install postfix öppnar denna ruta sen börjar den ladda ner.



```
50 packages can be upgraded. Run 'apt list --upgradable' to see them.
fillesten@fillesten-VirtualBox:/$ sudo apt install postfix
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite
```

Laddar ner postfix.

```
fillesten@fillesten-VirtualBox:/$ sudo apt-get install mailutils
Reading package lists... Done
Building dependency tree... Done
```

Hämtar mailutils paketen.

```
fillesten@fillesten-VirtualBox:/$ sudo systemctl restart postfix
```

Startar om postfix

```
fillesten@fillesten-VirtualBox:/etc/postfix$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 fillesten-VirtualBox ESMTP Postfix (Ubuntu)
ehlo localhost
250-fillesten-VirtualBox
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
mail from: fillesten@localhost
250 2.1.0 Ok
rcpt to: donald@localhost
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: My first mail on Postfix

Hi,
Are you there?
regards,
Admin
.
250 2.0.0 Ok: queued as 78E781C3432
quit
221 2.0.0 Bye
Connection closed by foreign host.
fillesten@fillesten-VirtualBox:/etc/postfix$
```

Kör telnet localhost 25 och följer instruktionerna från  
(<https://help.ubuntu.com/community/PostfixBasicSetupHowto>)

```

fillesten@fillesten-VirtualBox:/etc/postfix$ su - donald
Password:
donald@fillesten-VirtualBox:~$ mail
"/var/mail/donald": 1 message 1 new
>N 1 fillesten@localhos tis nov 7 18:53 16/473 My first mail on Postfix
?
Return-Path: <fillesten@localhost>
X-Original-To: donald@localhost
Delivered-To: donald@localhost
Received: from localhost (localhost [127.0.0.1])
        by fillesten-VirtualBox (Postfix) with ESMTP id 78E781C3432
        for <donald@localhost>; Tue, 7 Nov 2023 18:51:33 +0100 (CET)
Subject: My first mail on Postfix
Message-Id: <20231107175149.78E781C3432@fillesten-VirtualBox>
Date: Tue, 7 Nov 2023 18:51:33 +0100 (CET)
From: fillesten@localhost

Hi,
Are you there?
regards,
Admin

? 1
Return-Path: <fillesten@localhost>
X-Original-To: donald@localhost
Delivered-To: donald@localhost
Received: from localhost (localhost [127.0.0.1])
        by fillesten-VirtualBox (Postfix) with ESMTP id 78E781C3432
        for <donald@localhost>; Tue, 7 Nov 2023 18:51:33 +0100 (CET)
Subject: My first mail on Postfix
Message-Id: <20231107175149.78E781C3432@fillesten-VirtualBox>
Date: Tue, 7 Nov 2023 18:51:33 +0100 (CET)
From: fillesten@localhost

Hi,
Are you there?
regards,
Admin

? q
Saved 1 message in /home/donald/mbox
Held 0 messages in /var/mail/donald
donald@fillesten-VirtualBox:~$

```

Mailboxen för donald, man kan se det jag skickade från fillesten@localhost.

```

donald@fillesten-VirtualBox:/$ su - fillesten
Password:
fillesten@fillesten-VirtualBox:~$ sudo postconf -e 'home_mailbox = Maildir/'
[sudo] password for fillesten:
fillesten@fillesten-VirtualBox:~$ sudo postconf -e 'mailbox_command =
> ^C
fillesten@fillesten-VirtualBox:~$ sudo postconf -e 'mailbox_command = '
fillesten@fillesten-VirtualBox:~$ sudo systemctl restart postfix
fillesten@fillesten-VirtualBox:~$

```

Configurerar så den använder maildir i stället för mboxes.

ser till att procmail inte används.

Och restartar postfix

```

fillesten@fillesten-VirtualBox:~$ sudo dpkg-reconfigure postfix
setting synchronous mail queue updates: false
mailname is not a fully qualified domain name. Not changing /etc/mailname.
setting destinations: fillesten-VirtualBox, fillesten-VirtualBox, localhost.localdomain, , localhost
setting relayhost:
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
setting mailbox_size_limit: 0
setting recipient_delimiter: +
setting inet_interfaces: all
setting inet_protocols: all
WARNING: /etc/aliases exists, but does not have a root alias.

Postfix (main.cf) is now set up with the changes above. If you need to make
changes, edit /etc/postfix/main.cf (and others) as needed. To view Postfix
configuration values, see postconf(1).

After modifying main.cf, be sure to run 'systemctl reload postfix'.

Running newaliases
fillesten@fillesten-VirtualBox:~$

```

Gjorde konfigureringen enligt configuration kapitlet från

(<https://help.ubuntu.com/community/Postfix>)

```

fillesten@fillesten-VirtualBox:~$ sudo postconf -e 'smtpd_sasl_local_domain ='
fillesten@fillesten-VirtualBox:~$ sudo postconf -e 'smtpd_sasl_auth_enable = yes'
fillesten@fillesten-VirtualBox:~$ sudo postconf -e 'smtpd_sasl_security_options = noanonymous'
fillesten@fillesten-VirtualBox:~$ sudo postconf -e 'broken_sasl_auth_clients = yes'
fillesten@fillesten-VirtualBox:~$ sudo postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
fillesten@fillesten-VirtualBox:~$ sudo postconf -e 'inet_interfaces = all'

```

Konfigurerar postfix att utföra smtp auth genom SASL

```

fillesten@fillesten-VirtualBox: ~
File Edit View Search Terminal Help
GNU nano 6.2 /etc/postfix/sasl/smtpd.conf
pwcheck_method: saslauthd
mech_list: plain login

```

Lägger till dessa linjer i smtpd.conf

```

fillesten@fillesten-VirtualBox:~$ sudo nano /etc/postfix/sasl/smtpd.conf'
>
> ^C
fillesten@fillesten-VirtualBox:~$ sudo nano /etc/postfix/sasl/smtpd.conf
fillesten@fillesten-VirtualBox:~$ cd /etc/postfix/
fillesten@fillesten-VirtualBox:/etc/postfix$ ls
dynamicmaps.cf  main.cf  makedefs.out  master.cf.proto  postfix-files.d  post-install
dynamicmaps.cf.d  main.cf.proto  master.cf  postfix-files  postfix-script  sasl
fillesten@fillesten-VirtualBox:/etc/postfix$ touch smtpd.key
touch: cannot touch 'smtpd.key': Permission denied
fillesten@fillesten-VirtualBox:/etc/postfix$ sudo touch smtpd.key
fillesten@fillesten-VirtualBox:/etc/postfix$ chmod 600 smtpd.key
chmod: changing permissions of 'smtpd.key': Operation not permitted
fillesten@fillesten-VirtualBox:/etc/postfix$ sudo chmod 600 smtpd.key
fillesten@fillesten-VirtualBox:/etc/postfix$

fillesten@fillesten-VirtualBox:/etc/postfix/sasl$ sudo touch smtpd.key
fillesten@fillesten-VirtualBox:/etc/postfix/sasl$ sudo openssl genrsa 1024 > smtpd.key
-bash: smtpd.key: Permission denied
fillesten@fillesten-VirtualBox:/etc/postfix/sasl$ sudo openssl genrsa 1024 > sudo smtpd.key
-bash: sudo: Permission denied
fillesten@fillesten-VirtualBox:/etc/postfix/sasl$ sudo mv ~/smtpd.key /etc/postfix/sasl
fillesten@fillesten-VirtualBox:/etc/postfix/sasl$ ls
smtpd.conf  smtpd.key
fillesten@fillesten-VirtualBox:/etc/postfix/sasl$ sudo nano smtpd.key
fillesten@fillesten-VirtualBox:/etc/postfix/sasl$

```

Jag försöker skapa i /sasl men går ej så jag använder bilden nedan och sen fortsätter jag på sudo mv...

2023-11-10. have done more i will send my faulty configurations to appendix A.

2023-11-17, hoppar hit igen försöker från början från <https://help.ubuntu.com/community/Postfix> med generering av TLS encryption

```

root@fillesten-VirtualBox:/etc/ssl# touch smtpd.key
root@fillesten-VirtualBox:/etc/ssl# chmod 600 smtpd.key
root@fillesten-VirtualBox:/etc/ssl# openssl genrsa 1024 > smtpd.key
root@fillesten-VirtualBox:/etc/ssl# ls
certs  openssl.cnf  private  smtpd.key
root@fillesten-VirtualBox:/etc/ssl# sudo nano smtpd.key
root@fillesten-VirtualBox:/etc/ssl# openssl req -new -key smtpd.key -x509 -days 3650 -out smtpd.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SV
State or Province Name (full name) [Some-State]:VN
Locality Name (eg, city) []:Sundsvall
Organization Name (eg, company) [Internet Widgits Pty Ltd]:miun
Organizational Unit Name (eg, section) []:miun
Common Name (e.g. server FQDN or YOUR name) []:fillesten
Email Address []:fillesten@localhost
root@fillesten-VirtualBox:/etc/ssl#
root@fillesten-VirtualBox:/etc/ssl# openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650

```

then

[illegible]

PEM pass phrase: 1234 (in case i need myself for future reference). I didn't write a long enough

```
root@fillesten-VirtualBox:/etc/ssl# sudo mv smtpd.key /etc/ssl/private/
sudo mv smtpd.crt /etc/ssl/certs/
sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/
root@fillesten-VirtualBox:/etc/ssl# ls
certs  openssl.cnf  private
```

now since I used a long enough password it doesn't tell me that cacert.pem doesn't exist.

```

fillesten@fillesten-VirtualBox:/etc/postfix$ sudo postconf -e 'smtp_tls_security_level = may'
sudo postconf -e 'smtpd_tls_security_level = may'
sudo postconf -e 'smtpd_tls_auth_only = no'
sudo postconf -e 'smtp_tls_note_starttls_offer = yes'
sudo postconf -e 'smtpd_tls_key_file = /etc/ssl/private/smtpd.key'
sudo postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt'
sudo postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'
sudo postconf -e 'smtpd_tls_loglevel = 1'
sudo postconf -e 'smtpd_tls_received_header = yes'
sudo postconf -e 'smtpd_tls_session_cache_timeout = 3600s'
sudo postconf -e 'tls_random_source = dev:/dev/urandom'
sudo postconf -e 'myhostname = server1.example.com'
fillesten@fillesten-VirtualBox:/etc/postfix$

```

Konfigurerar TLS enkryptering för både in och utgående mejl. Ändrade myhostname till fillesten@VirtualBox.

```

fillesten@fillesten-VirtualBox: /etc/postfix
File Edit View Search Terminal Help
GNU nano 6.2 main.cf

# TLS parameters
smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt
smtpd_tls_key_file = /etc/ssl/private/smtpd.key
smtpd_tls_security_level = may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level = may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
#myhostname = server1.example.com
#myhostname = fillesten.example.com
#myhostname = example.com
myhostname = fillesten-VirtualBox
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = fillesten-VirtualBox, localhost.localdomain, , localhost, server1.example.com, example.com, localhost.example.com
relayhost =
mynetworks = 127.0.0.0/8
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
home_mailbox = Maildir/
mailbox_command =
smtpd_sasl_local_domain =
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
smtpd_tls_auth_only = no
smtpd_tls_note_starttls_offer = yes
smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom

```

Etc/postfix/main.cf filen:

```

fillesten@fillesten-VirtualBox:/etc/postfix$ sudo /etc/init.d/postfix restart
Restarting postfix (via systemctl): postfix.service.
fillesten@fillesten-VirtualBox:/etc/postfix$

```

Restarter postfix daemonnen.

```

fillesten@fillesten-VirtualBox:/etc/postfix$ sudo apt-get install libsasl2-2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libsasl2-2 is already the newest version (2.1.27+dfsg2-3ubuntu1.2).
libsasl2-2 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 38 not upgraded.
fillesten@fillesten-VirtualBox:/etc/postfix$ sudo apt-get install sasl2-bin

```

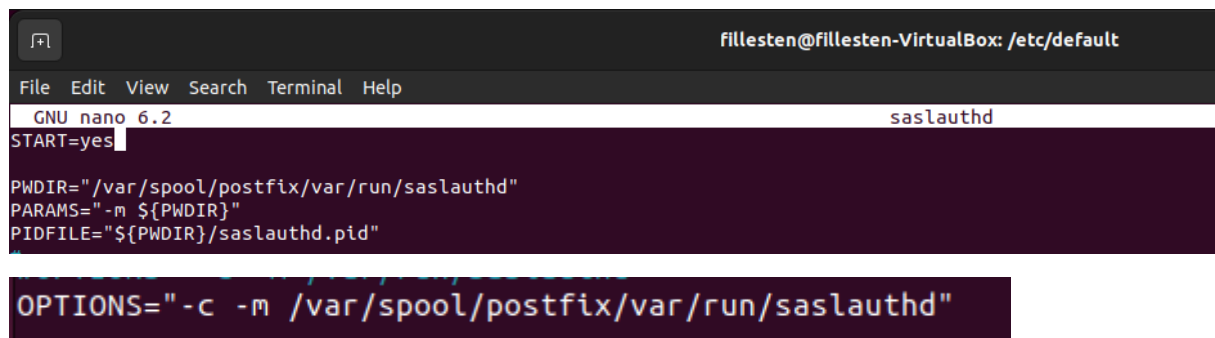
Laddar ner libsassl2-2 och sasl2-bin.

```
fillesten@fillesten-VirtualBox:/etc/postfix$ sudo apt-get install libsassl2-modules
Reading package lists... Done
```

Laddar ner libsassl2-modules.

```
fillesten@fillesten-VirtualBox:/etc/default$ ls
acpid          amd64-microcode  avahi-daemon     dbus            lm-config       kerneloops       networkd-dispatcher  openvpn  saned      useradd
acpi-support   anacron          console-setup    grub            intel-microcode keyboard          nfs-common           rpcbind  saslauthd
alsa           apport           cron             grub.d          irqbalance      locale           nfs-kernel-server    rsync    ufw
fillesten@fillesten-VirtualBox:/etc/default$ sudo nano saslauthd
```

Redigerar saslauthd



```
fillesten@fillesten-VirtualBox: /etc/default
File Edit View Search Terminal Help
GNU nano 6.2 saslauthd
START=yes

PWDIR="/var/spool/postfix/var/run/saslauthd"
PARAMS="-m ${PWDIR}"
PIDFILE="${PWDIR}/saslauthd.pid"

OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"
```

Lade till dessa linjer i saslauthd.

```
fillesten@fillesten-VirtualBox:/etc/default$ sudo dpkg-statoverride --force --update --add root sasl 755 /var/spool/postfix/var/run/saslauthd
dpkg-statoverride: warning: deprecated --force option; use --force-all instead
dpkg-statoverride: warning: --update given but /var/spool/postfix/var/run/saslauthd does not exist
fillesten@fillesten-VirtualBox:/etc/default$
```

"Next, we update the dpkg "state" of /var/spool/postfix/var/run/saslauthd. The saslauthd init script uses this setting to create the missing directory with the appropriate permissions and ownership" (<https://help.ubuntu.com/community/Postfix>)

```
fillesten@fillesten-VirtualBox:/etc/default$ sudo /etc/init.d/saslauthd start
Starting saslauthd (via systemctl): saslauthd.service.
```

Startar saslauthd service.

```

fillesten@fillesten-VirtualBox:~$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 server1.example.com ESMTP Postfix (Ubuntu)
ehlo localhost
250-server1.example.com
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING

```

Testar med telnet localhost 25 och sen ehlo localhost.

250-STARTTLS och 250-AUTH PLAIN LOGIN

### To answer in my report

- What did you have to do, to ensure that your MTA will only relay emails from your local network?

I etc/postfix/main.cf I set the  
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128

Dessutom dessa rader:

smtpd\_relay\_restrictions = permit\_mynetworks permit\_sasl\_authenticated defer\_unauth\_destination

smtpd\_recipient\_restrictions =  
permit\_sasl\_authenticated,permit\_mynetworks,reject\_unauth\_destination

- Discuss why it is important to restrict relaying emails, when it is not suitable to have this restriction.

Restricting relaying emails is important to prevent unauthorised use/spam, to secure the server, retain reputation; other servers can block if the reputation falls enough and to protect sensitive data.

It may be bad to restrict relaying emails if users are using old or legacy systems because they might not support more modern authentication technologies. If there is a shared hosting environment where multiple users share the same mail server. Restricting in this case can hinder sending legitimate emails for users.



## 4.2 DNS

```
fillersten@fillersten-VirtualBox:/$ sudo apt install opendkim opendkim-tools
Reading package lists... Done
```

```
fillersten@fillersten-VirtualBox:/etc$ sudo add-apt-repository universe
```

```
#smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
smtpd_tls_auth_only = no
smtpd_tls_note_starttls_offer = yes
smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom

#dkim
milter_default_action = accept
milter_protocol = 2
smtpd_milters = inet:localhost:8891
non_smtpd_milters = inet:localhost:8891

#spf
policy-spf_time_limit = 3600s

#spf
smtpd_recipient_restrictions =
...
    permit_sasl_authenticated
    permit_mynetworks
    reject_unauth_destination
    check_policy_service unix:private/policy-spf
...
```

etc/postfix/main.cf

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

```
fillersten@fillersten-VirtualBox:/$ sudo snap restart bind9-jdstrand.server
Restarted.
fillersten@fillersten-VirtualBox:/$
```

```
fillersten@fillersten: /var/spool/postfix/etc

File Edit View Search Terminal Help
GNU nano 6.2 hosts
1 127.0.0.1 localhost
2 127.0.1.1 fillersten-VirtualBox
```

Recipient for root and postmaster mail:

**fillesten**

<Ok> <Cancel>

```
fillesten@fillesten-VirtualBox: /etc
GNU nano 6.2                                opendkim.conf

# Signing domain, selector, and key (required). For example, perform signing
# for domain "example.com" with selector "2020" (2020._domainkey.example.com),
# using the private key stored in /etc/dkimkeys/example.private. More granular
# setup options can be found in /usr/share/doc/opendkim/README.opendkim.
Domain                example.com
Selector              mail
KeyFile               /etc/mail/dkim.key
KeyFile               /etc/dkimkeys/example.private
uc# Common settings. See dkim-filter.conf(5) for more information.
ucAutoRestart         yes
ucBackground          yes
Canonicalization      relaxed/relaxed
DNSTimeout            5
riMode                sv
SignatureAlgorithm     rsa-sha256
SubDomains             no
: #UseASPDiscard       no
: #Version              rfc4871
: #X-Header             no
```

```
fillesten@fillesten-VirtualBox: /etc/default
GNU nano 6.2                                opendkim

RUNDIR=/run/opendkim
#
# Uncomment to specify an alternate socket
# Note that setting this will override any Socket value in opendkim.conf
# default:
# -----TESTAR DETTA NUUUUUUUUUUUUUUUUU-----
SOCKET="inet:8891@localhost"
#GAHLLA v
#SOCKET=local:$RUNDIR/opendkim.sock
# listen on all interfaces on port 54321
#SOCKET=inet:54321
```

← NEW  
← before

- Include a screenshot showing your MX, DKIM and SPF-records.

```

fillesten@fillesten-VirtualBox: /var/snap/bind9-jdstrand/current/etc/bind$ cat mcduckcorp.duckburg.calli.db
$TTL 30d
$ORIGIN mcduckcorp.duckburg.calli.
@ IN SOA ns1. mail(
    2023103003 ; serial
    3600       ; refresh
    1800       ; retry
    604800     ; expire
    3600      ; minimum
)
@ IN NS ns1.
ns1 IN A 10.0.2.18
mail IN A 10.0.2.15
fille IN CNAME mail
@ IN MX 10 mail.mcduckcorp.duckburg.calli.
@ IN TXT "v=spf1 a mx -all"

mail._domainkey IN TXT ( "v=DKIM1; h=sha256; k=rsa; t=y; "
    "p=MIIBIjANBgkqhkiG9w0BAQEAFAAOCAQ8AMIIBCgKCAQEAyvm0gNyl/2RbSF5NQAAMsCdGZBj0BZs3A9NkVN+NX5xIagBBBjBMfk1ntKLXsvBxuiXg+VMJAb+7BfQZ37tM1rAPQTYiZi9tnEp9vcOC8g653zscpp
    /dsIoutwLlTq1ogATFFv4tyBkIQsEkvs0/XXRqr9DVTj4HyLheRy+vNYIFRfKpbuE05GzVogZqQvN7H28cpQGb2AyBKn"
    "2vcebaOKT4LizZeOkRncX39011j7NMULVAHRldz8DzRpvZpMQLD24hUAOTyAPH2/f3NOx9hldbDANS1iInZekGJ7L4Gagxh0MdsVZsXN5a64/bhwHvWIS3r8kGcqM/oBRaTuzBwIDAQAB" ) ; ----- DKIM
    key mail for ubuntu.ro
fillesten@fillesten-VirtualBox: /var/snap/bind9-jdstrand/current/etc/bind$

```

```

MX: @ IN MX 10 mail.mcduckcorp.duckburg.calli.
DKIM: mail._domainkey in TXT (...); ----- DKIM key mail for ubuntu.ro
SPF: @ IN TXT "v=spf1 a mx -all"

```

- Include a screenshot showing the full header of the email that you sent, to show that DKIM works properly.

```

fillesten@fillesten:/etc$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 fillesten ESMTP Postfix (Ubuntu)
mail from: fillesten@localhost
250 2.1.0 Ok
rcpt to: donald@localhost
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: qwer
mailname = localhost, domain in etc/openssl.conf = localhost
.
250 2.0.0 Ok: queued as D5E351C33FC
quit
221 2.0.0 Bye
Connection closed by foreign host.
fillesten@fillesten:/etc$

```

```

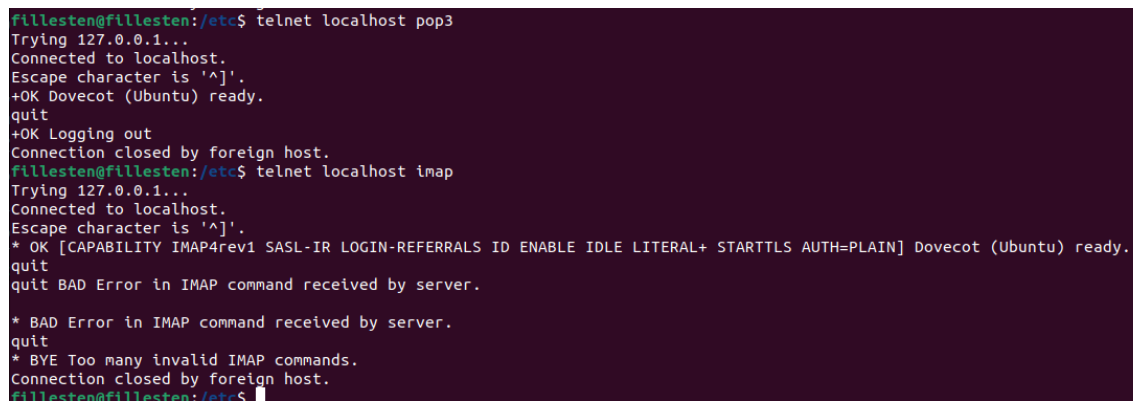
donald@fillesten: ~/Maildir/new$ cat 1700570625.V803Ia0ca3M909218.fillesten
Return-Path: <fillesten@localhost>
X-Original-To: donald@localhost
Delivered-To: donald@localhost
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=localhost; s=mail;
    t=1700570625; bh=mNiqGt1f0H2YgZbuG/LYEasVJbzzITr9R4fXfmevuxs=;
    h=subject:Date:From:From;
    b=mLLlWbyiYyvt3i8COfSCypw/Ea0hTdiq9LcyMtsaOK/Cx4ZYQwI3pQNfaj36hbDn
    UxXYuDBXYvmKYzE6CplXlOWWL4JJHIE3MtU4b3INo9PbtLOsaST8dRpwDkKFNO4TKd
    rijdhTX9turVhg17kMwslojd/Br7ywZ6yPl3ZCok41Q/RxAcMtpbg8CS/wQm7Vmej0
    KJ8Wt0Z/vc0r8hqpIQR1GP9xd3E0cqXhSp4656Sp0Y7bG/Z/XDItt06EO+uB8DY1kw
    SwLlD5gtzXgUleS0Jcev+uDUTFe5NwJhuEXik4R8YRpXM7gd1NXQS4RUyzThYuf9PS
    gGVZnlbRcGgEw==
Received: from localhost (localhost [127.0.0.1])
    by fillesten (Postfix) with SMTP id D5E351C33FC
    for <donald@localhost>; Tue, 21 Nov 2023 13:42:55 +0100 (CET)
subject: qwer
Message-Id: <20231121124259.D5E351C33FC@fillesten>
Date: Tue, 21 Nov 2023 13:42:55 +0100 (CET)
From: fillesten@localhost

mailname = localhost, domain in etc/openssl.conf = localhost
donald@fillesten: ~/Maildir/new$

```

## 4.3 Access Agents

- Include a screenshot showing that your AA is working properly.



```
fillesten@fillesten:/etc$ telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK Dovecot (Ubuntu) ready.
quit
+OK Logging out
Connection closed by foreign host.
fillesten@fillesten:/etc$ telnet localhost imap
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ STARTTLS AUTH=PLAIN] Dovecot (Ubuntu) ready.
quit
quit BAD Error in IMAP command received by server.

* BAD Error in IMAP command received by server.
quit
* BYE Too many invalid IMAP commands.
Connection closed by foreign host.
fillesten@fillesten:/etc$
```

- Include a screenshot showing that SSL is working as it should.

```
fillesten@fillesten:/etc$ openssl s_client -showcerts -connect localhost:995 -servername localhost
CONNECTED(00000003)
depth=0 CN = ubuntu
verify return:1
---
Certificate chain
 0 s:CN = ubuntu
  i:CN = ubuntu
  a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
  v:NotBefore: Oct 22 10:38:36 2023 GMT; NotAfter: Oct 19 10:38:36 2033 GMT
-----BEGIN CERTIFICATE-----
MIIC7zCCAdegAwIBAgIU8u5gU2d+Yyyn//K84+UQbo6LZrAwDQYJKoZIhvcNAQEL
BQAwETEPMA0GA1UEAwGdWJ1bnR1MB4XDTIzMTAyMjEwMzgzNLoXDTMzMTAxOTEx
MzgzNlowETEPMA0GA1UEAwGdWJ1bnR1MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBChgKCAQEAoB3zU5DnE/SWkPUE/gE7khj5TRmzh7I2VwwhSEW5iWAAVD6oL9YV
u3RqQ1+SUNN7gdLSmXUA+F+HtOoyCX0upGGJQ9AzhVv75ere07RaVXwzrjApmh
82hRBIEYCA0y1nF2qZWbPIIRwDx1pVAbnsRcXk0AT2oG1tBzFpBw+2hzLZVgQxBp
3yr1ky0Q1I6ob9rYW0x1JCxBckbMc0tTjpKSegDLL9aysy0bmkbmFQHwr0uBmzFB
ucDTpVpHqe0U1jwbrCGc12F9S8PqUNpBR/zDu1IeV7ATbZ0qVKU8/IA9dwtn9T83
wsiv6qh3Ws+0tUtA9DQA5yRrhwhAae9F5QIDAQABoz8wPTAJBgNVHRMEAjaAMBEG
A1UDEQQKMAiCBnVidw50dAdBgNVHQ4EFgQU4ixX/yaZykY3qnnFlf8/N4QdQYw
DQYJKoZIhvcNAQELBQADggEBAJI76XxrPlQFz2cnDoErqqDgvEGTsJxfYodJ2Y2k
zXevRpoeqMjaDlIsVjIgEf/XCx8u7iV2va7W+76eoRX+4qSUVuegJXh3p5HQReF0
a0qUETA8H8pG72Fv+bPT1gNwdQt3EZuA63Pz0xk0KUIh0y2/+ZZtI6dk4qswIdZP
BTQkTDf6Lgf7CUEo7MN1t9c+L5HenDU4VRztUt7Uamk0S65P9GsJv1DvxHzJ0gJ7
U3P8Mcm/jac/iWNPYRWSFjoGKgFudT7vc0+3PYtb7GZBR8knfFLkhUCG/11XBDUu
7tHmb2ssRtFFwK+ynLxaXX3GjZsuDqmrdu4JbGomM49ZfV4=
-----END CERTIFICATE-----
---
Server certificate
subject=CN = ubuntu
issuer=CN = ubuntu
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1315 bytes and written 391 bytes
Verification: OK
```

```

SSL handshake has read 1315 bytes and written 391 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol : TLSv1.3
    Cipher : TLS_AES_256_GCM_SHA384
    Session-ID: D6857ABEC1FCF2EC2B8B24F8FF61BF80194F66DF38C1BD7ED9504C4EACACD2D3
    Session-ID-ctx:
    Resumption PSK: 98A3BB018B86ECAD5D6A71A90607F9B70C46B9A89E2A177789DAB0D09D95E4A21515F5EE0CA17A237E85C40608D2A59D
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
0000 - ed 37 e3 ca be 39 6a ff-e8 6d c7 e3 8f 8c 5f 6f .7...9j..m...._o
0010 - df 05 0e a4 4a ab ce a8-d5 58 32 e0 dd ee 5d b8 ....J....X2...].
0020 - 15 11 98 3c b7 27 35 74-b9 5c b0 20 12 27 31 a8 ...<.'5t.\. .'1.
0030 - c7 a0 0e f1 30 48 1d 47-5e 57 0e 7d 24 89 7a 20 ....0H.G^W.)$.z
0040 - 85 86 05 60 ad 38 8b 3c-1e c3 5c b9 ed 47 a0 ef ...'.8.<...\..G..
0050 - 7c b1 96 00 a6 ed 51 bf-42 b7 dc c4 0e ed 9e d6 |.....Q.B.....
0060 - 60 68 7f 16 da 91 4a 8f-04 c4 7f 0f 8c 47 e9 7c `h....J.....G.|
0070 - e8 e0 64 49 06 0d a0 c9-e9 cf 50 a7 52 84 f5 d6 ..dI.....P.R...
0080 - bc 3b 2b fd 4a 35 d4 01-5d 94 3a c7 d6 41 e1 28 .;+.J5..]....A.(
0090 - 00 70 da 18 05 3f 4b 09-f5 c0 07 db b4 d6 26 44 .p...?K.....&D
00a0 - a3 7a 4c 48 3e 1f 0a ec-36 fc 2f 90 40 72 11 8b .zLH>...6./..@r..
00b0 - ba fa a0 a4 ce 04 89 7b-9c e8 ac fd 2c f0 fa f8 .....{.....,....
00c0 - 52 55 e5 fc cf 4d e4 b6-74 ef f9 26 5f 47 43 7e RU...M..t...&_GC~

    Start Time: 1700683981
    Timeout : 7200 (sec)
    Verify return code: 0 (ok)

```

```

    Timeout : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol : TLSv1.3
    Cipher : TLS_AES_256_GCM_SHA384
    Session-ID: 9F1F3012B638331DBE8F647CC3D3B7F1E015D2249607A324F6FA57C092057C45
    Session-ID-ctx:
    Resumption PSK: 2EF9E3DB8FF1DD4A839F1906AA55F3088E918BBC1B0F0CD22F5037E1EF4B44161A38858FACBCFB88EEBD10EDB8130FDF
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
0000 - ed 37 e3 ca be 39 6a ff-e8 6d c7 e3 8f 8c 5f 6f .7...9j..m...._o
0010 - 98 e9 d6 92 5e 1d 3d 58-34 da ab e5 58 29 a0 4c ....^.=X4...X).L
0020 - 97 89 d7 23 dc 7d d3 54-64 99 64 f4 bb 79 f3 82 ...#.}.Td.d..y..
0030 - ae 04 da 89 4a 11 38 70-ae d1 c8 6f 83 7e b8 02 ...J.8p...o.~..
0040 - 73 18 ed 5a 73 e3 cd 47-fc 8a d7 3b 00 3f 2d ce s..Zs..G...;?-.
0050 - 41 d3 a9 9f 41 40 1f be-b8 3b 26 fb 12 1f 1a 22 A...A@...;&...."
0060 - 3e d8 fa bd d6 2a 32 ff-52 c3 90 80 4e 53 35 a2 >....*2.R...NS5.
0070 - 96 55 df ea 5e ae 4f dc-b3 3b 6a aa 06 a7 2c c8 .U..^..0...;j....,
0080 - 30 f1 3b 92 f0 33 49 b8-67 56 65 ca 8c 23 4b a6 0.;..3I.gVe..#K.
0090 - 32 13 32 ee b1 b6 b5 23-29 61 7e 53 d5 d2 06 a4 2.2....#)a~S....
00a0 - 31 3d e2 51 df c8 71 89-3e 61 10 12 51 36 8d 3d 1=.Q...q.>a...Q6.=
00b0 - ff bc c2 dc e9 3a 8b 65-32 10 da c3 a1 1a 94 db .....:e2.....
00c0 - c5 4e 52 98 85 25 7b be-01 3b ff c8 11 b3 f4 59 .NR...%[...;....Y

    Start Time: 1700683981
    Timeout : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
+OK Dovecot (Ubuntu) ready.

```