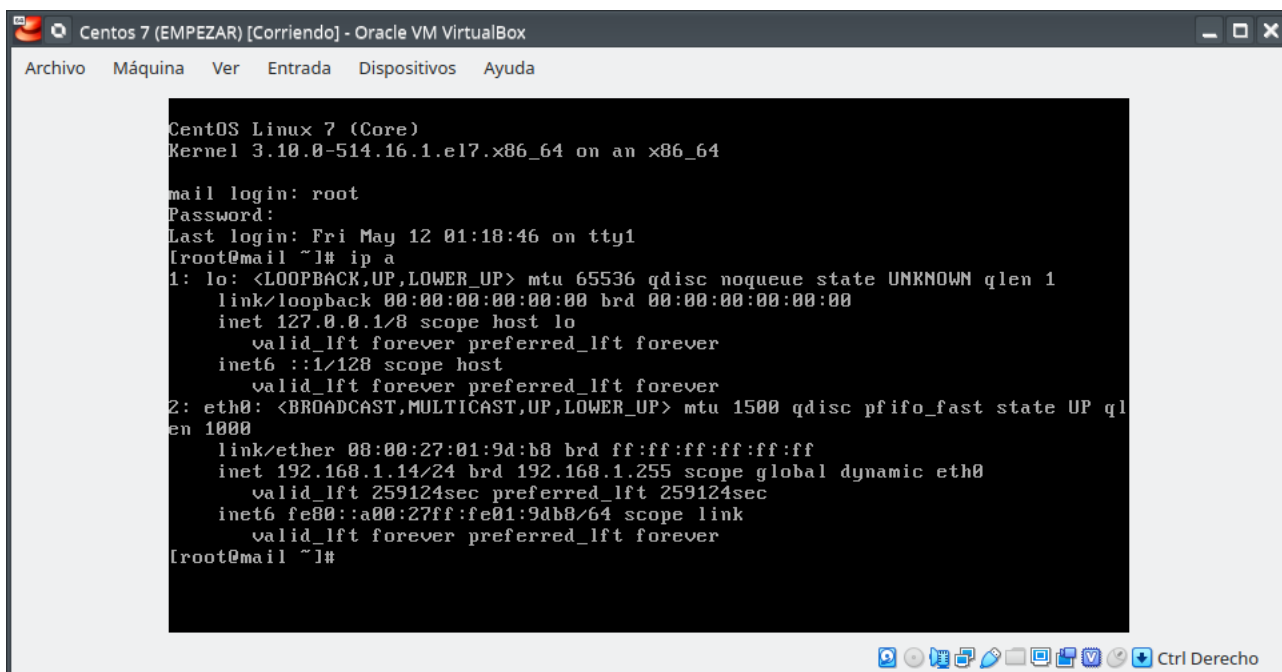


Antivirus y antispam en servidor de correo corporativo

Lo primero de todo descargaremos la maquina de la Classroom de Google la importaremos a nuestro Virtualbox, seguidamente en la configuración de red la pondremos en modo puente e iniciamos.

Entraremos con root y comprobamos que ip le ha asignado.

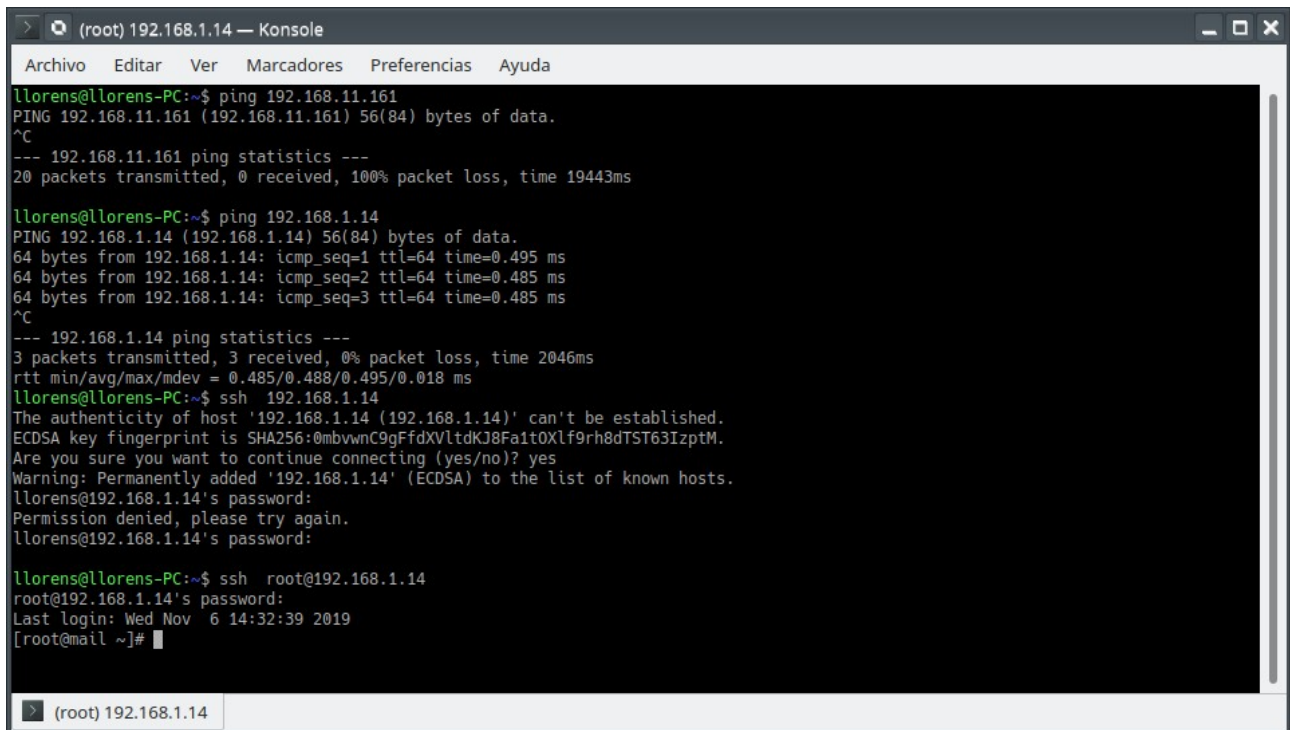


```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.16.1.el7.x86_64 on an x86_64

mail login: root
Password:
Last login: Fri May 12 01:18:46 on tty1
[root@mail ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 08:00:27:01:9d:b8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.14/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 259124sec preferred_lft 259124sec
    inet6 fe80::a00:27ff:fe01:9db8/64 scope link
        valid_lft forever preferred_lft forever
[root@mail ~]#
```

Antivirus y antispam en servidor de correo corporativo

Una vez que sabemos la ip de la maquina podremos acceder desde la maquina anfitriona (mi pc) y desde una terminal iniciamos sesión con SSH



```
(root) 192.168.1.14 — Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

llorens@llorens-PC:~$ ping 192.168.11.161
PING 192.168.11.161 (192.168.11.161) 56(84) bytes of data.
^C
--- 192.168.11.161 ping statistics ---
20 packets transmitted, 0 received, 100% packet loss, time 19443ms

llorens@llorens-PC:~$ ping 192.168.1.14
PING 192.168.1.14 (192.168.1.14) 56(84) bytes of data.
64 bytes from 192.168.1.14: icmp_seq=1 ttl=64 time=0.495 ms
64 bytes from 192.168.1.14: icmp_seq=2 ttl=64 time=0.485 ms
64 bytes from 192.168.1.14: icmp_seq=3 ttl=64 time=0.485 ms
^C
--- 192.168.1.14 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2046ms
rtt min/avg/max/mdev = 0.485/0.488/0.495/0.018 ms
llorens@llorens-PC:~$ ssh 192.168.1.14
The authenticity of host '192.168.1.14 (192.168.1.14)' can't be established.
ECDSA key fingerprint is SHA256:0mbvwnC9gFfdXVltdKJ8Fa1t0Xlf9rh8dTST63IzptM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.14' (ECDSA) to the list of known hosts.
llorens@192.168.1.14's password:
Permission denied, please try again.
llorens@192.168.1.14's password:

llorens@llorens-PC:~$ ssh root@192.168.1.14
root@192.168.1.14's password:
Last login: Wed Nov  6 14:32:39 2019
[root@mail ~]#
```

Seguimos el tutorial de la web que indica la practica

https://www.server-world.info/en/note?os=CentOS_7&p=mail&f=6

Para no atiborrar este documento en capturas de instalación pongo primero los copia/pega que le pongo a la sesion de SSH

Instalacion Clamav, actualizacion y “scaneo” a lo ultimo si nos fijamos según el tutorial a lo ultimo se descarga Eicar que es el mismo de la practica anterior para comprobar su efectividad. Dejo comandos y la ultima captuta del escaneo donde localiza la infeccion de Eicar.

`yum --enablerepo=epel -y install clamav clamav-update`

`sed -i -e "s/^Example/#Example/" /etc/freshclam.conf`

`freshclam`

`clamscan --infected --remove --recursive /home`

`curl -O http://www.eicar.org/download/eicar.com`

`clamscan --infected --remove --recursive .`

Antivirus y antispam en servidor de correo corporativo

```
llorens: bash — Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

Instalando : clamav-0.101.4-1.el7.x86_64 6/6
Comprobando : pcre2-10.23-2.el7.x86_64 1/6
Comprobando : clamav-lib-0.101.4-1.el7.x86_64 2/6
Comprobando : clamav-filesystem-0.101.4-1.el7.noarch 3/6
Comprobando : clamav-0.101.4-1.el7.x86_64 4/6
Comprobando : libtool-ltdl-2.4.2-22.el7_3.x86_64 5/6
Comprobando : clamav-update-0.101.4-1.el7.x86_64 6/6

Instalado:
clamav.x86_64 0:0.101.4-1.el7 clamav-update.x86_64 0:0.101.4-1.el7

Dependencia(s) instalada(s):
clamav-filesystem.noarch 0:0.101.4-1.el7 clamav-lib.x86_64 0:0.101.4-1.el7 libtool-ltdl.x86_64 0:2.4.2-22.el7_3
pcre2.x86_64 0:10.23-2.el7

¡Listo!
[root@mail ~]# sed -i -e "s/^Example/#Example/" /etc/freshclam.conf
[root@mail ~]# freshclam
ClamAV update process started at Thu Nov 7 01:15:09 2019
Downloading main.cvd [100%]
main.cvd updated (version: 58, sigs: 4566249, f-level: 60, builder: sigmgr)
Downloading daily.cvd [100%]
daily.cvd updated (version: 25625, sigs: 1974998, f-level: 63, builder: raynman)
Downloading bytecode.cvd [100%]
bytecode.cvd updated (version: 331, sigs: 94, f-level: 63, builder: anvilleg)
Database updated (6541341 signatures) from database.clamav.net (IP: 104.16.219.84)
[root@mail ~]# clamscan --infected --remove --recursive /home

----- SCAN SUMMARY -----
Known viruses: 6530258
Engine version: 0.101.4
Scanned directories: 12
Scanned files: 15
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 54.467 sec (0 m 54 s)
[root@mail ~]# curl -O http://www.eicar.org/download/eicar.com
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 68 100 68 0 0 36 0 0:00:01 0:00:01 --:--:-- 36
[root@mail ~]# clamscan --infected --remove --recursive .
./eicar.com: Eicar-Test-Signature FOUND
./eicar.com: Removed.

----- SCAN SUMMARY -----
Known viruses: 6530258
Engine version: 0.101.4
Scanned directories: 3
Scanned files: 11
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 1.00:1)
Time: 49.611 sec (0 m 49 s)
[root@mail ~]#
```

Antivirus y antispam en servidor de correo corporativo

Instalacion y configuracion de Amavisd y Clamav Server.

`yum --enablerepo=epel -y install amavisd-new clamav-scanner clamav-scanner-systemd`

`setsebool -P antivirus_can_scan_system on`

`vi /etc/amavisd/amavisd.conf`

```
$mydomain = 'cursoseg.lan'; # a convenient default for other settings
```

```
# OTHER MORE COMMON SETTINGS (defaults may suffice):  
$myhostname = 'mail.cursoseg.lan'; # must be a fully-qualified domain name!
```

descomentar

```
$notify_method = 'smtp:[127.0.0.1]:10025';  
$forward_method = 'smtp:[127.0.0.1]:10025'; # set to undef with militer!
```

descomentar

```
['ClamAV-clamd-stream',  
 \&ask_daemon, ["*", 'clamd:/var/run/clamav/clamd.sock'],  
 qr/\bOK$/m, qr/\bFOUND$/m,  
 qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
```

Guardamos que por cierto nunca viene nada mal el recordar como funciona VI estoy acostumbrado al editor NANO.

Antivirus y antispam en servidor de correo corporativo

Seguiremos metiendo comandos del tutorial

`systemctl start clamd@amavisd amavisd spamassassin`

`systemctl enable clamd@amavisd amavisd spamassassin`

```
llorens : bash — Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

perl-DBD-SQLite.x86_64 0:1.39-3.el7
perl-DB_File.x86_64 0:1.830-6.el7
perl-Digest.noarch 0:1.17-245.el7
perl-Digest-MD5.x86_64 0:2.52-3.el7
perl-Digest-SHA1.x86_64 0:2.13-9.el7
perl-Encode-Locale.noarch 0:1.03-5.el7
perl-ExtUtils-Install.noarch 0:1.58-294.el7_6
perl-ExtUtils-Manifest.noarch 0:1.61-244.el7
perl-File-Listing.noarch 0:6.04-7.el7
perl-HTML-Parser.x86_64 0:3.71-4.el7
perl-HTTP-Cookies.noarch 0:6.01-5.el7
perl-HTTP-Date.noarch 0:6.02-8.el7
perl-HTTP-Negotiate.noarch 0:6.01-5.el7
perl-IO-HTML.noarch 0:1.00-2.el7
perl-IO-Socket-INET6.noarch 0:2.69-5.el7
perl-IO-Socket-SSL.noarch 0:1.94-7.el7
perl-IO-stringy.noarch 0:2.110-22.el7
perl-LDAP.noarch 1:0.56-6.el7
perl-MIME-tools.noarch 0:5.505-1.el7
perl-Mail-SPF.noarch 0:2.8-0-4.el7
perl-Mozilla-CA.noarch 0:20130114-5.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-Net-LibIDN.x86_64 0:0.12-15.el7
perl-Net-SSLey.x86_64 0:1.55-6.el7
perl-NetAddr-IP.x86_64 0:4.069-3.el7
perl-PLRPC.noarch 0:0.2020-14.el7
perl-Socket6.x86_64 0:0.23-15.el7
perl-Test-Harness.noarch 0:3.28-3.el7
perl-Text-Unidecode.noarch 0:0.04-20.el7
perl-URI.noarch 0:1.60-9.el7
perl-WWW-RobotRules.noarch 0:6.02-5.el7
perl-XML-NamespacesSupport.noarch 0:1.11-10.el7
perl-XML-SAX-Writer.noarch 0:0.53-4.el7
perl-libwww-perl.noarch 0:6.05-2.el7
portreserve.x86_64 0:0.0.5-11.el7
psmisc.x86_64 0:22.20-16.el7
spamassassin.x86_64 0:3.4.0-4.el7_5
tmpwatch.x86_64 0:2.11-6.el7

perl-DBI.x86_64 0:1.627-4.el7
perl-Data-Dumper.x86_64 0:2.145-3.el7
perl-Digest-HMAC.noarch 0:1.03-5.el7
perl-Digest-SHA.x86_64 1:5.85-4.el7
perl-Encode-Detect.x86_64 0:1.01-13.el7
perl-Error.noarch 1:0.17020-2.el7
perl-ExtUtils-MakeMaker.noarch 0:6.68-3.el7
perl-ExtUtils-ParseXS.noarch 1:3.18-3.el7
perl-GSSAPI.x86_64 0:0.28-9.el7
perl-HTML-Tagset.noarch 0:3.20-15.el7
perl-HTTP-Daemon.noarch 0:6.01-8.el7
perl-HTTP-Message.noarch 0:6.06-6.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-IO-Multiplex.noarch 0:1.13-6.el7
perl-IO-Socket-IP.noarch 0:0.21-5.el7
perl-IO-Zlib.noarch 1:1.10-294.el7_6
perl-JSON.noarch 0:2.59-2.el7
perl-LWP-MediaTypes.noarch 0:6.02-2.el7
perl-Mail-DKIM.noarch 0:0.39-8.el7
perl-MailTools.noarch 0:2.12-2.el7
perl-Net-DNS.x86_64 0:0.72-6.el7
perl-Net-HTTP.noarch 0:6.06-2.el7
perl-Net-SMTP-SSL.noarch 0:1.01-13.el7
perl-Net-Server.noarch 0:2.007-2.el7
perl-Package-Constants.noarch 1:0.02-294.el7_6
perl-Razor-Agent.x86_64 0:2.85-15.el7
perl-Sys-Syslog.x86_64 0:0.33-3.el7
perl-Text-Soundex.x86_64 0:3.04-4.el7
perl-TimeDate.noarch 1:2.30-2.el7
perl-Unix-Syslog.x86_64 0:1.1-17.el7
perl-XML-Filter-BufferText.noarch 0:1.01-17.el7
perl-XML-SAX-Base.noarch 0:1.08-7.el7
perl-devel.x86_64 4:5.16.3-294.el7_6
perl-version.x86_64 3:0.99.07-3.el7
procmail.x86_64 0:3.22-36.el7_4.1
pyparsing.noarch 0:1.5.6-9.el7
systemtap-sdt-devel.x86_64 0:4.0-10.el7_7
unzoo.x86_64 0:4.4-16.el7

Dependencia(s) actualizada(s):
glibc.x86_64 0:2.17-292.el7 glibc-common.x86_64 0:2.17-292.el7 libdb.x86_64 0:5.3.21-25.el7 libdb-utils.x86_64 0:5.3.21-25.el7

¡Listo!
[root@mail ~]# vi /etc/amavisd/amavisd.conf
[root@mail ~]# start clamd@amavisd amavisd spamassassin
-bash: start: no se encontró la orden
[root@mail ~]# systemctl start clamd@amavisd amavisd spamassassin
[root@mail ~]# enable clamd@amavisd amavisd spamassassin
-bash: enable: clamd@amavisd: no es una orden interna del shell
-bash: enable: amavisd: no es una orden interna del shell
-bash: enable: spamassassin: no es una orden interna del shell
[root@mail ~]# systemctl enable clamd@amavisd amavisd spamassassin
Created symlink from /etc/systemd/system/multi-user.target.wants/amavisd.service to /usr/lib/systemd/system/amavisd.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/spamassassin.service to /usr/lib/systemd/system/spamassassin.servic
e.
[root@mail ~]#
```

Una captura para mostrar el proceso

Antivirus y antispam en servidor de correo corporativo

Configurar Postfix

[`vi /etc/postfix/main.cf`](#)

añadimos “`content_filter=smtp-amavis:[127.0.0.1]:10024`”

Editaremos tambien

[`vi /etc/postfix/master.cf`](#)

añadiendo las siguientes lineas

```
smtp-amavis unix -      -      n      -      2 smtp
-o smtp_data_done_timeout=1200
-o smtp_send_xforward_command=yes
-o disable_dns_lookups=yes
127.0.0.1:10025 inet n      -      n      -      - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
```

Antivirus y antispam en servidor de correo corporativo

Y seguidamente reiniciaremos Postfix y te puedo enseñar su estado actual.

```
llorens: bash — Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

perl-NetAddr-IP.x86_64 0:4.069-3.el7
perl-PLRPC.noarch 0:0.2020-14.el7
perl-Socket6.x86_64 0:0.23-15.el7
perl-Test-Harness.noarch 0:3.28-3.el7
perl-Text-Unidecode.noarch 0:0.04-20.el7
perl-URI.noarch 0:1.60-9.el7
perl-WWW-RobotRules.noarch 0:6.02-5.el7
perl-XML-NamespacesSupport.noarch 0:1.11-10.el7
perl-XML-SAX-Writer.noarch 0:0.53-4.el7
perl-libwww-perl.noarch 0:6.05-2.el7
portreserve.x86_64 0:0.0.5-11.el7
psmisc.x86_64 0:22.20-16.el7
spamassassin.x86_64 0:3.4.0-4.el7_5
tmpwatch.x86_64 0:2.11-6.el7
perl-Package-Constants.noarch 1:0.02-294.el7_6
perl-Razor-Agent.x86_64 0:2.85-15.el7
perl-Sys-Syslog.x86_64 0:0.33-3.el7
perl-Text-Soundex.x86_64 0:3.04-4.el7
perl-TimeDate.noarch 1:2.30-2.el7
perl-Unix-Syslog.x86_64 0:1.1-17.el7
perl-XML-Filter-BufferText.noarch 0:1.01-17.el7
perl-XML-SAX-Base.noarch 0:1.08-7.el7
perl-devel.x86_64 4:5.16.3-294.el7_6
perl-version.x86_64 3:0.99.07-3.el7
procmail.x86_64 0:3.22-36.el7_4.1
pyparsing.noarch 0:1.5.6-9.el7
systemtap-sdt-devel.x86_64 0:4.0-10.el7_7
unzoo.x86_64 0:4.4-16.el7

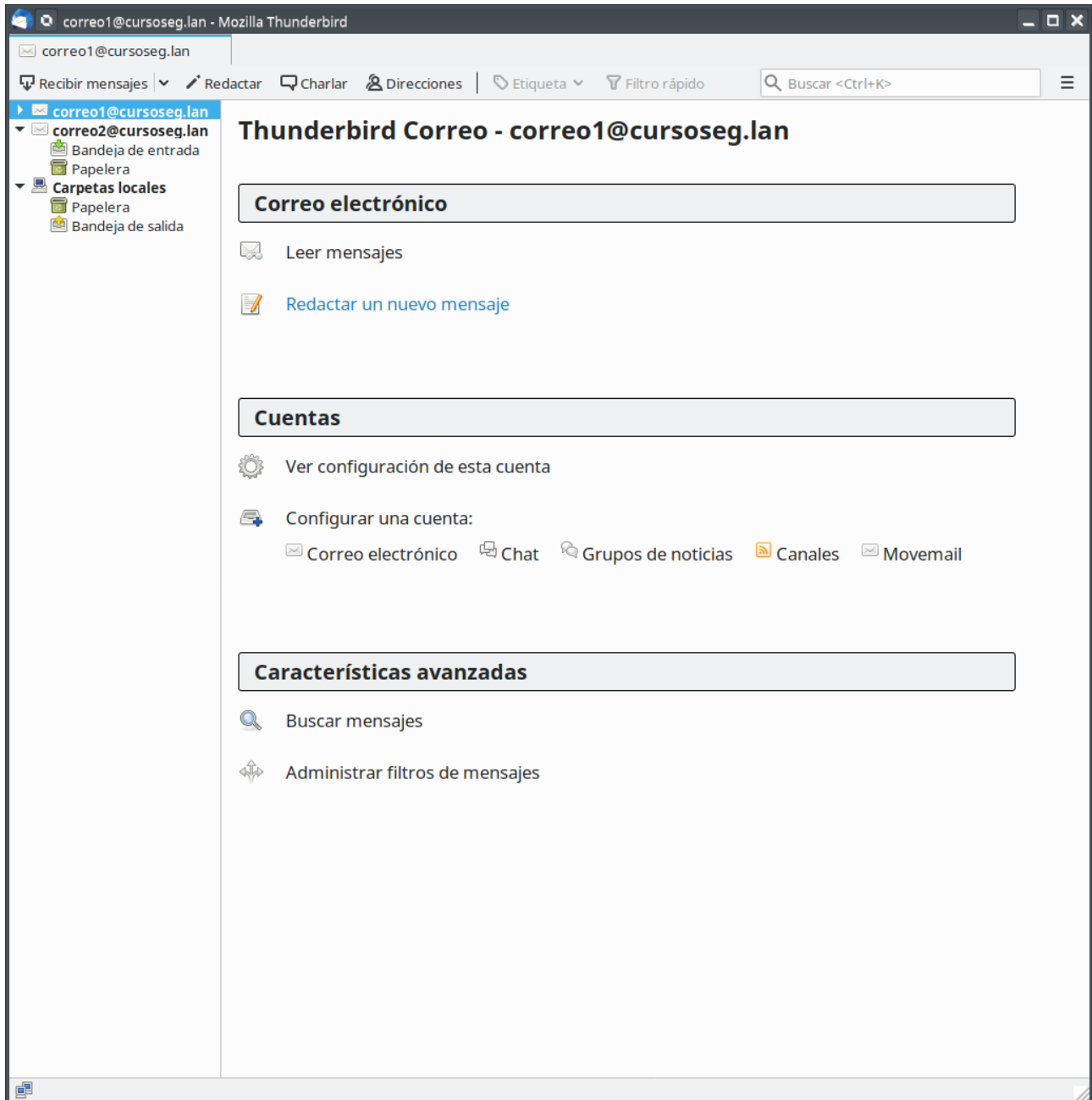
Dependencia(s) actualizada(s):
glibc.x86_64 0:2.17-292.el7 glibc-common.x86_64 0:2.17-292.el7 libdb.x86_64 0:5.3.21-25.el7 libdb-utils.x86_64 0:5.3.21-25.el7

¡Listo!
[root@mail ~]# vi /etc/amavisd/amavisd.conf
[root@mail ~]# start clamd@amavisd amavisd spamassassin
-bash: start: no se encontró la orden
[root@mail ~]# systemctl start clamd@amavisd amavisd spamassassin
[root@mail ~]# enable clamd@amavisd amavisd spamassassin
-bash: enable: clamd@amavisd: no es una orden interna del shell
-bash: enable: amavisd: no es una orden interna del shell
-bash: enable: spamassassin: no es una orden interna del shell
[root@mail ~]# systemctl enable clamd@amavisd amavisd spamassassin
Created symlink from /etc/systemd/system/multi-user.target.wants/amavisd.service to /usr/lib/systemd/system/amavisd.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/spamassassin.service to /usr/lib/systemd/system/spamassassin.service.
[root@mail ~]# vi /etc/postfix/main.cf
[root@mail ~]# vi /etc/postfix/main.cf
[root@mail ~]# vi /etc/postfix/main.cf
[root@mail ~]# vi /etc/postfix/main.cf
main.cf master.cf
[root@mail ~]# vi /etc/postfix/master.cf
[root@mail ~]# systemctl restart postfix
[root@mail ~]# systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; vendor preset: disabled)
   Active: active (running) since jue 2019-11-07 02:27:03 CET; 7s ago
     Process: 2721 ExecStop=/usr/sbin/postfix stop (code=exited, status=0/SUCCESS)
     Process: 2738 ExecStart=/usr/sbin/postfix start (code=exited, status=0/SUCCESS)
     Process: 2736 ExecStartPre=/usr/libexec/postfix/chroot-update (code=exited, status=0/SUCCESS)
     Process: 2734 ExecStartPre=/usr/libexec/postfix/aliasesdb (code=exited, status=0/SUCCESS)
   Main PID: 2811 (master)
     CGroup: /system.slice/postfix.service
            └─2811 /usr/libexec/postfix/master -w
              └─2812 pickup -l -t unix -u
                └─2813 qmgr -l -t unix -u

nov 07 02:27:03 mail.curoseglan systemd[1]: Starting Postfix Mail Transport Agent...
nov 07 02:27:03 mail.curoseglan postfix/master[2811]: daemon started -- version 2.10.1, configuration /etc/postfix
nov 07 02:27:03 mail.curoseglan systemd[1]: Started Postfix Mail Transport Agent.
[root@mail ~]#
```

Antivirus y antispam en servidor de correo corporativo

Seguidamente desde Thunderbird de mi equipo (Tengo Kubuntu) configuramos las cuentas y quedaría una cosa así.

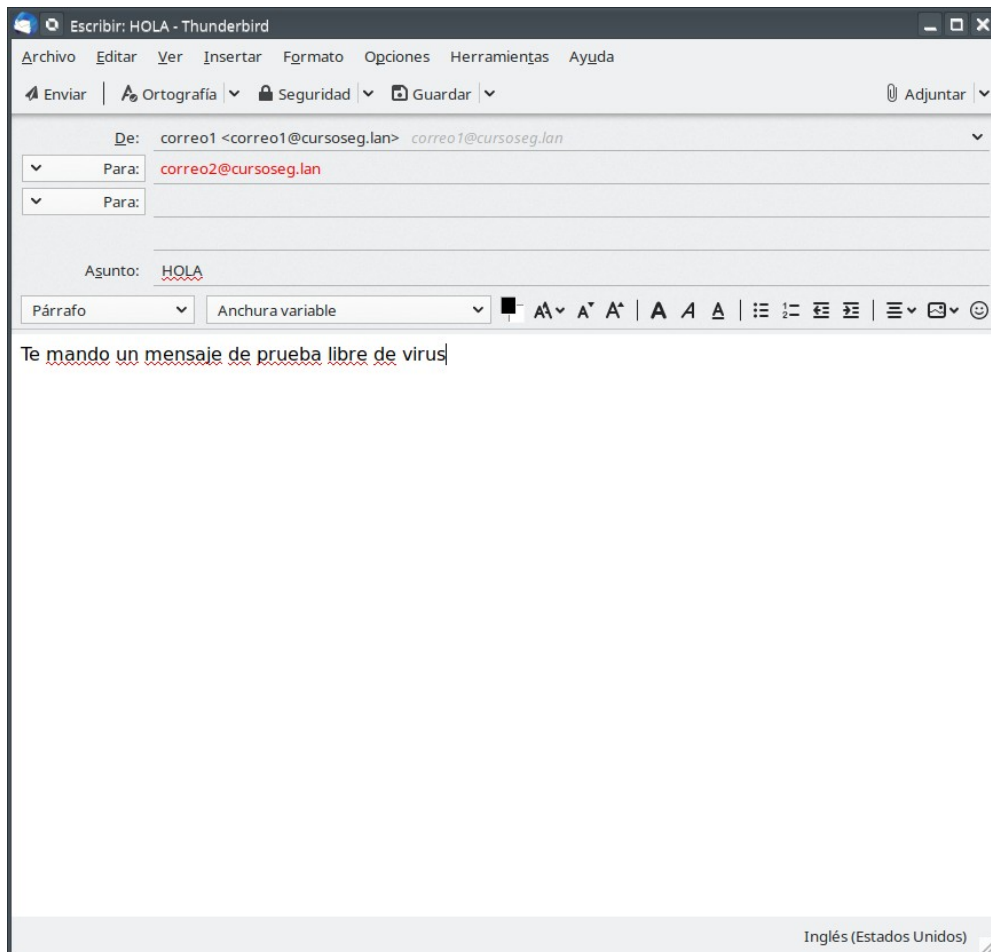


Antivirus y antispam en servidor de correo corporativo

Después ya realizaremos el propósito de la prueba que es mandar un virus de prueba “Eicar” y comprobar que el servidor de correo lo bloquee.

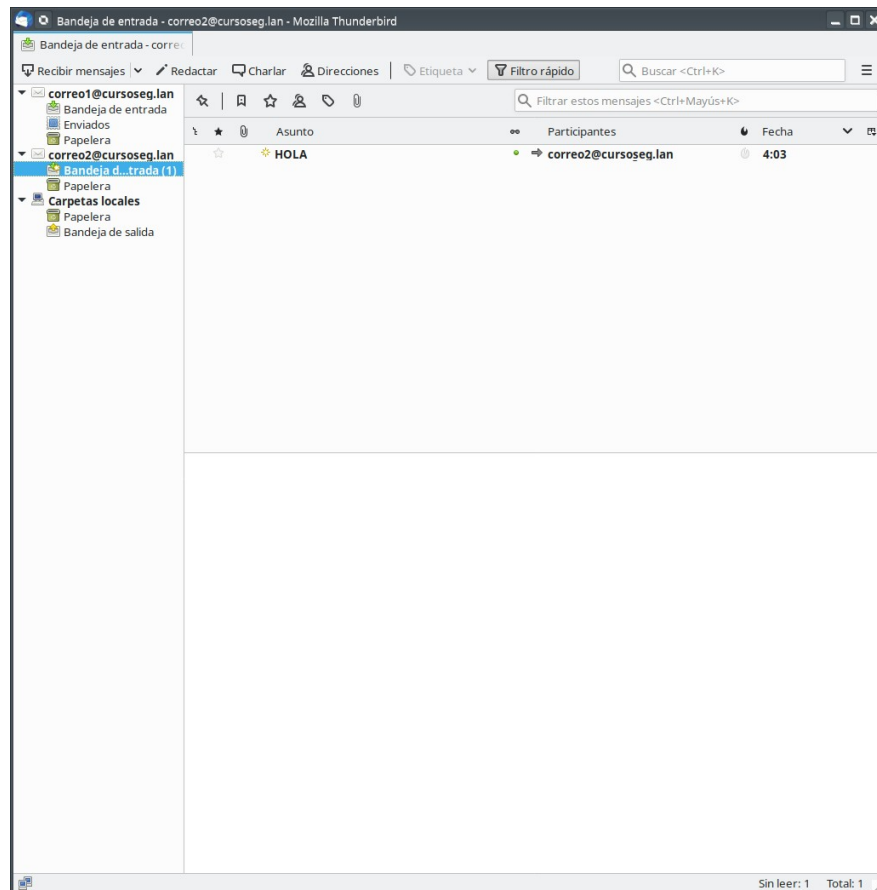
Las pruebas serán las siguientes: mandare primero un simple Hola del correo1 al correo2, será señal que el servidor está funcionando correctamente y seguidamente desde el correo2 al correo1 mandare el virus y a ver que pasa.

Mandamos el hola



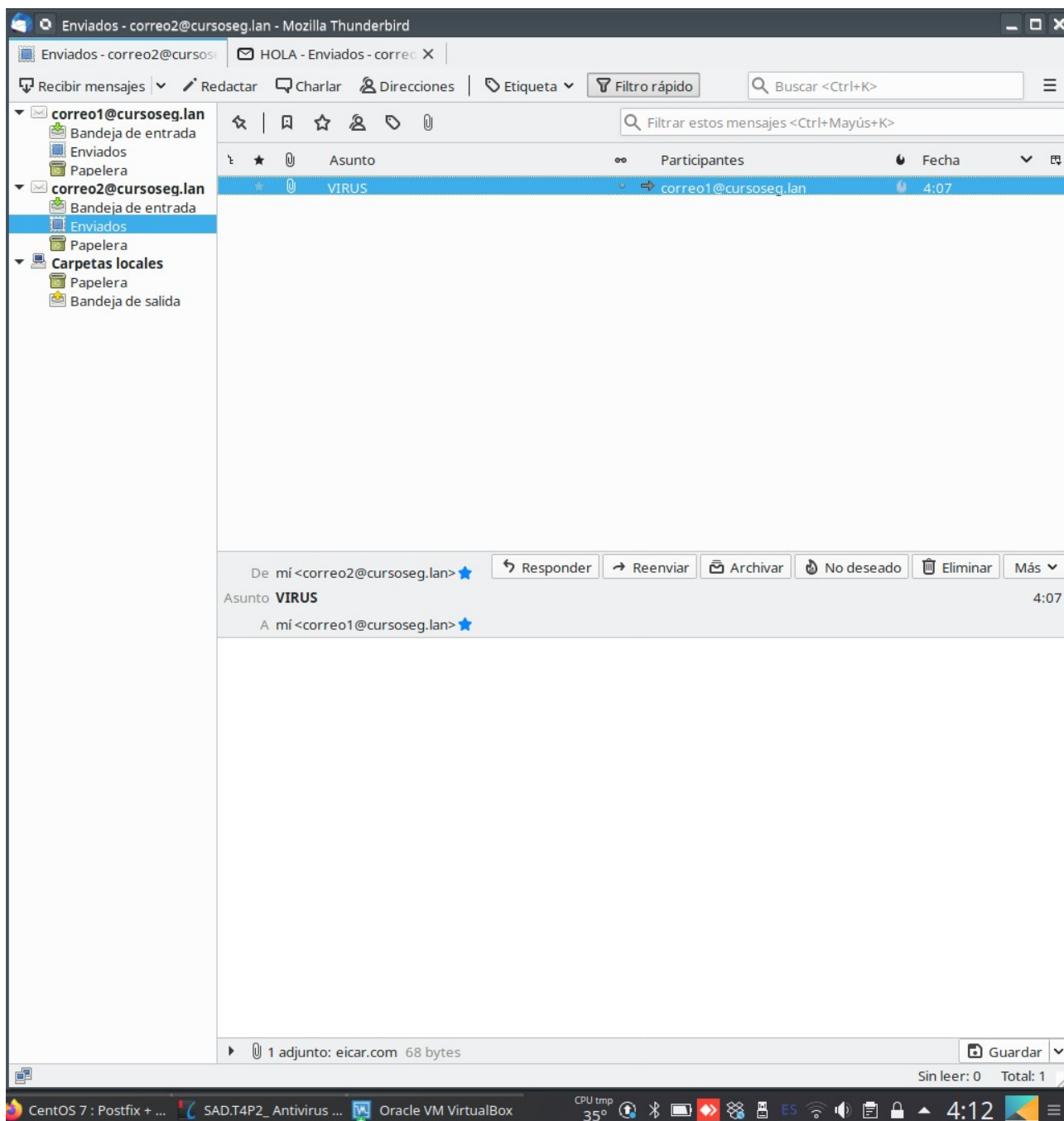
Antivirus y antispam en servidor de correo corporativo

Comprobamos el correo2 que haya recibido el correo



Antivirus y antispam en servidor de correo corporativo

Después haremos la prueba de fuego y le mandaremos un correo con un archivo adjunto con el virus desde correo2 a correo1 y este no lo manda, es bloqueado por el servidor.



Si nos fijamos estamos en la bandeja de salida de enviados de correo2 y sin embargo en la bandeja de recibidos de correo1 no hay nada.

Antivirus y antispam en servidor de correo corporativo

De todas formas para demostrarlo te muestro el log del servidor haciendo un “ cat /var/log/maillog ” y veras como en la ultima linea se ve que a detectado el virus y directamente lo elimina. Por cierto si he probado a manda un correo a mi correo personal XD

```
llorens: bash — Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
Nov 7 02:57:12 mail dovecot: pop3(correo1): Disconnected: Logged out top=0/0, retr=0/0, del=0/0, size=0
Nov 7 02:57:28 mail dovecot: imap-login: Login: user=<correo2>, method=PLAIN, rip=192.168.1.172, lip=192.168.1.130, mpid=3087, session=<q3PP/LewhADAqAGs>
Nov 7 02:57:52 mail postfix/smtpd[3026]: timeout after END-OF-MESSAGE from localhost[127.0.0.1]
Nov 7 02:57:52 mail postfix/smtpd[3026]: disconnect from localhost[127.0.0.1]
Nov 7 02:58:38 mail postfix/smtpd[3094]: connect from unknown[192.168.1.172]
Nov 7 02:58:38 mail postfix/smtpd[3094]: 4E48E1882CBE: client=unknown[192.168.1.172]
Nov 7 02:58:38 mail postfix/cleanup[3096]: 4E48E1882CBE: message-id=<140b991e-80b0-2557-3db1-ccd4a69bf1f0@cursoseg.lan>
Nov 7 02:58:38 mail postfix/qmgr[2813]: 4E48E1882CBE: from=<correo1@cursoseg.lan>, size=611, nrcpt=1 (queue active)
Nov 7 02:58:38 mail postfix/smtpd[3094]: disconnect from unknown[192.168.1.172]
Nov 7 02:59:03 mail postfix/smtpd[3026]: connect from localhost[127.0.0.1]
Nov 7 02:59:03 mail postfix/smtpd[3026]: 7A1471882CC1: client=localhost[127.0.0.1]
Nov 7 02:59:03 mail postfix/cleanup[3096]: 7A1471882CC1: message-id=<140b991e-80b0-2557-3db1-ccd4a69bf1f0@cursoseg.lan>
Nov 7 02:59:03 mail postfix/qmgr[2813]: 7A1471882CC1: from=<correo1@cursoseg.lan>, size=1059, nrcpt=1 (queue active)
Nov 7 02:59:03 mail postfix/smtpd[3026]: disconnect from localhost[127.0.0.1]
Nov 7 02:59:03 mail amavis[2644]: (02644-02) Passed CLEAN {RelayedOutbound}, MYNETS LOCAL [192.168.1.172]:35854 <correo1@cursoseg.lan> -> <llorensarbiol@gmail.com>, Queue-ID: 4E48E1882CBE, Message-ID: <140b991e-80b0-2557-3db1-ccd4a69bf1f0@cursoseg.lan>, mail_id: eTnMwPuP7r00, Hits: 1.439, size: 611, queued as: 7A1471882CC1, 25167 ms
Nov 7 02:59:03 mail postfix/smtp[3097]: 4E48E1882CBE: to=<llorensarbiol@gmail.com>, relay=127.0.0.1[127.0.0.1]:10024, delay=25, delays=0.03/0.02/0/25, dsn=2.0.0, status=sent (250 2.0.0 from MTA[smtp:127.0.0.1]:10025): 250 2.0.0 Ok: queued as 7A1471882CC1)
Nov 7 02:59:03 mail postfix/qmgr[2813]: 4E48E1882CBE: removed
Nov 7 02:59:25 mail postfix/smtp[3102]: 7A1471882CC1: to=<llorensarbiol@gmail.com>, relay=google-smtp-in.l.google.com[74.125.133.27]:25, delay=22, delays=0.01/0.02/0.68/21, dsn=5.7.1, status=bounced (host gmail-smtp-in.l.google.com[74.125.133.27] said: 550-5.7.1 [85.52.230.96] The IP you're using to send mail is not authorized to 550-5.7.1 send email directly to our servers. Please use the SMTP relay at your 550-5.7.1 service provider instead. Learn more at 550 5.7.1 https://support.google.com/mail/?p=NotAuthorizedError a8si468713wme.0 - gsmtpt (in reply to end of DATA command))
Nov 7 02:59:25 mail postfix/cleanup[3096]: 1E0431882CB2: message-id=<20191107015925.1E0431882CB2@mail.cursoseg.lan>
Nov 7 02:59:25 mail postfix/qmgr[2813]: 1E0431882CB2: from=<>, size=3654, nrcpt=1 (queue active)
Nov 7 02:59:25 mail postfix/bounce[3105]: 7A1471882CC1: sender non-delivery notification: 1E0431882CB2
Nov 7 02:59:25 mail postfix/qmgr[2813]: 7A1471882CC1: removed
Nov 7 02:59:25 mail postfix/local[3106]: 1E0431882CB2: to=<correo1@cursoseg.lan>, relay=local, delay=0.03, delays=0.01/0.02/0/0, dsn=2.0.0, status=sent (delivered to maildir)
Nov 7 02:59:25 mail postfix/qmgr[2813]: 1E0431882CB2: removed
Nov 7 03:00:27 mail dovecot: pop3-login: Login: user=<correo1>, method=PLAIN, rip=192.168.1.172, lip=192.168.1.130, mpid=3122, session=<ywt4B7iWdgDAqAGs>
Nov 7 03:00:27 mail dovecot: pop3(correo1): Disconnected: Logged out top=0/0, retr=1/3761, del=0/1, size=3744
Nov 7 03:08:38 mail clamd[2646]: SelfCheck: Database status OK.
Nov 7 03:09:04 mail postfix/smtpd[3187]: connect from unknown[192.168.1.172]
Nov 7 03:09:04 mail postfix/smtpd[3187]: C931C1882CBE: client=unknown[192.168.1.172]
Nov 7 03:09:04 mail postfix/cleanup[3192]: C931C1882CBE: message-id=<41ab28f6-ca28-9298-77d6-61fe0267497a@cursoseg.lan>
Nov 7 03:09:04 mail postfix/qmgr[2813]: C931C1882CBE: from=<correo2@cursoseg.lan>, size=3067, nrcpt=1 (queue active)
Nov 7 03:09:04 mail postfix/smtpd[3187]: disconnect from unknown[192.168.1.172]
Nov 7 03:09:04 mail dovecot: imap(correo2): Connection closed in=3699 out=3691
Nov 7 03:09:04 mail dovecot: imap-login: Disconnected (no auth attempts in 0 secs): user=<>, rip=192.168.1.172, lip=192.168.1.130, session=<0BdXJriw+ADAqAGs>
Nov 7 03:09:04 mail clamd[2646]: /var/spool/amavis/tmp/amavis-20191107T025641-02645-1ujmbjL8/parts/p006: Eicar-Test-Signature FOUND
Nov 7 03:09:05 mail clamd[2646]: /var/spool/amavis/tmp/amavis-20191107T025641-02645-1ujmbjL8/parts/p003: Eicar-Test-Signature FOUND
Nov 7 03:09:05 mail amavis[2645]: (02645-02) Blocked INFECTED (Eicar-Test-Signature) [DiscardedInternal,Quarantined], MYNETS LOCAL [192.168.1.172]:35962 <correo2@cursoseg.lan> -> <correo1@cursoseg.lan>, Queue-ID: C931C1882CBE, Message-ID: <41ab28f6-ca28-9298-77d6-61fe0267497a@cursoseg.lan>, mail id: LuNyD5hlrEM2, Hits: -, size: 3066, 228 ms
Nov 7 03:09:05 mail postfix/smtp[3193]: C931C1882CBE: to=<correo1@cursoseg.lan>, relay=127.0.0.1[127.0.0.1]:10024, delay=0.27, delays=0.03/0.01/0/0.23, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=02645-02 - INFECTED: Eicar-Test-Signature)
Nov 7 03:09:05 mail postfix/qmgr[2813]: C931C1882CBE: removed
[root@mail ~]#
```