UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Practica 07

López Bautista José Luis PROFESOR

Yeudiel Hernández Torres

AYUDANTES

Raúl Ríos Ciriaco
Virgilio Castro Rendón

ASIGNATURA

Administración de Sistemas Unix/Linux

4 de diciembre de 2024

1. Desarrollo

Realizamos la instalación del paquete fail2ban

```
jose@debian:~$ sudo apt install fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify python3-systemd whois
Suggested packages:
  mailx system-log-daemon monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify python3-systemd whois
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded
```

Nos cambiamos al directorio de fail2ban, de forma que se crea una copia del archivo de configuración, en donde se agrega lo siguiente

```
jose@debian: /etc/fail2ban

# To use more aggressive sshd modes set filter pa
# normal (default), ddos, extra or aggressive (co
# See "tests/files/logs/sshd" or "filter.d/sshd.c
#mode   = normal
port    = ssh
logpath = %(sshd_log)s
# backend = %(sshd_backend)s
backend = systemd
```

Ahora recargamos la configuración del servicio y vemos el status.

```
jose@debian:~$ sudo systemctl start fail2ban
jose@debian:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Sun 2024-11-10 18:07:50 CST; 21s ago
       Docs: man:fail2ban(1)
   Main PID: 1760 (fail2ban-server)
      Tasks: 5 (limit: 2264)
     Memory: 19.5M
        CPU: 359ms
     CGroup: /system.slice/fail2ban.service
             └─1760 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Nov 10 18:07:50 debian systemd[1]: Started fail2ban.service - Fail2Ban Service.
Nov 10 18:07:50 debian fail2ban-server[1760]: 2024-11-10 18:07:50,311 fail2ban.config
Nov 10 18:07:50 debian fail2ban-server[1760]: Server ready
```

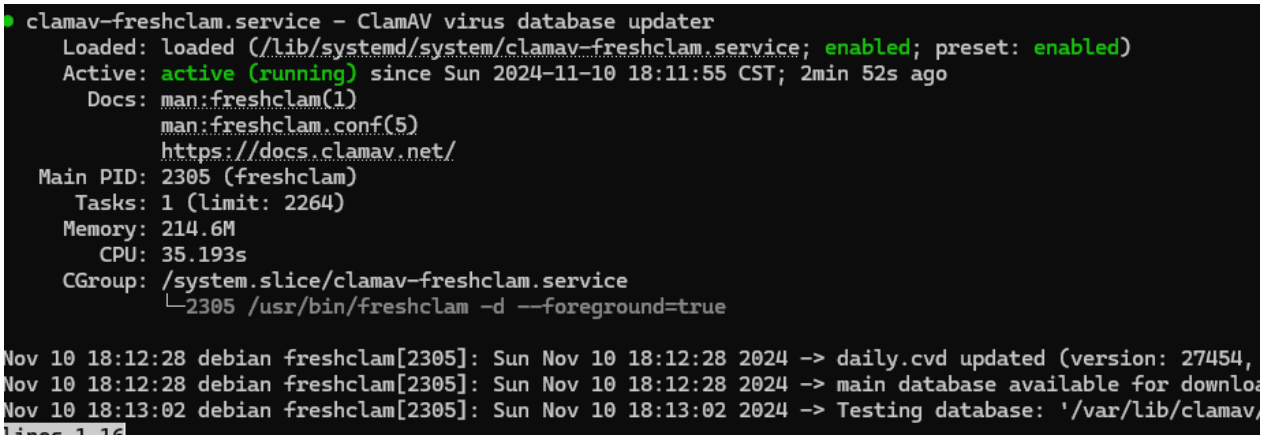
Luego revisamos el estado de Fail2ban para el servicio SSHD

```
jose@debian:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

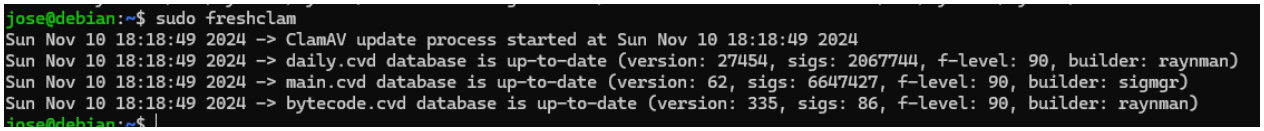
Para la instalación de ClamaV primero se instala el paquete clamav y su demonio, luego con el comando dpkg-reconfigure clamav-daemon, configuramos las especificaciones del servicio. De forma que al ver el estatus se tiene:

```
jose@debian:~$ sudo systemctl status clamav-freshclam.service
● clamav-freshclam.service - ClamAV virus database updater
     Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; disabled; preset: enabled)
     Active: active (running) since Sun 2024-11-10 18:11:55 CST; 28s ago
       Docs: man:freshclam(1)
             man:freshclam.conf(5)
             https://docs.clamav.net/
   Main PID: 2305 (freshclam)
      Tasks: 2 (limit: 2264)
     Memory: 687.9M
        CPU: 16.456s
     CGroup: /system.slice/clamav-freshclam.service
             ├─2305 /usr/bin/freshclam -d --foreground=true
             └─2755 /usr/bin/freshclam -d --foreground=true
```

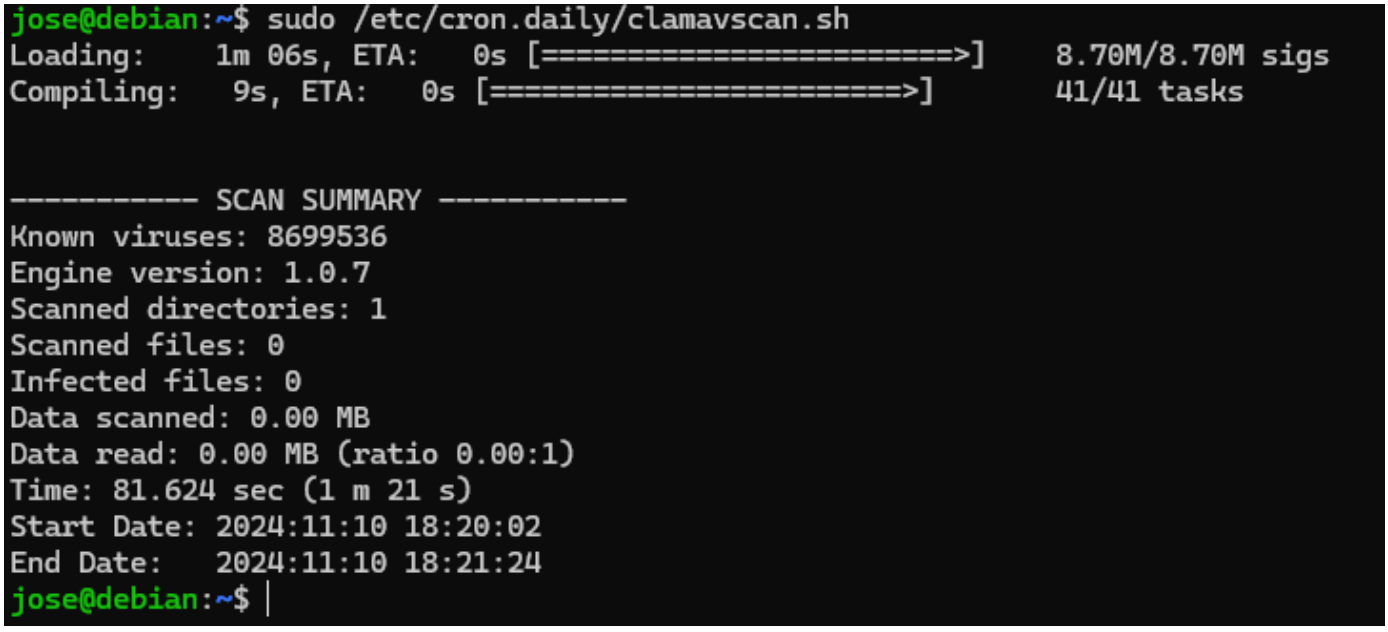
Por lo que con systemctl enable clamav-freshclam.service, se activa el servicio



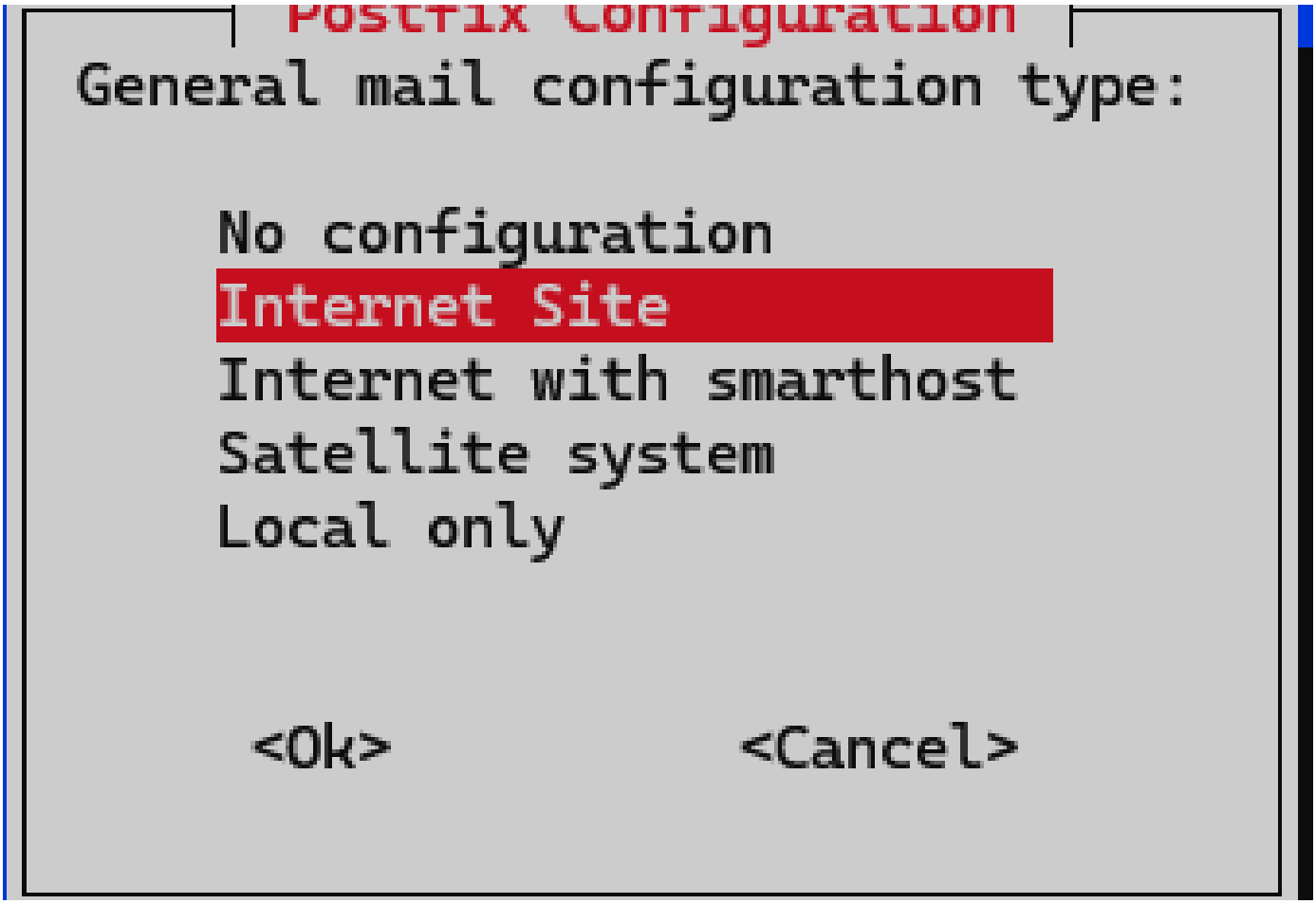
Luego de esto ejecutamos manualmente la actualización de la base de datos



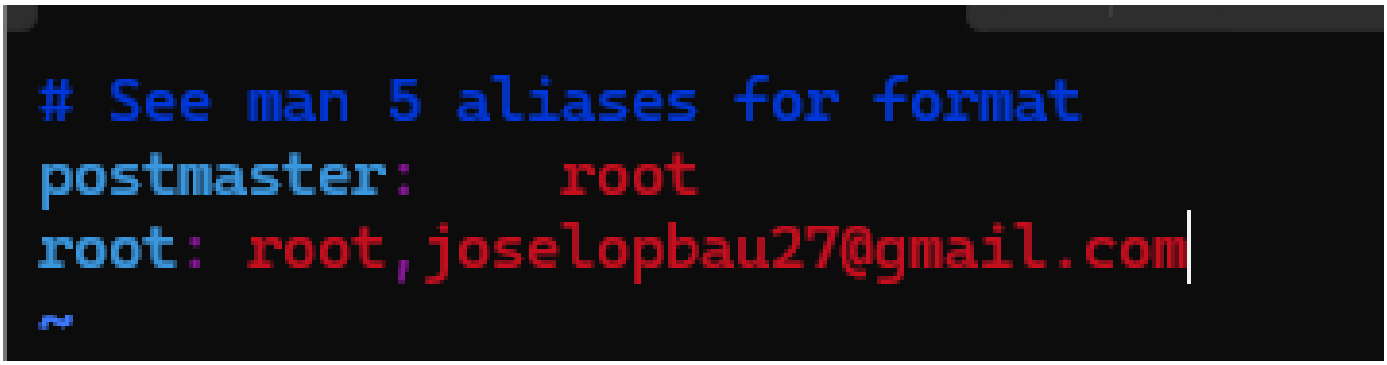
Ahoras lo que hacemos es editar el archivo de tareas diarias de clamav, en el cual se indica que analice todos los documentos del directorio home “clamscan /home/”, luego se le da permisos de ejecución y por último se ejecuta el script



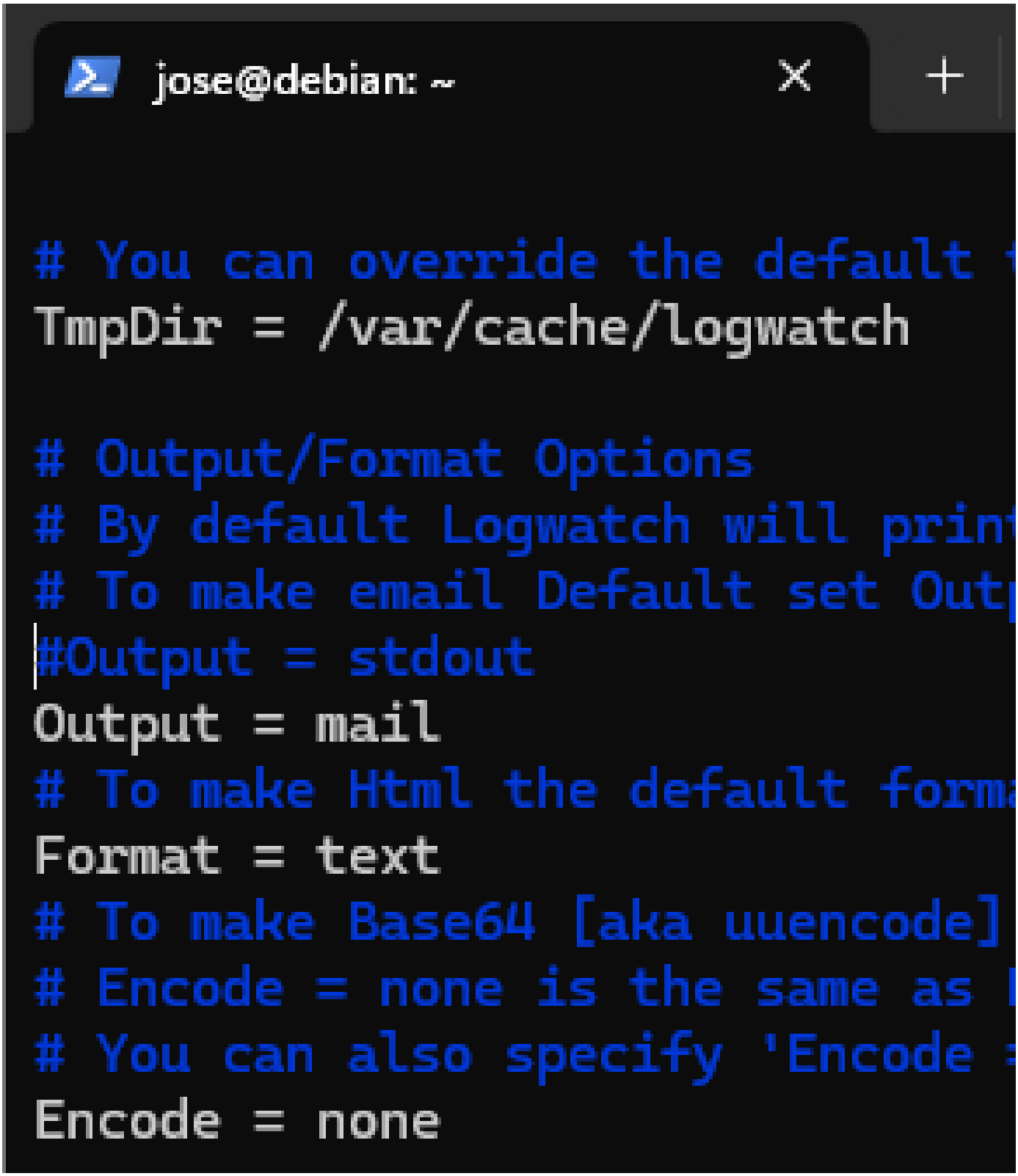
Por último para logwatch primero descargamos los paquetes mailutils postfix logwatch, y se inicia la configuración del servicio con dpkg-reconfigure.



Se edita el archivo de aliases, en donde colocamos lo siguiente



Después con newaliases actualizamos la base de datos, se crea un directorio cache para logwatch y se copia el archivo de configuración principal en ese directorio. Luego se abre el archivo de configuración y se hace un cambio



Con el comando logwatch –detail Low –range today. Ejecuta Logwatch manualmente para generar un informe de baja profundidad :

```
jose@debian:~$ sudo cat /var/mail/root
From root@debian.localdomain  Sun Nov 10 18:29:05 2024
Return-Path: <root@debian.localdomain>
X-Original-To: root
Delivered-To: root@debian.localdomain
Received: by debian.localdomain (Postfix, from userid 0)
        id E9983C0E; Sun, 10 Nov 2024 18:29:05 -0600 (CST)
To: root@debian.localdomain
From: logwatch@debian.localdomain
Subject: Logwatch for debian (Linux)
Auto-Submitted: auto-generated
Precedence: bulk
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
Content-Type: text/plain; charset="UTF-8"
Message-Id: <20241111002905.E9983C0E@debian.localdomain>
Date: Sun, 10 Nov 2024 18:29:05 -0600 (CST)


 ###################### Logwatch 7.7 (07/22/22) ######################
        Processing Initiated: Sun Nov 10 18:29:05 2024
        Date Range Processed: today
                              ( 2024-Nov-10 )
                              Period is day.
        Detail Level of Output: 0
        Type of Output/Format: mail / text
        Logfiles for Host: debian
 ####################################################################
```

Se Abre el archivo de tareas diarias 00logwatch , se agregan los cambios siguientes

```
jose@debian: ~
#!/bin/bash

#Check if removed-but-not-purged
test -x /usr/share/logwatch/scripts/logwatch.pl || exit 0

#execute
/usr/sbin/logwatch --output mail --mailto joselopbau27@gmail.com --detail medium --range today

#Note: It's possible to force the recipient in above command
#Just pass --mailto address@a.com instead of --output mail
~
~
~
~
~
~
:
```

Y para las tareas semanales se tiene:

```
jose@debian: ~
#!/bin/bash
/usr/sbin/logwatch --output mail --mailto joselopbau27@gmail.com --detail high --range "since 7 days ago"
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/cron.weekly/00logwatch" 3L, 119B
```