**Implementación de un Servidor de Correo Empresarial**

# Fase 1: Instalación y configuración del servidor de correo

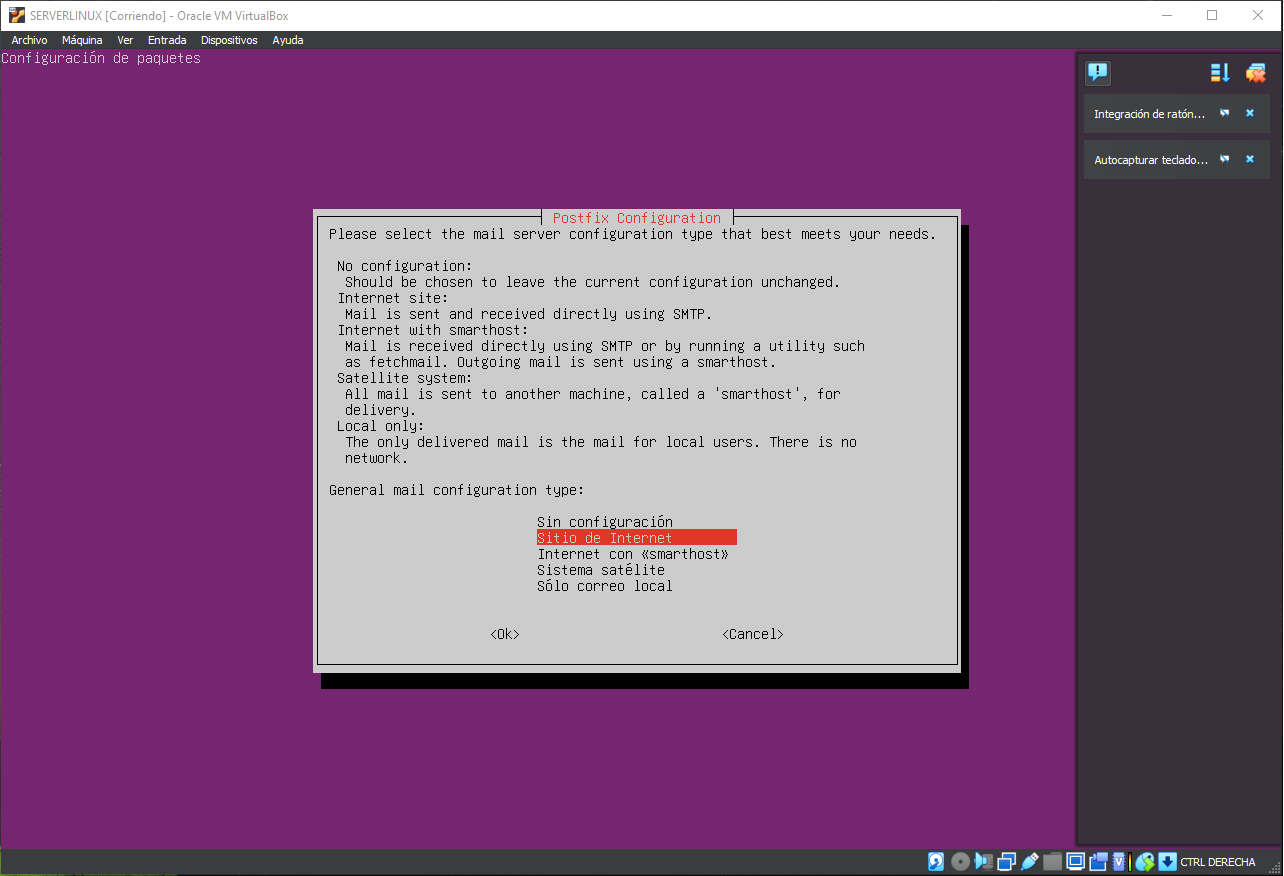
Instalamos Postfix, Devecot y certificados:

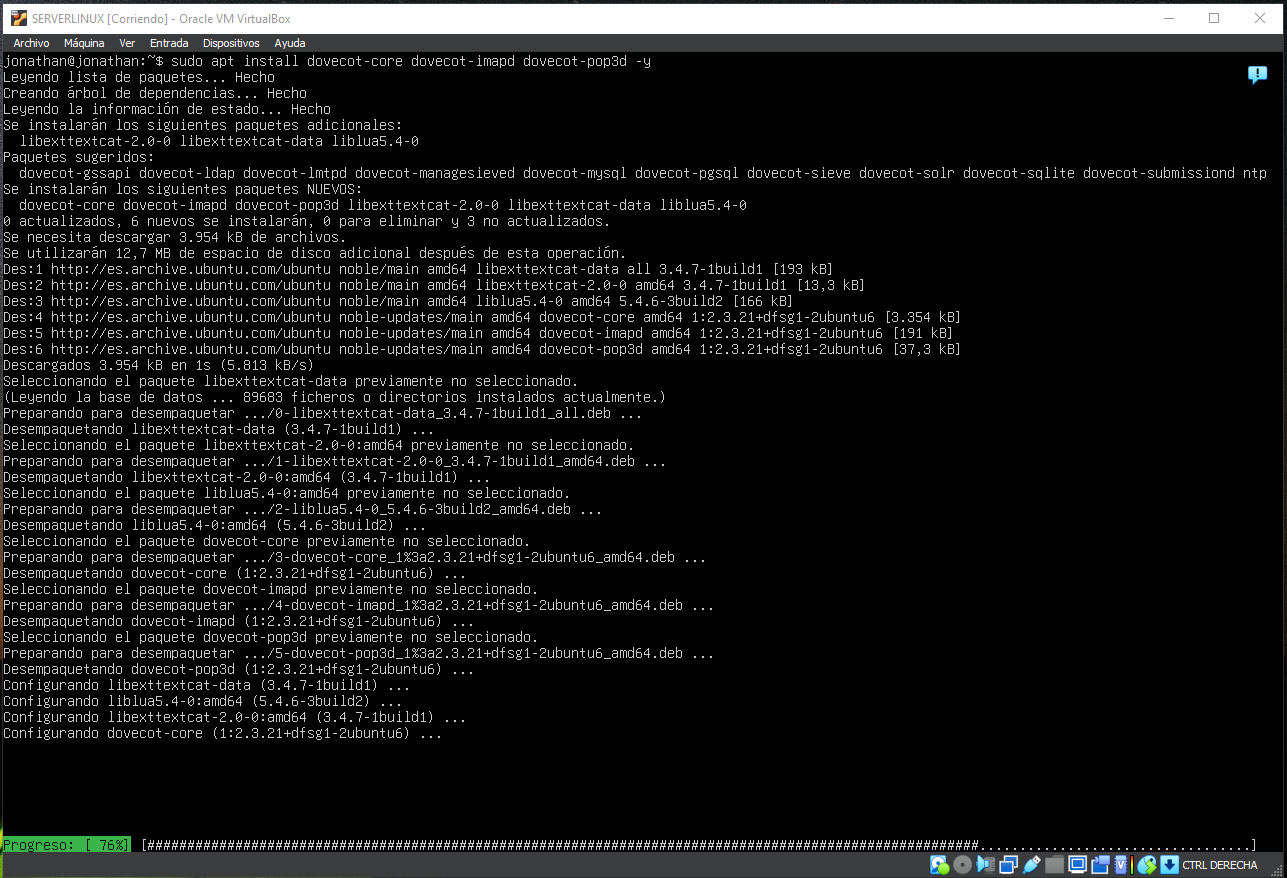
sudo apt install postfix dovecot-core dovecot-imapd

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \

-keyout /etc/ssl/private/ssl-cert-snakeoil.key \

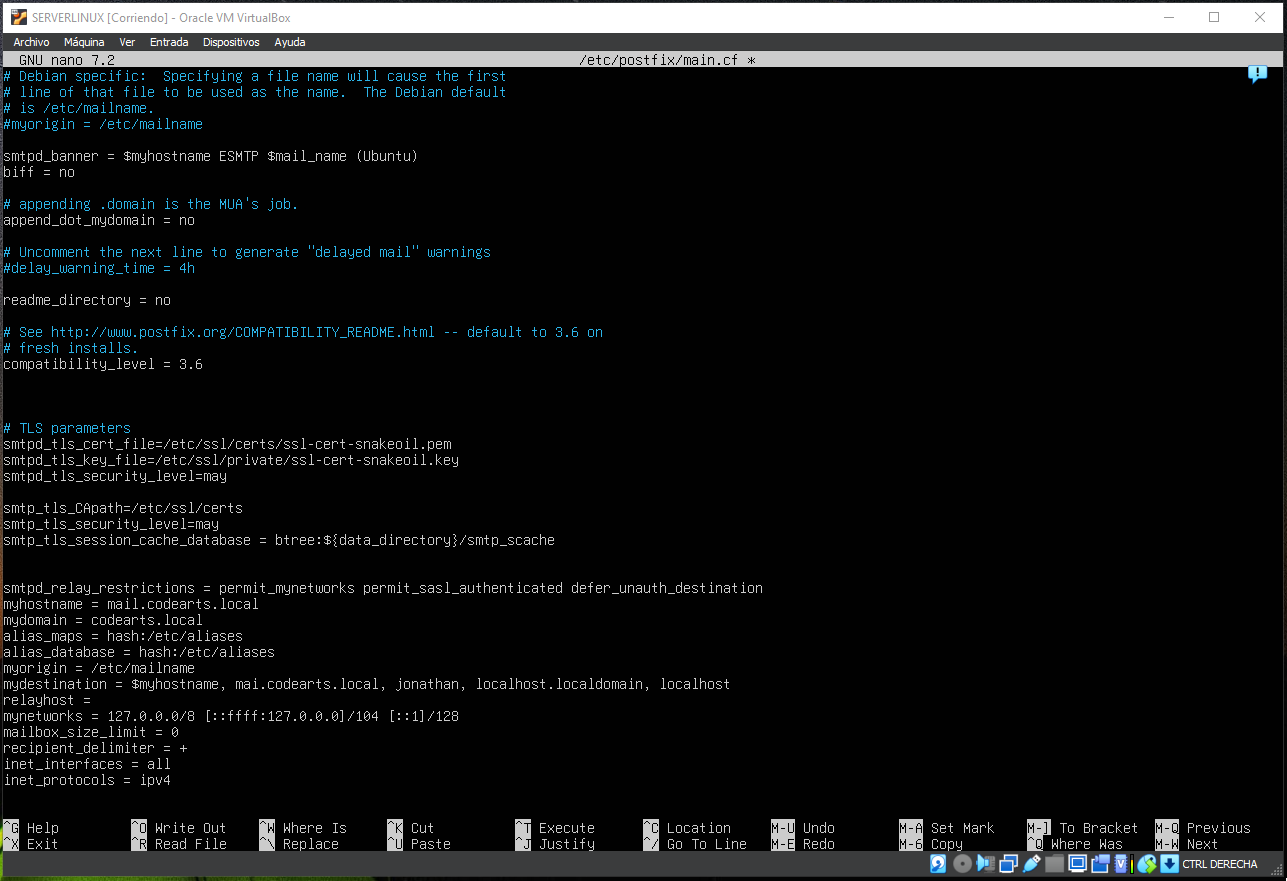
-out /etc/ssl/certs/ssl-cert-snakeoil.pem





Configuramos el domino de correo y definimos la estructura de los buzones:

Sudo nano /etc/postfix/main.cf

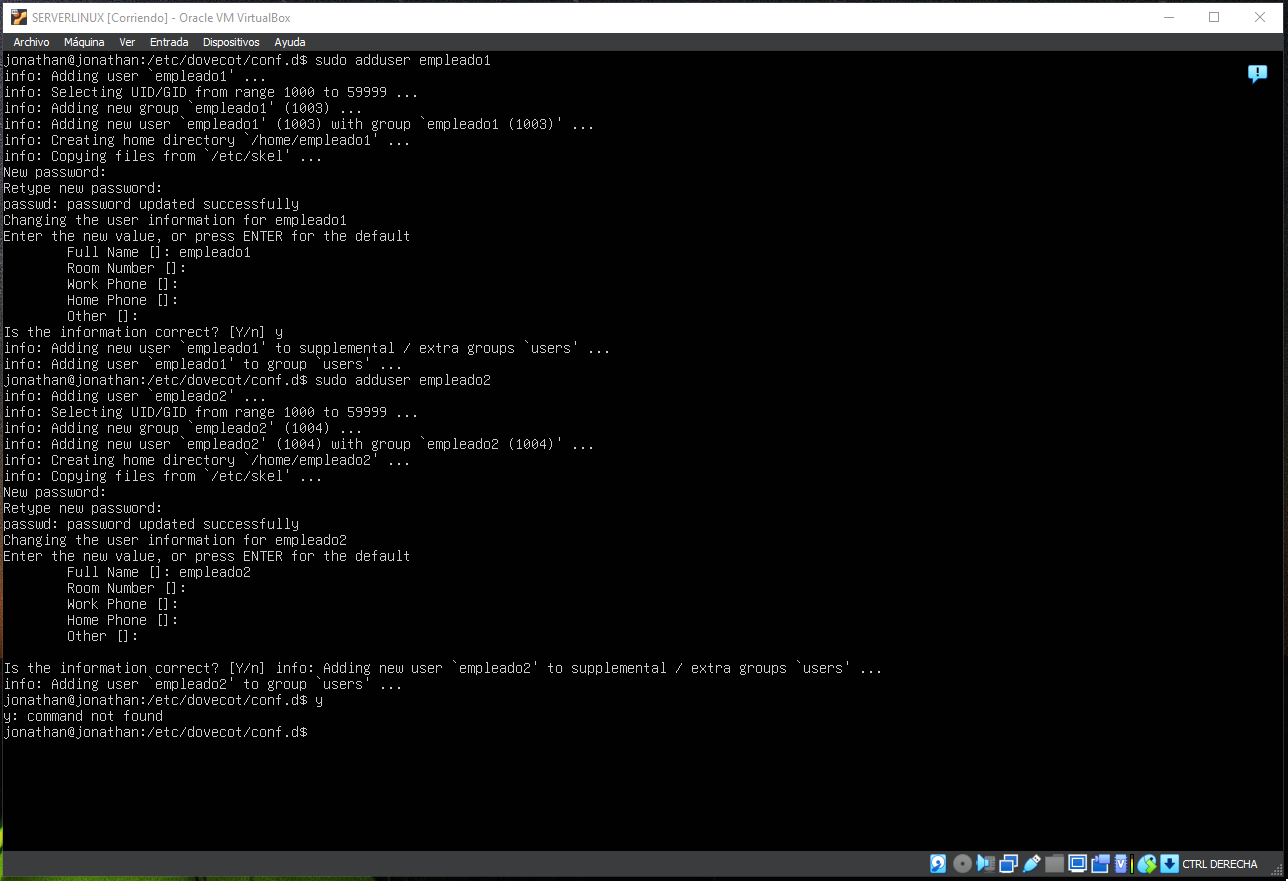


# Fase 2: Creación y gestión de cuentas de correoç

Creamos los buzones de correo para los empleados:

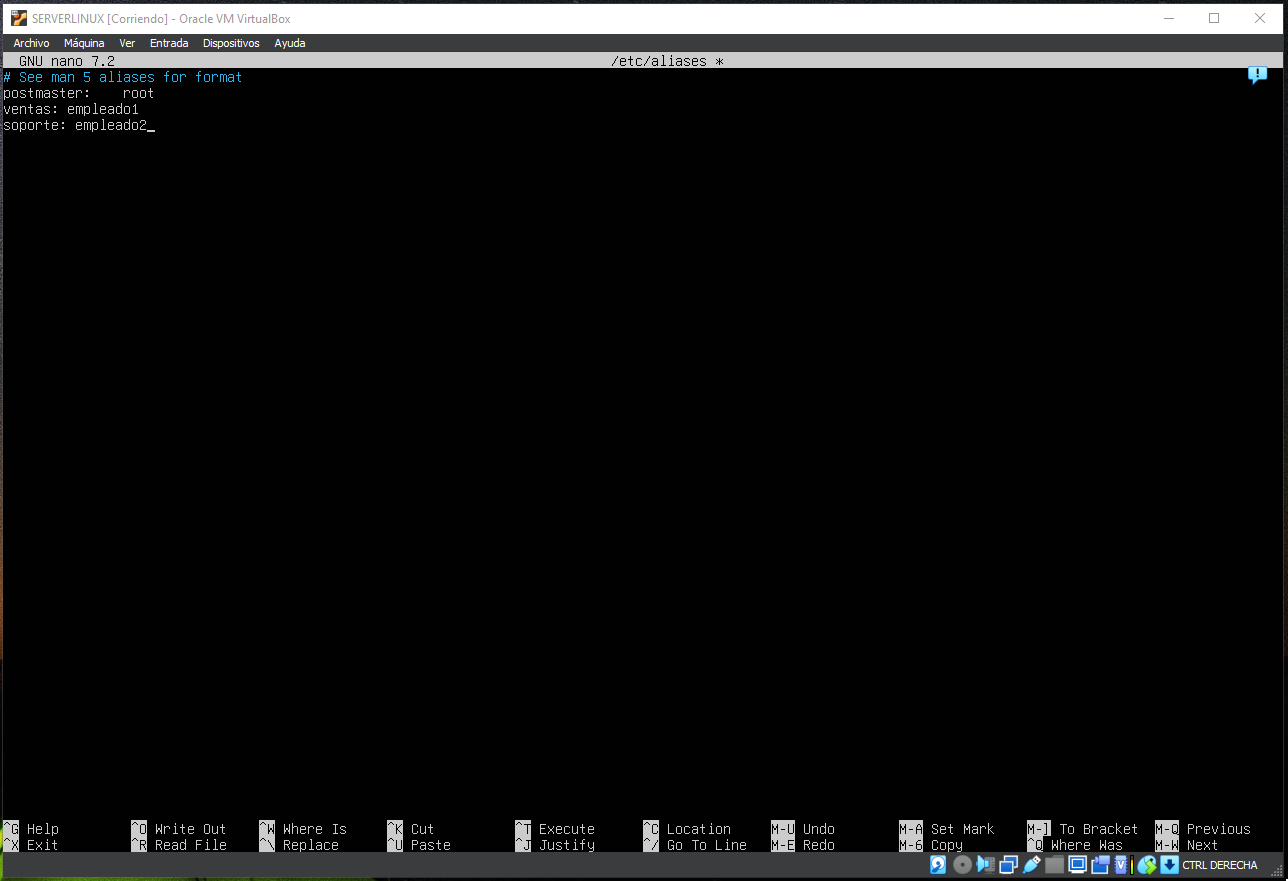
sudo adduser empleado1

sudo adduser empleado2



Configuramos los alias y reenvío:

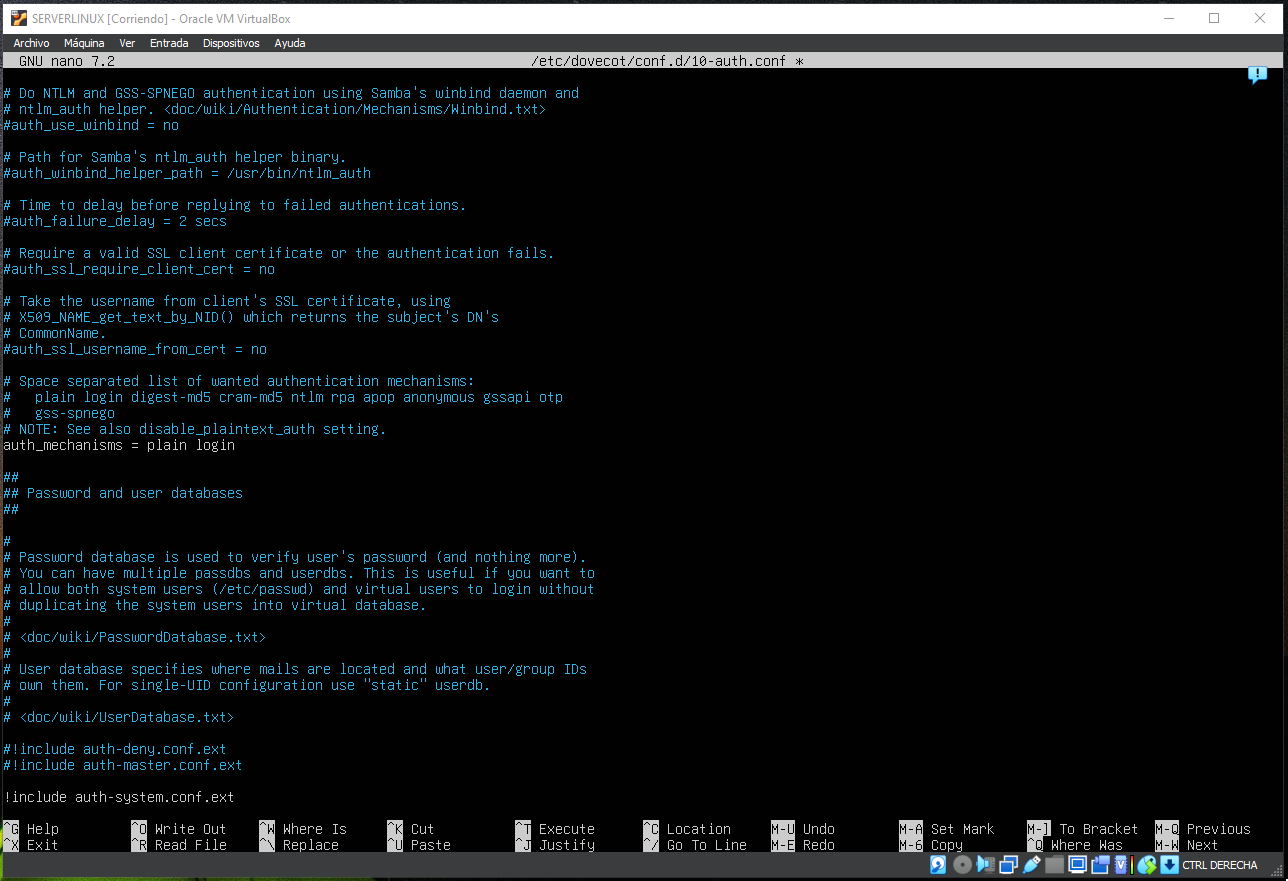
sudo nano /etc/aliases \*

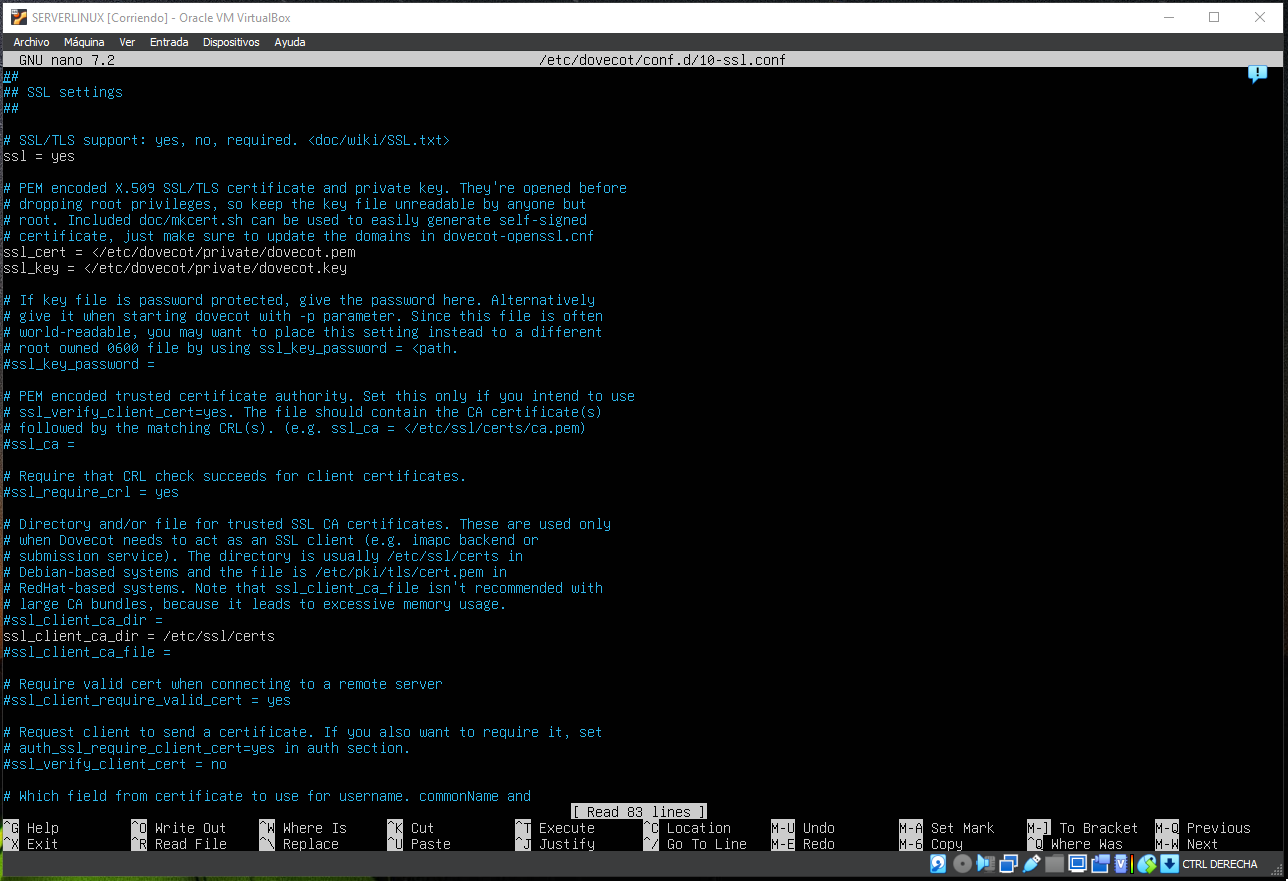


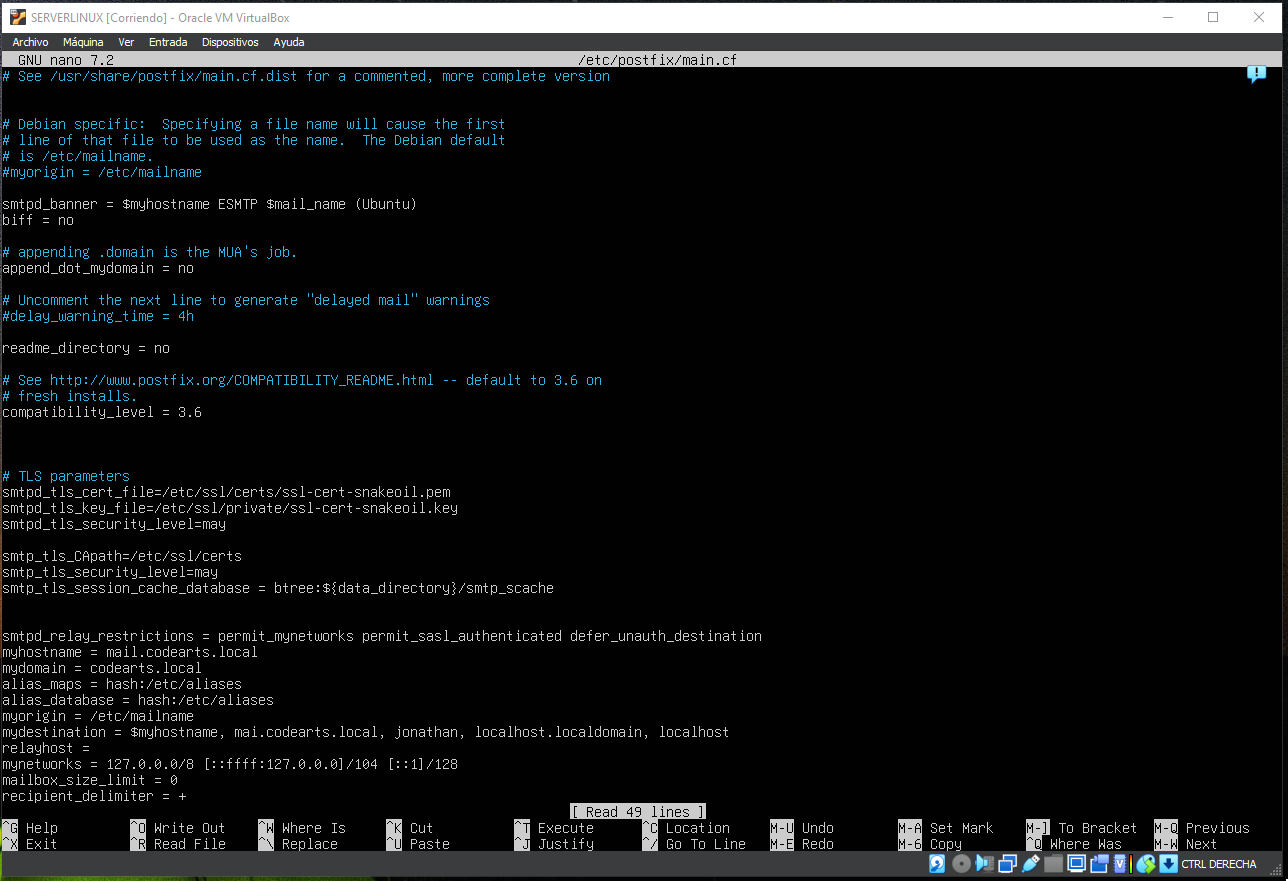
# Fase 3: Seguridad y autenticación

Implementamos la autenticación SASL, la configuracion SSL/TLS, y configuramos SPF, DKIM y DMARC

sudo nano /etc/postfix/[main.cf](http://main.cf)

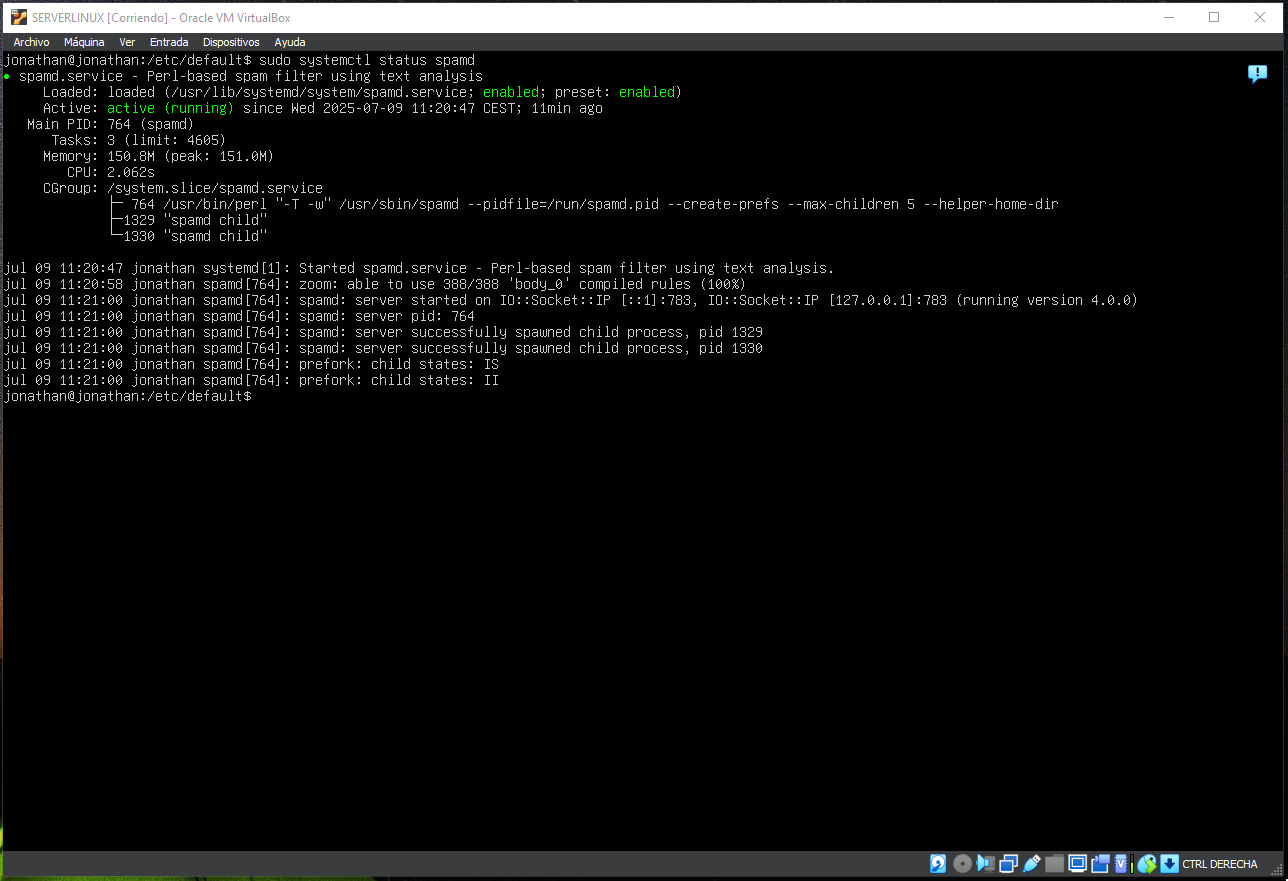


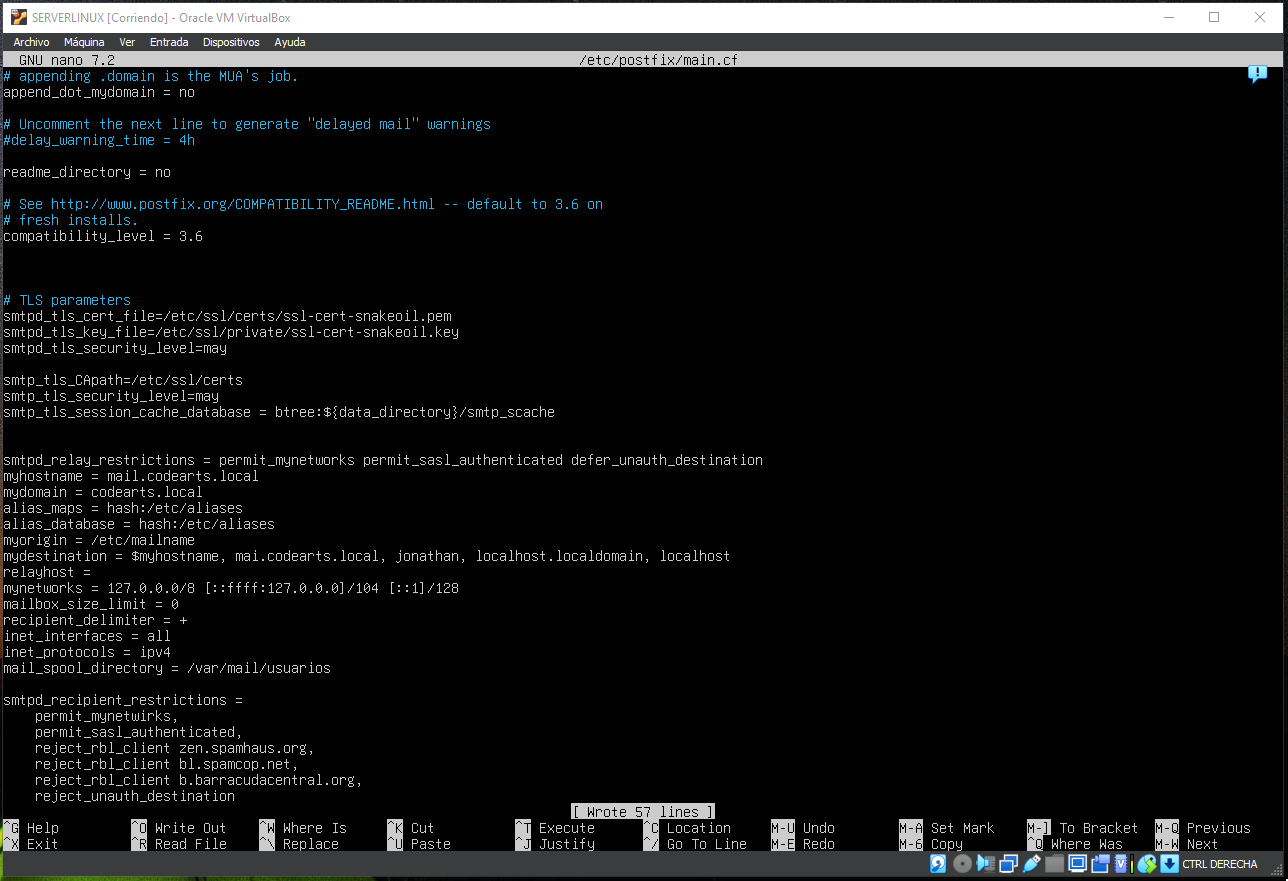




Instalamos SpamAssassin para establecer listas negras y filtrado de spam:

sudo apt install spamassassin





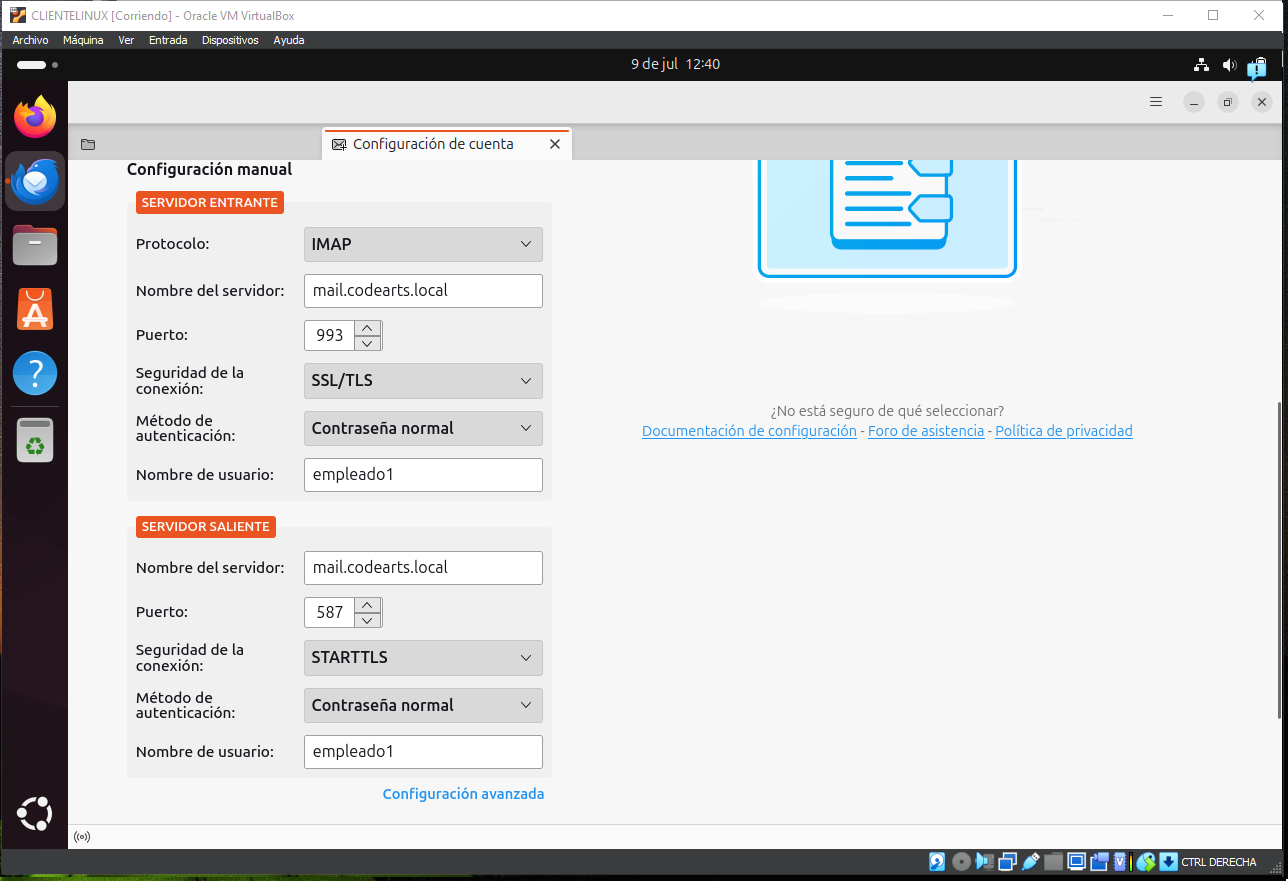
# Fase 4: Integración con clientes de correo y pruebas

Configuramos los clientes de correo:

Thunderbird u Outlook:

IMAP: mail.codearts.local, puerto 993

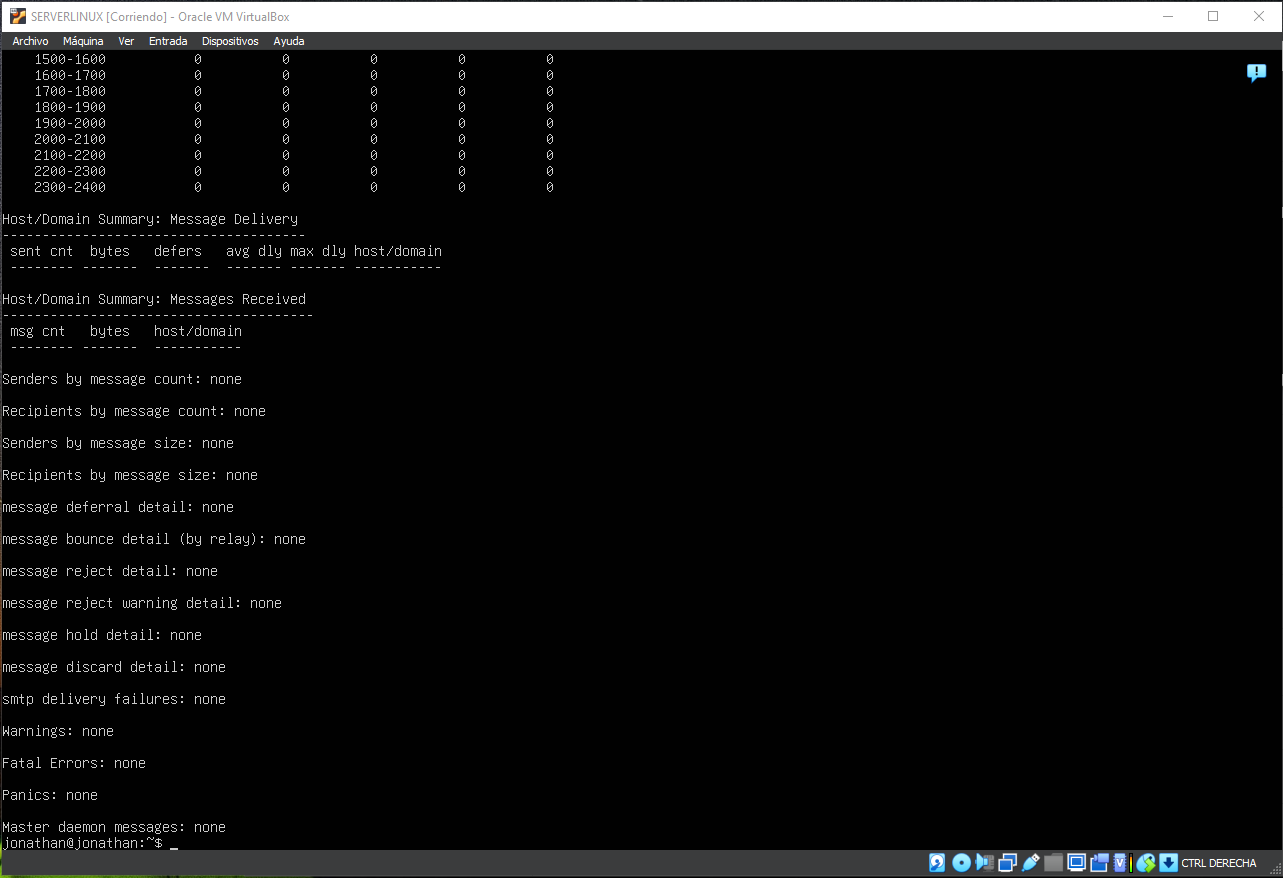
SMTP: mail.codearts.local, puerto 465



# Fase 5: Monitoreo y optimización del servidor

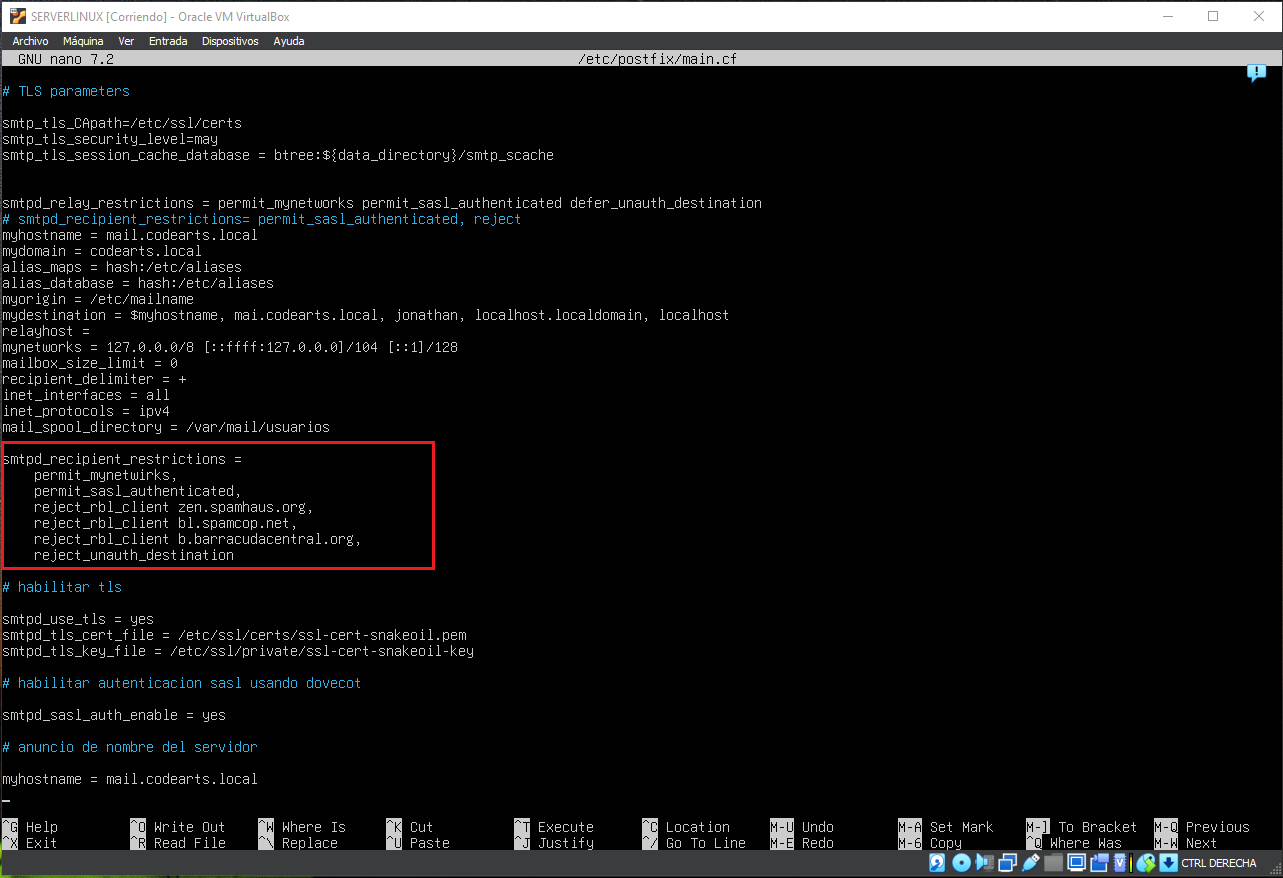
Instalamos pflogsumm para el monitoreo de correos:

sudo apt install pflogsumm



Y configuramos la reglas de filtrado:

sudo nano /etc/postfix/[main.cf](http://main.cf)



Instalamos Fail2Ban para protegernos de fuerza bruta y spam y configuramos el archivo:

sudo apt install fail2ban

sudo nano /etc/fail2ban/jail.d/postfix.local

