**TP B**

**Sistemas Operativos**

**Conexión entre SO distintos**

Para esta actividad utilizaremos un sistema operativo Ubuntu 18.04 y un sistema Windows 10

**Configuración de IP estatica**

Lo primero que debemos hacer es configurar la direccion ip del servidor, por lo que debemos desactivar el DHCP y definir una ip estatica. Para ello debemos modificar como administrador el archivo /etc/netplan/01-network-manager-all.yaml, esto debido a que utilizamos un Ubuntu > 17, nos encontraremos un archivo en formato yaml

Antes de realizar cualquier cambio en un archivo del sistema es recomendable realizar una copia de los mismos , sin modificación, para poder restaurarlos en caso de algún problema.

Network:

Versión: 2

Renders: NetworkManager

Modificaremos el parámetro renders, por networkd. Al tratarse de un archivo yaml, es importante prestar atención a el ESPACIADO, es decir que la estructura utiliza 2 espacios por estructura, es decir, versión, que esta dentro de network esta a dos espacios del inicio de línea.

Agregaremos la siguiente estructura, comenzando con la palabra ethernets a dos espacios del comienzo de linea

Ethernets:

Enp0s8:

addresses: [192.168.1.27/24]

gateway4: 192.168.1.1

nameservers:

search: [estuviani.com]

addresses: [8.8.8.8, 8.8.4.4]

por el momento utilizaremos el DNS, de google, luego lo modificaremos para el servidor de correo.

Si deseamos verificar que cumplimos la sintaxis, pero no deseamos aun aplicar los cambio utilizamos el comando

netplan generate

*Ahora debemos aplicar los cambios*

*Netplan apply*

*si no cometimos ningun error el promp regresara sin ningun mensaje significando que se aplico la configuración. Para comprobar que esto sea correcto utilizaremos el comando*

*ip add*

*para verificar la información de la red.*

*ip add previo*

*1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000*

*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: enp0s8: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000*

*link/ether 08:00:27:83:b4:d5 brd ff:ff:ff:ff:ff:ff*

*inet* ***192.168.1.26/24*** *brd 192.168.1.255 scope global dynamic enp0s8*

*valid\_lft 85625sec preferred\_lft 85625sec*

*inet6 fe80::1829:4442:bb5c:9848/64 scope link noprefixroute*

*valid\_lft forever preferred\_lft forever*

*ip add nuevo*

*1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000*

*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: enp0s8: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000*

*link/ether 08:00:27:83:b4:d5 brd ff:ff:ff:ff:ff:ff*

*inet* ***192.168.1.27/24*** *brd 192.168.1.255 scope global enp0s8*

*valid\_lft forever preferred\_lft forever*

*inet6 fe80::1829:4442:bb5c:9848/64 scope link noprefixroute*

*valid\_lft forever preferred\_lft forever*

*Para verificar que el puerto de enlace se configuro correctamente utilizamos el comando*

*ip route*

*para verificar el DNS utilizamos el comando*

*systemd-resolve --status*

**Instalar Samba**

Para compartir archivos instalaremos un servidor Samba en el SO Ubuntu, por medio del comando

*apt install samba*

*,* para instalar el servidor Samba.

**Crear o definir usuarios**

Podemos crear usuarios específicos para Samba, o podemos generar una contraseña para uno o más usuarios existentes.

Crear un usuario:

*useradd sambauser*

o usamos un usuario existente, esteban

luego generamos la contraseña para el usuario en samba

*smbpasswd -a* sambauser

ó *smbpasswd -a* esteban

le colocamos la contraseña, que debería ser distinta a la del mismo usuario, si se utiliza uno existente, para su acceso, verificamos los usuarios de Samba con el comando

*pdbedit -L*

Con el comando

*smbpasswd -x* USER podremos eliminar un usuario de Samba

**Usuarios creados**

Para pruebas creamos tres usuarios

suser : usuario de lectura en todos los directorios. Podra escribir y ejecutar en *public* y *lectura*

USERPASS: suse

SAMBAPASS: susamba

sreader: solo tendrá permisos de lectura en los directorios *lectura,*y no podrá acceder a ningún otro directorio

USERPASS sure

SAMBAPASS: resamba

swrite: podrá leer escribir en la carpeta *soloAutWrite* y *public,* y podrá acceder a el directorio *lectura*

USERPASS: swri,

SAMBAPASS: wrsamba

nobody: usuario anonimo, ya existente en el sistema UNIX, este usuario es el usuario anonimo, por lo que podrá ver que existen los directorios, pero no podrá ver ningún dato de ellas

**Creación de directorio locales**

Podemos utilizar directorios ya existentes o generar espacios específicos para compartir.

Crear las carpetas locales, soloLectura, publico, soloAutWrite

Mkdir /samba/FOLDER

**Creación de grupo de usuarios**

creamos el grupo admines, escribe y validos

groupadd admines

groupadd validos

groupadd escribe

agregamos a cada usuario al grupo correspondiente

usermod -G admines,validos swrite

usermod -G validos,escribe suser

usermod -G validos sreader

cambiamos el grupo de los directorios del grupo root, a el grupo que estará habilitado para modificar, con la opción -R, nos aseguramos que la misma configuración de grupo se aplique a los archivos y directorios existentes, como a los nuevos que se crearan

chgrp -R admines /samba/soloAutWrite

chgrp -R validos /samba/publico

chgrp -R escribe /samba/soloLectura

Cambiamos los permisos del directorio, diciendo que se aplicara a todos los nuevos directorios y archivo (-R), 0775, significa en octal, el 0 es indicador de la base, el primer 7, en octal, indica que el propietario, es decir el usuario ROOT, podrá leer, escribir y ejecutar cualquier archivo o directorio, el segundo 7 indica que cualquiera perteneciente al grupo correspondiente, podrá realizar lectura, escritura y ejecución, y el ultimo 5 indica que cualquier usuario no perteneciente a el grupo solo podrá leer y ejecutar. La opción 0774, en soloAutWrite, permite que el dueño y el grupo admines puedan realizar toda acción, pero cualquier otro usuario solo podrá leer.

chmod -R 0774 /samba/soloAutWrite

chmod -R 0775 /samba/soloLectura

chmod -R 0775 /samba/publico

**Configuración de samba**

Ahora debemos configurar el Samba, modificaremos el archivo smb.conf, ubicado en etc/samba/

Modificaremos la configuración global del Samba

Agregaremos el identificador del servidor, el nombre del workgroup, y el nombre que tendrá el servidor

[global]

## Browsing/Identification ###

netbios name= so-tpb

# Change this to the workgroup/NT-domain name your Samba server will part of

workgroup = WORKGROUP

# server string is the equivalent of the NT Description field

server string = %h - Sistema servidorS

debemos indicar en que red esta escuchando, como es un servidor local añadiremos la ip/mask privada

#### Networking ####

# The specific set of interfaces / networks to bind to

# This can be either the interface name or an IP address/netmask;

# interface names are normally preferred

; interfaces = 127.0.0.0/8 eth0

*interfaces = 192.168.1.0/24 eth0*

Podemos definir que rol tendra el servidor, standalone server, member serve, classic primary domain controller

####### Authentication #######

# Server role. Defines in which mode Samba will operate. Possible

# values are "standalone server", "member server", "classic primary

# domain controller", "classic backup domain controller", "active

# directory domain controller".

#

# Most people will want "standalone sever" or "member server".

# Running as "active directory domain controller" will require first

# running "samba-tool domain provision" to wipe databases and create a

# new domain.

server role = standalone server

lo dejaremos en *standalone server*

Pondremos que la seguridad, necesitara un usuario y contraseña para el acceso, esto es redundante, ya que el rol del servidor standalone, toma este parámetro, pero nos aseguraremos que se utilice esta opción

####### Authentication #######

.

.

Security = user

En la sección donde definiremos los directorios compartidos tenemos diferentes parámetros que podemos definir para el directorio compartido, lo que se debe tener en cuenta es que el control sobre escritura, lectura lo hace el mismo sistema operativo Linux, por lo que debemos generar los usuarios, grupos y permisos, sobre los archivos o directorios para el correcto funcionamiento

Estructura básica

[SHARENAME] nombre con el que se conocerá el directorio, publicamente

**Path**= PATH/TO/FOLDER, ubicación del directorio local

Comment= INFO, información sobre el archivo compartido

Read only= yes/no, será de solo lectura o permitirá escritura

Guest ok = yes/no, permitirá el acceso de usuarios anónimos

Browseable = yes/no, permitirá que al acceder a la dirección ip se vea el directorio compartido

Valid users= USER, @GROUP; indica que usuario o grupo de usuarios tiene permitido acceder al directorio

Invilid users= USER,@GROUP; indica que usuario o grupo de usuarios no podrán acceder al directorio

Write list= USER,@GROUP; indica que usuario o grupo de usuarios podrán escribir específicamente, esto es en el caso de read only = yes

Create mask = [0775], define el valor por defecto de los atributos que tendrán, los archivos generados en este directorio, es decir, que el usuario y el grupo al que pertenece podrán realizar toda acción, pero los demás usuarios solo podrán leer y ejecutar

Directory mask=[0700], define el valor por defecto de los directorios que se creen en este directorio, es decir, solo el creador podrá realizar acciones sobre los directorio generados

Ahora agregaremos los recursos a compartir en smb.conf, crearemos una carpeta llamada **public**, que apunta al directorio local **/samba/publico**

[**public**]

Path= **/samba/publico**

Comment= carpeta publica a todos

Read only =no

Guest ok = no

Browseable = yes

Invalid users = sreader

Write list = @validos

Esto define un directorio llamado public, que permitirá lecturas y escrituras, no permitirá el acceso anónimo, toda persona que ingrese a la dirección ip vera el directorio, y sreader no podrá acceder a los archivos de este directorio, pero si podrá ver que existe el mismo

Ahora configuraremos una carpeta de solo lectura, es decir solo los miembros del grupo **escribe** podrán escribir en ella, y los otros usuarios podrán solo ver, a este directorio le llamaremos **lectura**, apuntando a el directorio local **\samba\soloLectura**

[**lectura**]

path=/**samba/soloLectura**

comment= carpeta publica a todos

read only = yes

guest ok = no

browseable = no

valid users= @validos

write list = @escribe

A este directorio no se podrá acceder siendo un usuario anónimo, solo podrán acceder los usuarios definidos en Samba, todos pertenecen al grupo validos, y los miembros del grupo escribe serán los únicos que podrán escribir.

Ahora configuraremos la carpeta que solo el dueño y los miembros del grupo admines puedan modificar y ver, y el usuario suser podrá acceder pero solo podrá leer los datos

[**paraAdmin**]

path=/**samba/soloAutWrite**

comment=solo admin y root

read only = no

guest ok = no

browseable = no

valid users = @admines, suser

write list = @admines

Reiniciamos el servicio, para que los cambios tomen efecto

Systemctl restart smbd.services

ó

service smbd restart && service nmbd restart

Ahora iremos a Windows

Podemos ejecutar la llamada a alguna de las carpetas ejecutando una nueva tarea

Windows+R

Y escribiendo la dirección ip con la carpeta especifica, esto nos dará un acceso a la carpeta pero no agregara la ubicación al sistema de archivos

\\IP\SHAREFOLDER

O en el explorador de archivos ingresando la ip, esto nos mostrara todas las carpetas que tengan la bandera browseable = yes

\\IP

\\IP\SHAREFOLDER

Esto nos dará acceso al sistema de archivos compartido, pero no tendremos un enlace permanente al servido, es decir, siempre deberemos indicar el path con su dirección ip y/o carpeta específica para acceder.

Para agregar un enlace permanente, en Windows 10, debemos estar en el equipo agregar una unidad de red y especificar el ip o dominio y la carpeta especifica a la que queremos vincular

\\192.168.1.17\public

\\192.168.1.17\paraAdmin

\\192.168.1.17\lectura

Para acceder debemos ingresar las credenciales necesarias, y se obtendrá el acceso y permisos definidos.

En esta experiencia, todas las carpetas serán visibles en el explorador de archivos, pero exigirá credenciales para acceder a los diferentes directorios. Si se hubiera definido browseable = no, deberemos indicar el path correspondiente para acceder al recurso.

Las carpetas a las cuales se definió guest ok = no, exigirán que se utilice el usuario y contraseña, existente en el servidor Samba para su acceso, pero aquellos usuarios o grupos de usuarios sin los permisos necesarios no podrán leer, escribir ni ejecutar ningún archivo o directorio.

|  |  |
| --- | --- |
| User | Group |
| Suser | Escribe, validos |
| Sreader | Sreader, validos |
| Swrite | Admines, validos |
| nobody | Nogroup |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Directorio/Usuario | suser | sreader | swrite | nobody |
| Public | RWX | Invalid user | RWX | Invalid user |
| paraAdmin | R | Invalid user | RWX | Invalid user |
| lectura | RWX | RX | RX | Invalid user |

Archivo smb.conf

[global]

## Browsing/Identification ###

   netbios name= so-tpb

# Change this to the workgroup/NT-domain name your Samba server will part of

   workgroup = WORKGROUP

# server string is the equivalent of the NT Description field

   server string = %h - Sistema servidor

# This will prevent nmbd to search for NetBIOS names through DNS.

   dns proxy = no

wins support=yes

encrypt passwords = yes

#### Networking ####

interfaces = 192.168.1.0/24 eth0

#### Debugging/Accounting ####

# This tells Samba to use a separate log file for each machine

# that connects

   log file = /var/log/samba/log.%m

# Cap the size of the individual log files (in KiB).

   max log size = 1000

# If you want Samba to only log through syslog then set the following

# parameter to 'yes'.

#   syslog only = no

# We want Samba to log a minimum amount of information to syslog. Everything

# should go to /var/log/samba/log.{smbd,nmbd} instead. If you want to log

# through syslog you should set the following parameter to something higher.

   syslog = 0

# Do something sensible when Samba crashes: mail the admin a backtrace

   panic action = /usr/share/samba/panic-action %d

####### Authentication #######

# Server role. Defines in which mode Samba will operate. Possible

# values are "standalone server", "member server", "classic primary

# domain controller", "classic backup domain controller", "active

# directory domain controller".

#

# Most people will want "standalone sever" or "member server".

# Running as "active directory domain controller" will require first

# running "samba-tool domain provision" to wipe databases and create a

# new domain.

   server role = standalone server

# If you are using encrypted passwords, Samba will need to know what

# password database type you are using.

   passdb backend = tdbsam

   obey pam restrictions = yes

# This boolean parameter controls whether Samba attempts to sync the Unix

# password with the SMB password when the encrypted SMB password in the

# passdb is changed.

   unix password sync = yes

# For Unix password sync to work on a Debian GNU/Linux system, the following

# parameters must be set (thanks to Ian Kahan <<kahan@informatik.tu-muenchen.de> for

# sending the correct chat script for the passwd program in Debian Sarge).

   passwd program = /usr/bin/passwd %u

   passwd chat = \*Enter\snew\s\*\spassword:\* %n\n \*Retype\snew\s\*\spassword:\* %n\n \*password\supdated\ssuccessfully\* .

# This boolean controls whether PAM will be used for password changes

# when requested by an SMB client instead of the program listed in

# 'passwd program'. The default is 'no'.

   pam password change = yes

# This option controls how unsuccessful authentication attempts are mapped

# to anonymous connections

   map to guest = bad user

############ Misc ############

# Allow users who've been granted usershare privileges to create

# public shares, not just authenticated ones

   usershare allow guests = yes

#======================= Share Definitions =======================

[public]

   path=/samba/publico

   comment= carpeta publica a todos

   read only = no

   guest ok = yes

   browseable = yes

   invalid users= sreader

write list= @validos

[lectura]

   path=/samba/soloLectura

   comment= carpeta de solo lectura

   read only = yes

   guest ok = no

   browseable= yes

   valid users= @validos

   write list = @escribe

[paraAdmin]

   path=/samba/soloAutWrite

   comment=solo admin y root

   read only = no

   guest ok = no

   browseable= yes

   valid users= @admines, suser

   write list = @admines

**Servidor de correo**

**Configuración DNS**

Intalaremos Bin9

Apt install bind9

Luego de la instalación comprobaremos el estado del servicio,

Service bind9 status

El servicio puede estar activo o inactivo, para mayor seguridad lo detendremos

Service bind9 stop

Ahora volveremos a modificar el archivo /etc/netplan/01-network-manager-all.yaml, agregando los datos del servidor DNS local

nameservers:

search: [estuviani.com]

***addresses: [192.168.1.27]***

Y ahora aplicamos la confirguracion

netplan apply

verificamos que se tomara correctamente

systemd-resolve –status

debemos ver que el resolv.conf, ubique el sevidor DNS, mirando el archivo *etc/*resolv.conf, veremos si nuestro servidor se encuentra cargado

cat *etc*/resolv.conf

# This file is managed by man:systemd-resolved(8). Do not edit.

#

# This is a dynamic resolv.conf file for connecting local clients to the

# internal DNS stub resolver of systemd-resolved. This file lists all

# configured search domains.

#

# Run "systemd-resolve --status" to see details about the uplink DNS servers

# currently in use.

#

# Third party programs must not access this file directly, but only through the

# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,

# replace this symlink by a static file or a different symlink.

#

# See man:systemd-resolved.service(8) for details about the supported modes of

# operation for /etc/resolv.conf.

nameserver 127.0.0.53

options edns0

search estuviani.com

como podemos observar el server no esta cargado, se encuentra el dominio al haber sido cargado en la instancia anterior de configuracion

por lo que utilizaremos el comando

resolvconf -u

para recargar los datos del resolv, si al volver a mostrar el contenido de resolv.conf, el nameserver no se agrego, podremos hacerlo, manualmente editando el archivo /etc/resolvconf/resolv.conf.d/head.

nameserver 192.168.1.27

modificaremos el orden de busqueda de resolucion, para que busque en el DNS y no en el host

nano *etc*/nsswitch.conf

hosts: files mdns4\_minimal [NOTFOUND=return] dns myhostname

hosts: dns files mdns4\_minimal [NOTFOUND=return] myhostname

**Configurar BIND9**

Para trabajar mas comodos nos moveremos al directorio bind

cd *etc*/bind/

dentro del directorio bind, encontraremos una serie de archivos los archivos

named.conf → este archivo contiene las indicaciones a los distintos archivos que incluira bind

.default-zones → almacena las zonas por defecto donde comenzara las busquedas

.options → contiene informacion general de bind9

.local → es un archivo en blanco donde se deberan agregar los paramentros para la resolucion de nombres

db.roof → contiene los servidores raiz que estan distribuidos por el mundo

Carga del archivo named.conf.local

//Zona directa para el dominio estuviani.com

zone "estuviani.com" {

type master;

file "/etc/bind/db.estuviani.com";

};

//Zona inversa para la red 192.168.1.0

zone "1.168.192.in-addr.arpa" {

type master;

file "/etc/bind/db.1.168.192";

};

ahora utilizaremos el archivo plantilla db.local, generando el archivo del domino db.estuviani.com

cp db.local db.estuviani.com

ahora editamos el archivo dp.estuviani.com

;

; fichero de Regisros de recursos BIND para la zona estuviani.com

;

$TTL 604800

@ IN SOA servidor.estuviani.com. root.estuviani.com. (

2 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS servidor.estuviani.com.

servidor IN A 192.168.1.27

router IN A 192.168.1.1

mail IN A 192.168.1.27

server IN CNAME servidor.estuviani.com.

estuviani.com. IN MX 10 mail

Ahora crearemos y cargaremos el archivo para la busqueda inversa

cp db.estuviani.com db.1.168.192

;

; fichero de Regisros de recursos BIND para la zona inversa 1.168.192

;

$TTL 604800

@ IN SOA servidor.estuviani.com. root.estuviani.com. (

2 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS servidor.estuviani.com.

27 IN PTR servidor.estuviani.com.

1 IN PTR router.estuviani.com.

27 IN PTR mail.estuviani.com.

27 IN PTR server.estuviani.com.

Ahora verificaremos si la sintaxis esta correcta, no funcional

verificamos la sintaxis del archivo named.conf.local

named-checkconf named.conf.local

verificamos los archivos de zona

named-checkzone estuviani.com db.estuviani.com

named-checkzone 1.168.169.in-addr.arpa db.1.168.192

Ya comprobado que la sintaxis esta bien iniciaremos el servicio bind9

service bind9 restart

Verificamos el estado del servicio

service bind9 status

Haremos una pruebas para asegurar que el DNS funciones correctamente

ping -c 4 192.168.1.27

si hay respuesta estamos ok

ping -c 4 server

esto permitira verificar si la resolucion de nombre funciona, podemos probar con el nombre completo servidor.estuviani.com

ping -c 4 server.estuviani.com

Ahora probaremos hacer una consulta para que consocamos el dirección del servidor

host server

host mail

con nslookup, podemos conocer la ip como asi tambien el nombre de dominio

nslookup mail

esto nos permitira conocer si se realizo un salto entre el servidor local o un servidor externo

con el comando dig, podemos obtener, varios datos del servidor

dig @192.168.1.27 mail.estuviani.com

Crearemos dos usuarios para el correo admin y help, ya que los ususarios para el servidor samba no poseen directorio en el servidor

adduser admin

adduser help

para comprobar que se crearan, iremos al directorio home y ejecutaremos un ls, alli deberiamos ver los directorios de los usuarios creados

**~~Creacion de certificados ssl~~**

~~creamos los certificados, debe existir la ruta que declaramos en la ubicación de los cerificados /etc/pki/tls/certs/~~

~~openssl req -config /usr/lib/ssl/openssl.cnf -new -nodes -keyout mail.estuviani.com.key -out mail.estuviani.com.pem~~

~~mv mail.estuviani.com.pem certs/~~

~~mv mail.estuviani.com.key private/~~

~~openssl x509 -signkey private/mail.estuviani.com.key -in certs/mail.estuviani.com.pem -req -days 3650 -out mail.estuviani.com.crt~~

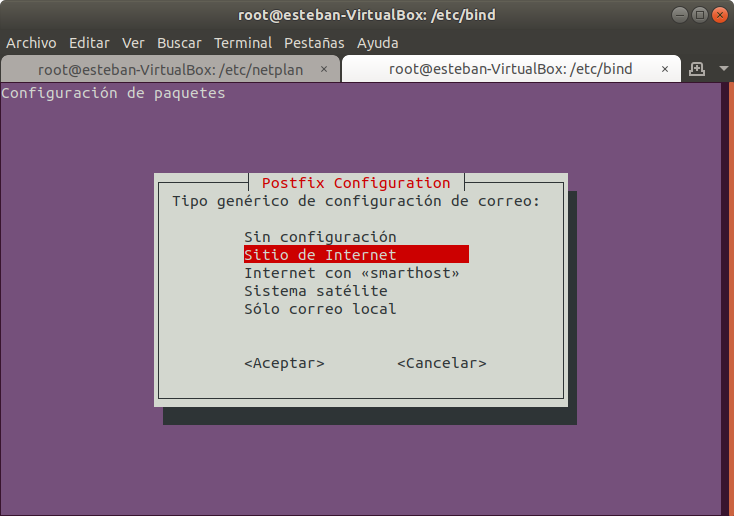
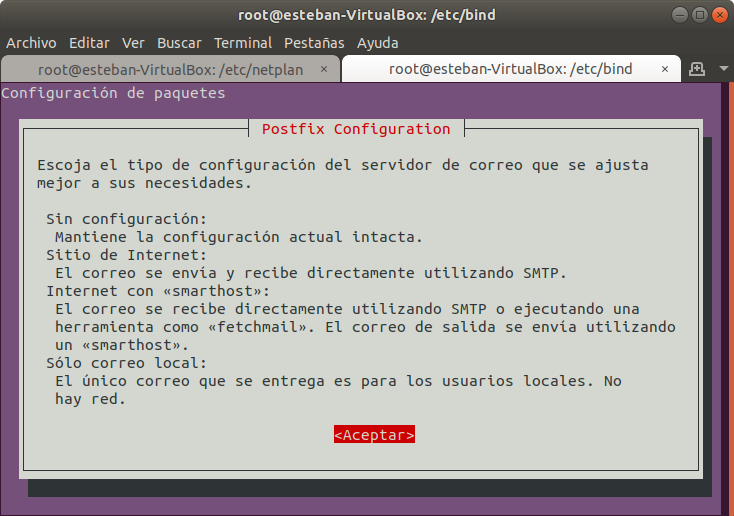
~~mv mail.estuviani.com.crt certs/~~

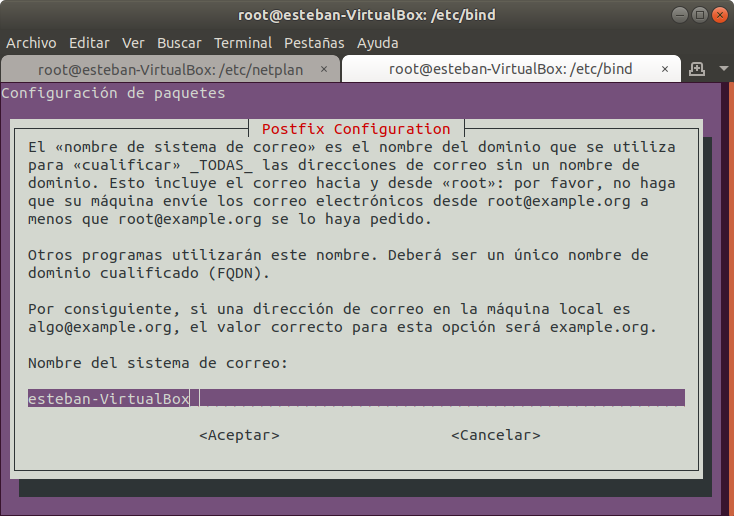
~~so-estu~~

**Intalacion y configuración del servidor Postfix**

ahora instalaremos el servidor Postfix

apt install postfix

Seleccionamos la opcion sitio de internet ya que deseamos que utilice el SMTP

, agregamos el dominio, por defecto colocara el dominio que posee el equipo, que no es el mismo que esta definido en el DNS, reemplazamos y nos movemos con TAB y confirmamos con la barra espaciadora.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Verificamos el estado del servicio

service postfix status

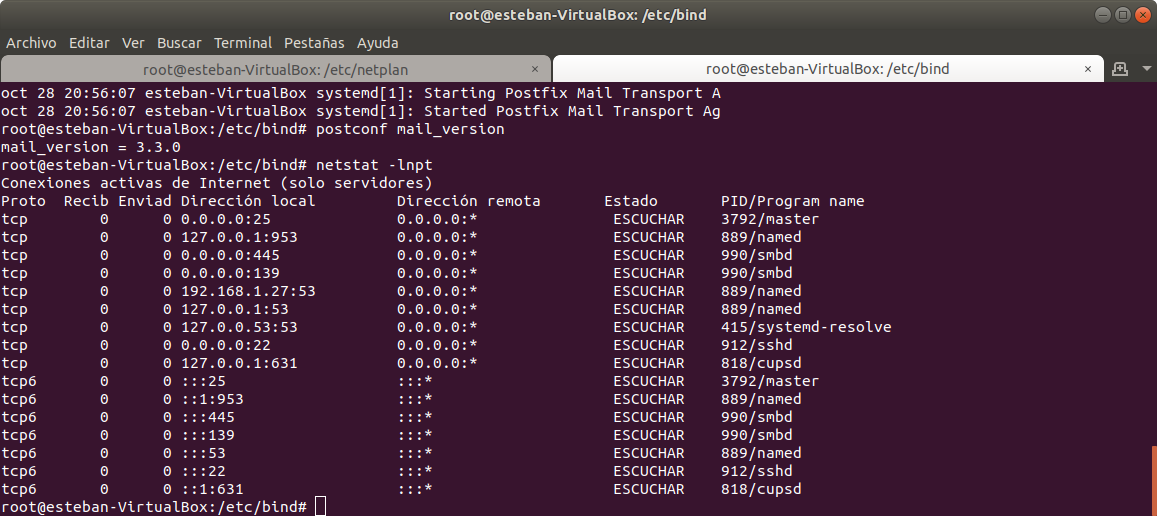
Luego verremos que version de postfix se instalo

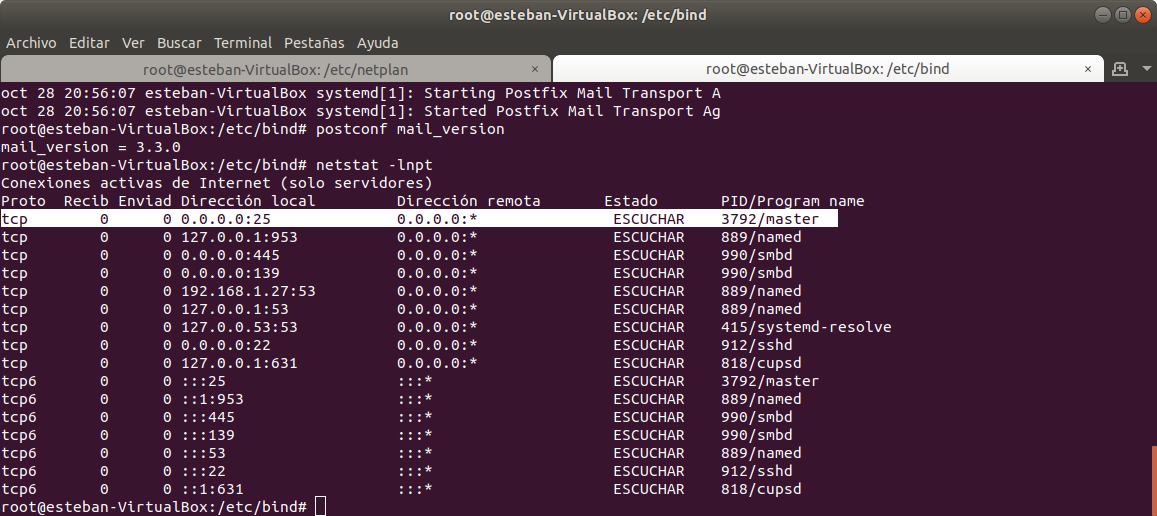
postconf mail\_version

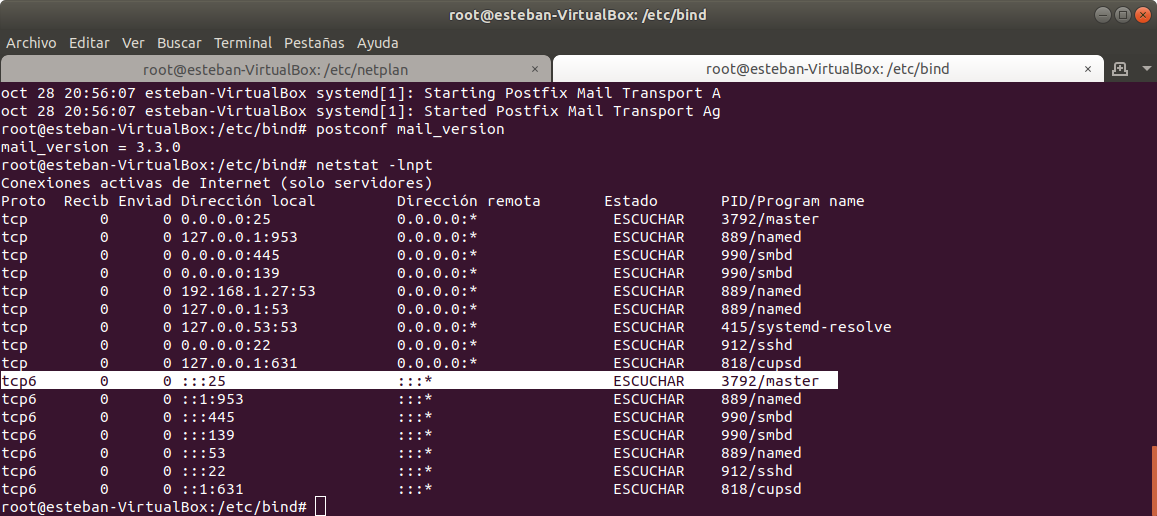
en este caso la 3.3.0

veremos si el servidor esta escuchando en el puerto 25, que es el por defecto, de postfix

netstat -lnpt







Debemos verificar que el firewall, no este bloqueando el puerto 25.

Para esto debemos acceder desde otro equipo y utilizar el comando

nc -zv 192.168.1.27 25

Al no estar el puerto 25, de entrada habilitado debemos habilitarlo

con el comando ufw podemos hablitar y deshabilitar puertos

ufw allow 25/tcp

Ahora modificaremos el archivo de confirguracion main,cf

*etc*/postfix/main.cf

# TLS parameters

smtpd\_tls\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

smtpd\_tls\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key

**smtp\_use\_tls = yes**

**smtpd\_tls\_security\_level = may**

**smtpd\_tls\_loglevel = 1**

**smtpd\_tls\_received\_header = yes**

smtpd\_tls\_cert\_file=/etc/pki/tls/**certs/mail.estuviani.com.crt**

smtpd\_tls\_key\_file=/etc/pki/tls/**private/mail.estuviani.com.key**

**smtpd\_tls\_session\_cache\_timeout = 3600s**

# information on enabling SSL in the smtp client.

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

myhostname = **mail**.estuviani.com

alias\_maps = hash:/etc/aliases

alias\_database = hash:/etc/aliases

myorigin = /etc/mailname

mydestination = $myhostname, estuviani.com, localhost.localdomain, localhost

relayhost =

mynetworks = **192.168.1.0/24** 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128

mailbox\_size\_limit = 0

recipient\_delimiter = +

inet\_interfaces = all

inet\_protocols = all

Agreganremos la siguiente linea al archivo main.cf para que se almacenen los mail en un directorio dentro de cada usuairio

home\_mailbox = Maildir/

recargamos el servicio postfix

service postfix reload

podemos revisar la configuracion usando el comando

postconf -n

ahora instalaremos las utilidades para mails

# apt install mailutils

Ahora enviaremos un mail por consola y veremos que se creara un nuevo directorio en el directorio del usuario, llamador Maildir, donde se almacenaran los correos

echo "SUbject:COrreo Maildir" | sendmail [admin@estuviani.com](mailto:admin@estuviani.com)

cd *home*/admin/Maildir/

alli veremos que hay 3 directorios, cur, new y tmp. En new se almacenara todo correo entrante; en cur se colocaran los mail que fueron vistos, leido o no leidos;

Entramos al directorio new, y veremos que hay un archivo, el correo entrante, y veremos su contenido con el comando cat

Return-Path: <root@estuviani.com>

X-Original-To: admin@estuviani.com

Delivered-To: admin@estuviani.com

Received: by mail.estuviani.com (Postfix, from userid 0)

id 1FD24603E2; Sat, 29 Oct 2022 20:49:44 -0300 (-03)

SUbject:COrreo Maildir

Message-Id: <20221029234945.1FD24603E2@mail.estuviani.com>

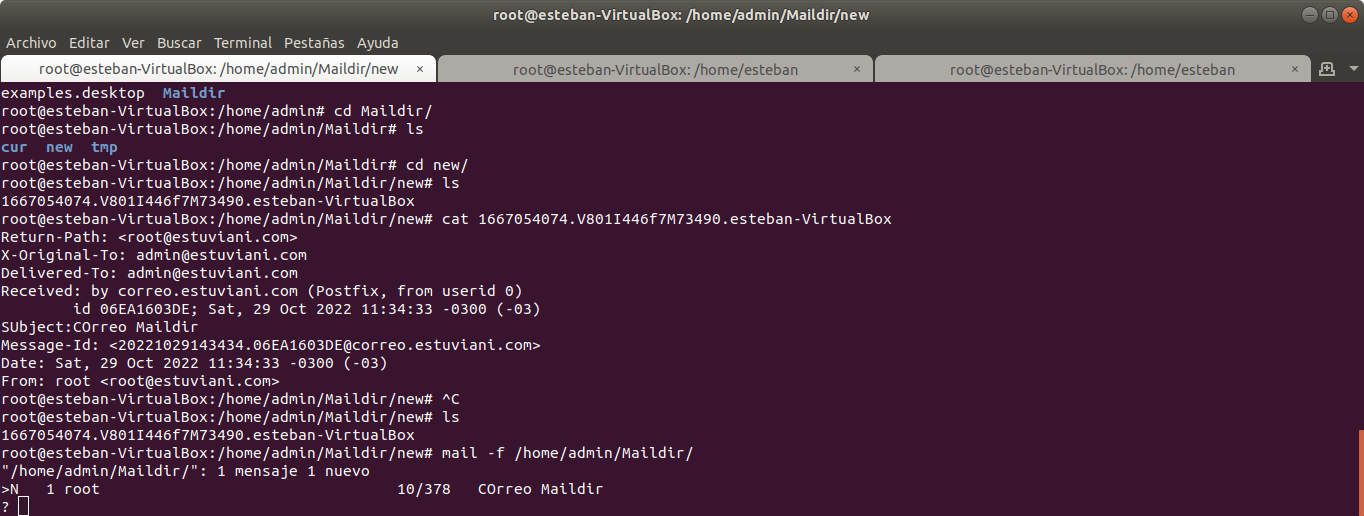
Date: Sat, 29 Oct 2022 20:49:44 -0300 (-03)

From: root <root@estuviani.com>

Utilizaremos una de las utilidades de mailutils, el comando mail, para entrar y ver los correos que tiene el usuario.

Si se ejecuta tomara como usuario del correo el usuario que este ejecutando el comando, si queremos podemos cambiar de usuario o podemos pasarle el parametro -f, e indicar la ubicación del directorio Maildir de usuario

# mail -f *home*/admin/Maildir/

Alli podemos ver que, el promp cambio a ?, y que hay un correo nuevo proveniente del root, que aun no hemos leido (N), y que podremos leer el mismo eligiendo su numero de mail (1)

? 1

Return-Path: <root@estuviani.com>

X-Original-To: admin@estuviani.com

Delivered-To: admin@estuviani.com

Received: by mail.estuviani.com (Postfix, from userid 0)

id 1FD24603E2; Sat, 29 Oct 2022 20:49:44 -0300 (-03)

SUbject: COrreo Maildir

Message-Id: <20221029234945.1FD24603E2@mail.estuviani.com>

Date: Sat, 29 Oct 2022 20:49:44 -0300 (-03)

From: root <[root@estuviani.com](mailto:root@estuviani.com)>

Ahora podemos eliminar el correo(d NUMERO), volver a la lista de correos (h) o salir (q)

? h

>R 1 root NA/378 COrreo Maildir

como vemos se marco el correo como leido (R)

? q

si se envia un correo y no hemos salido el mismo no se mostrara, por lo que debemos salir.

Enviamos otro correo para ver como se modifica el entorno

echo "Subject:Correo para admin" | sendmail [admin@estuviani.com](mailto:admin@estuviani.com)

y volvemos a utilizar mail

mail -f /home/admin/Maildir/

"/home/admin/Maildir/": 2 mensajes 1 nuevo

1 root 10/378 COrreo Maildir

>N 2 root 10/381 Correo para admin

? q

si salimos y volvemos a entrar el mail nuevo(N) sera marcado como no leido (U)

1 root 10/378 COrreo Maildir

>U 2 root 10/381 Correo para admin

**Instalación Dovecot**

Dovecot, nos permite utilizar tanto imap o pop3. Utilizaremos imap, es decir consultaremos los mail del servidor, y no los descargaremos en el equipo

# apt install dovecot-core dovecot-imapd

Verificamos la version de dovecot instalada

dovecot --version

2.2.33.2 (d6601f4ec)

veremos los protocolos que estan instalados en docevot, en este caso solo el imap, para eso veremos el archivo de configuración para conocer donde se almacenan los protocolos

cat *etc*/dovecot/dovecot.conf | more

y buscaremos la linea

# Enable installed protocols

!include\_try **/usr/share/dovecot/protocols.d/\*.protocol**

ahora haremos un cat a esa ubicación

cat **/usr/share/dovecot/protocols.d/\*.protocol**

protocols = $protocols imap

**CONFIGURAR EL SSL**

**gedit /etc/dovecot/conf.d/10-ssl.conf**

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>

ssl = **required**

ssl\_cert = </etc/dovecot/private/dovecot.pem

ssl\_key = </etc/dovecot/private/dovecot.key

ssl\_cert = **</etc/pki/tls/certs/mail.estuviani.com.pem**

ssl\_key = **</etc/pki/tls/private/mail.estuviani.com.key**

gedit /etc/dovecot/conf.d/10-mail.conf

editar mail\_location, descomentando la linea

mail\_location = maildir:~/Maildir

y comentar

#mail\_location = mbox:~/mail:INBOX=/var/mail/%u

Recargamos el servicio

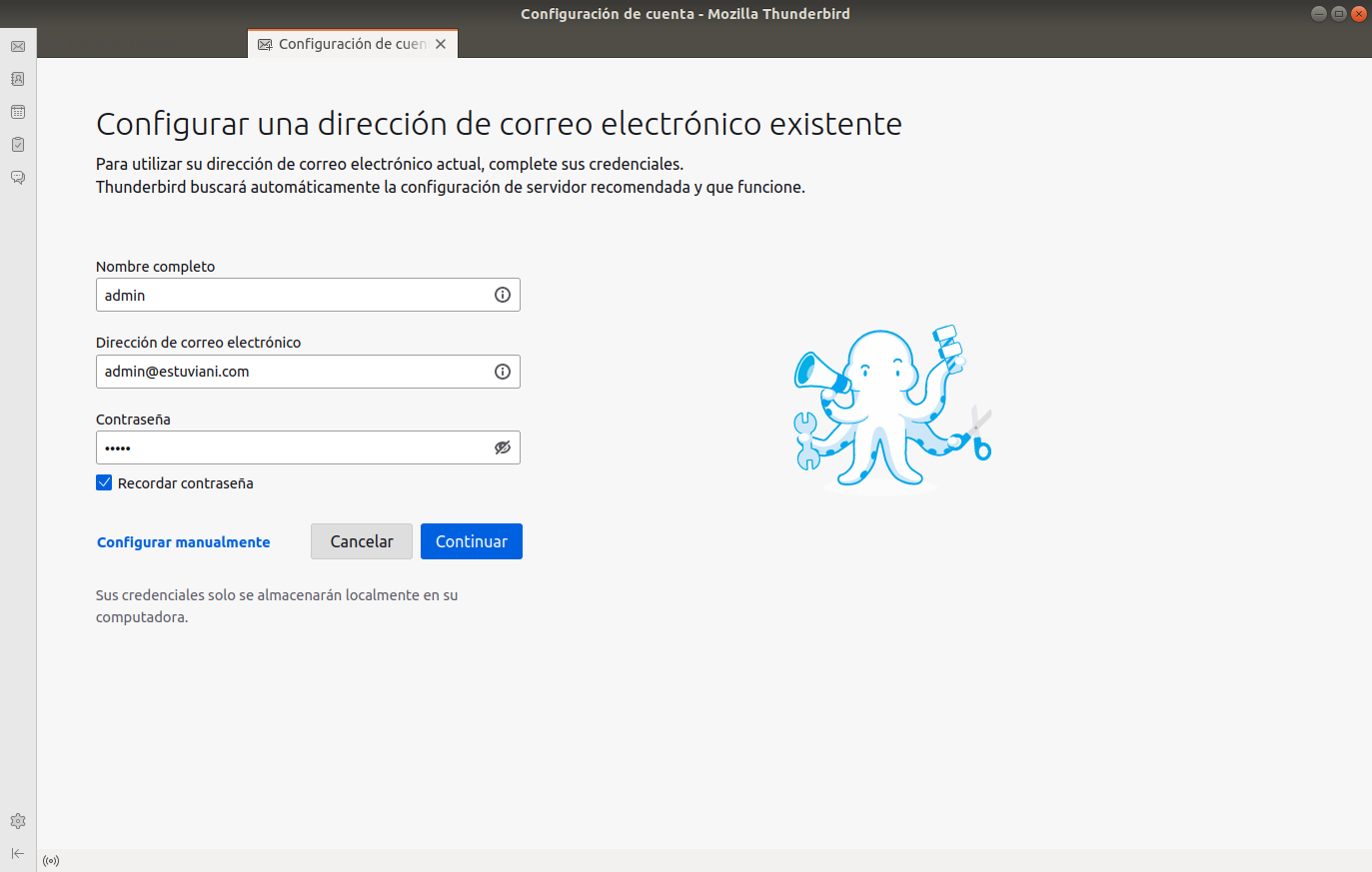
systemctl start dovecot && systemctl enable dovecot

**Ahora configuraremos un cliente de correo**

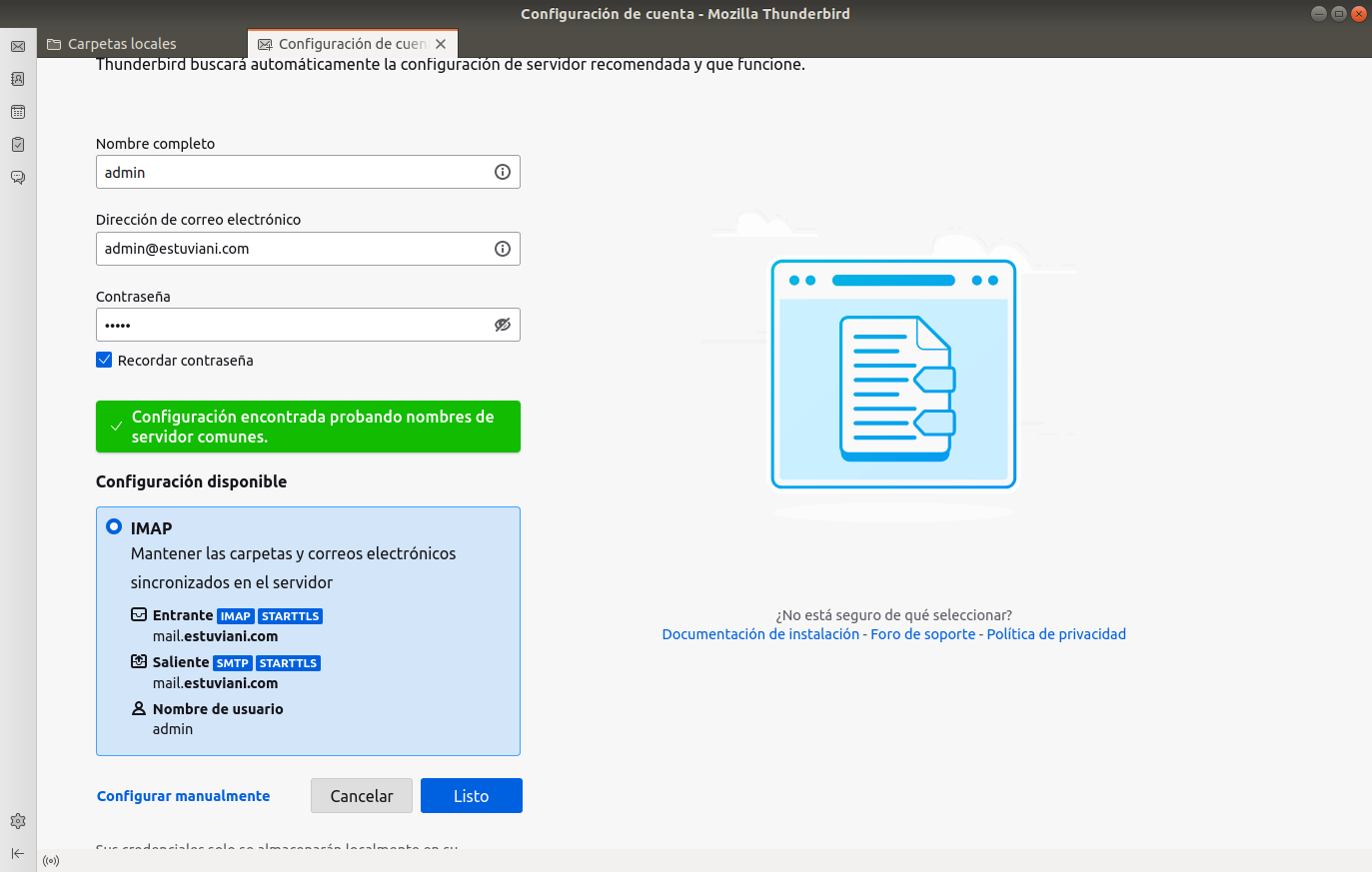
Utilizaremos Thunderbd, por lo que si no lo tenemos instalado ejecutaremos

apt install thunderbird

abriremos Thunderbird y agregaremos el correo, administrador



ahora debemos cargar la configuracion del servidor de correo



Como notamos el cliente identifico los datos del servidor, si no fuera asi deberemos ingresarlos a mano

Al continus nos mustra la siguiente advertencia agregamos la excepcion



Ahora falta probar que desde un cliente externo, se pueda acceder al mail

estoy tratando pero no me toma la resolucion de nombres del servidor desde afuera, por lo que dudo que funcione al usar el mail

Para permitir las conexiones desde afuera debemos habilitar el puerto imap 143/tcp y el puerto DNS 53/tcp

ufw allow 53/tcp

ufw allow 143/tcp

comprobamos los puestos que estan abieros

ufw status

Hasta Acción Desde

----- ------ -----

25/tcp ALLOW Anywhere

53/tcp ALLOW Anywhere

143/tcp ALLOW Anywhere

25/tcp (v6) ALLOW Anywhere (v6)

53/tcp (v6) ALLOW Anywhere (v6)

143/tcp (v6) ALLOW Anywhere (v6)

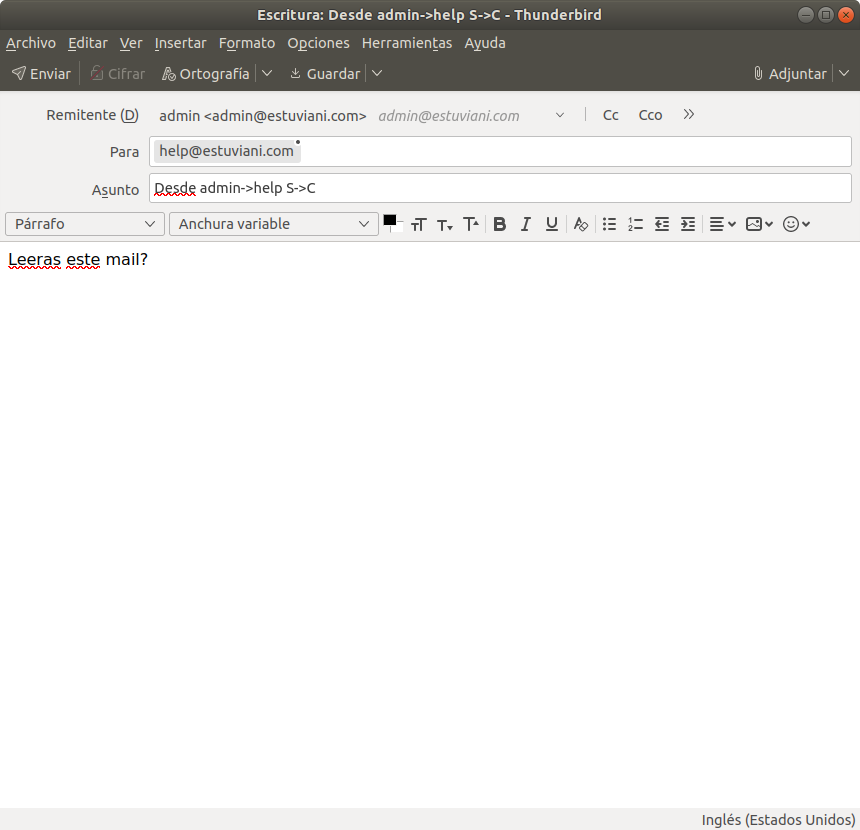
Luego en el equipo cliente se debe definir la direccion IP, del servidor DNS, reiniciamos el servicio de networking, para asegurarnos que tome los cambios

service networking restart

Ahora abrimos el cliente de correo del equipo cliente y colocamos los datos de la cuenta

si todo salio bien tendremos la cuenta configurada en el cliente.

Por lo que ahora tenemos dos cuentas de correo, la cuenta admin en el servidor y la cuenta help en el cliente, ahora probaremos enviar un correo entre los dos clientes de correo



Si no anda modificar dovecot.conf y descomentar lintener



Nos saltara un excepcion ya que no usamos SSL

Por el moemnto agregaremos la excepcion

Certificado SSL V2

Puerto SMTP SSL 587

IMAP SSL 993

mkdir /*et*c/pki/tls

chown root:root /*etc*/pki/tls

chmod 700 /*etc*/pki/tls

openssl req -new -newkey rsa:2048 -nodes -keyout mail.eviani.key -out mail.eviani.csr

openssl genrsa -des3 -out myCA.key 2048

openssl req -x509 -new -nodes -key myCA.key -sha256 -days 365 -out myCA.pem

openssl x509 -req -in mail.eviani.csr -CA myCA.pem -CAkey myCA.key -CAcreateserial -out mail.eviani.com -days 365 -sha256

openssl req -new -newkey rsa:2048 -nodes -keyout mail.mydomain.key -out mail.mydomain.csr

openssl genrsa -des3 -out myCA.key 2048

openssl req -x509 -new -nodes -key myCA.key -sha256 -days 1825 -out myCA.pem

openssl x509 -req -in mail.mydomain.csr -CA myCA.pem -CAkey myCA.key -CAcreateserial -out mail.mydomain.pem -days 1825 -sha256

***postfix*/main.cf**

smtpd\_use\_tls = yes

smtpd\_tls\_cert\_file = /*etc*/pki/tls/mail.eviani.pem

smtpd\_tls\_key\_file= /etc/pki/tls/mail.eviani.key

smtpd\_tls\_eecdh\_grade = strong

smtpd\_tls\_protocols= !SSLv2, !SSLv3, !TLSv1, !TLSv1.1

smtpd\_tls\_mandatory\_protocols= !SSLv2, !SSLv3, !TLSv1, !TLSv1.1

smtpd\_tls\_mandatory\_ciphers = high

smtpd\_tls\_security\_level=may

smtpd\_tls\_ciphers = high

tls\_preempt\_cipherlist = yes

smtpd\_tls\_mandatory\_exclude\_ciphers = aNULL, MD5 , DES, ADH, RC4, PSD, SRP, 3DES, eNULL

smtpd\_tls\_exclude\_ciphers = aNULL, MD5 , DES, ADH, RC4, PSD, SRP, 3DES, eNULL

smtp\_tls\_mandatory\_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1

smtp\_tls\_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1

master.cf

descomentar lineas

***dovecot*/dovecot.conf**

ssl = required

ssl\_cert =</etc/pki/tls/mail.eviani.pem

ssl\_key = </etc/pki/tls/mail.eviani.key

Test

openssl s\_client -connect mail.eviani.com:993

openssl s\_client -starttls imap -connect mail.eviani.com:143

openssl s\_client -starttls smtp -connect mail.eviani.com:587

chmod 600 /*etc*/pki/tls/\*

Glosario

<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

https://opensource.com/article/20/4/securing-linux-email