.Instalación desde un DVD/CD-ROM

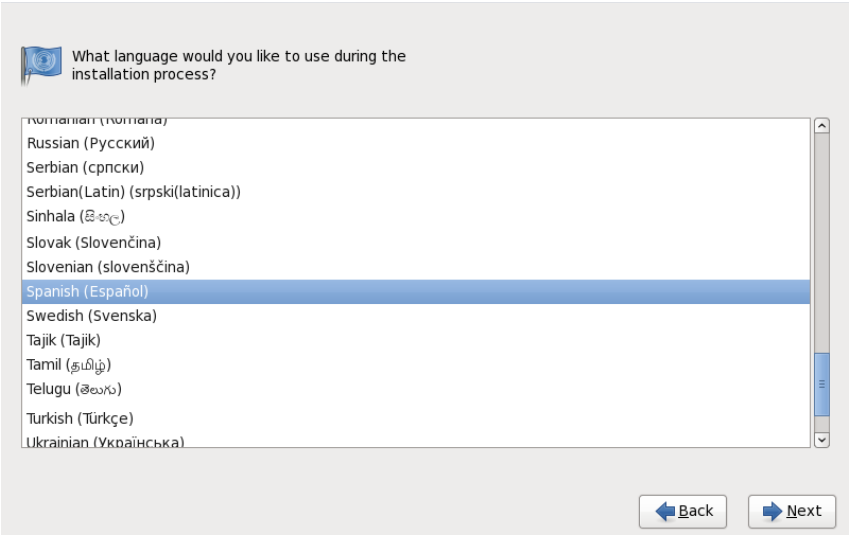
Para instalar Fedora desde un DVD/CD-ROM, introduzca el DVD o CD #1 en el dispositivo de DVD/
CD-ROM e inicie su sistema desde DVD/CD-ROM.

Si el dispositivo de DVD/CD-ROM es encontrado y cargado, el programa de instalación le ofrecerá
la opción de revisar la integridad del DVD/CD-ROM. Este proceso tomará algún tiempo. Usted tiene la opción de saltarse este paso. Sin embargo, si luego encuentra problemas con el programa de instalación, usted deberá reiniciar la máquina y ejecutar la revisión del medio antes de solicitar soporte.

La pantalla de Bienvenida no le pide ninguna información.

Selección del lenguaje

El idioma que escoja aquí será el idioma predeterminado para el sistema operativo una vez lo instale. La selección del idioma apropiado también le ayudará a configurar el huso horario en una etapa posterior del proceso de instalación. El programa de instalación intentará definir el huso horario adecuado basándose en lo que usted especifique en la pantalla.

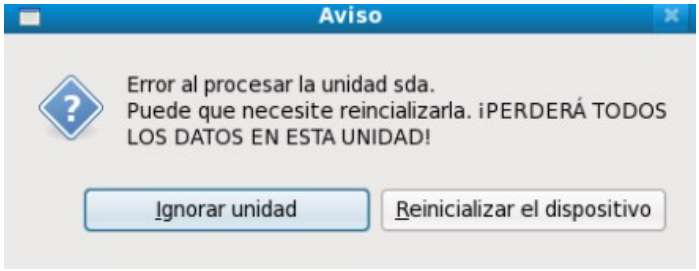


Seleccione configuración del teclado

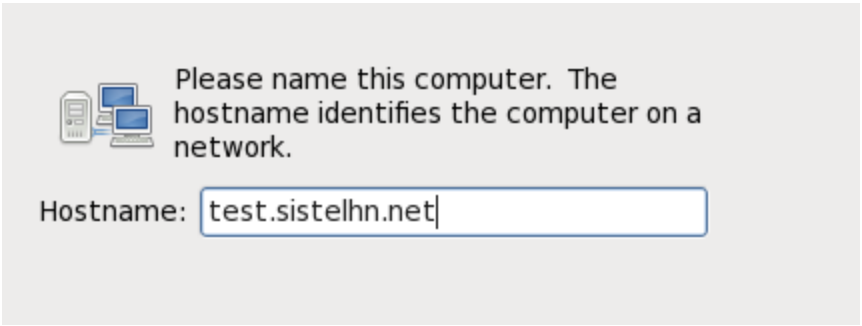
Utilizando el ratón, seleccione el tipo de teclado que le gustaría utilizar durante el proceso de instalación y como teclado predeterminado del sistema.

Inicializar el Disco Duro

Si el programa de instalación no encuentra particiones legibles en los discos rígidos existentes, pregunta si debe inicializar el disco rígido. Esta operación provoca que cualquier dato que se encuentre en el disco sea ilegible. Si su sistema tiene un nuevo disco rígido sin ningún sistema operativo instalado, o si ha eliminado todas las particiones, responda Reinicializar disco.

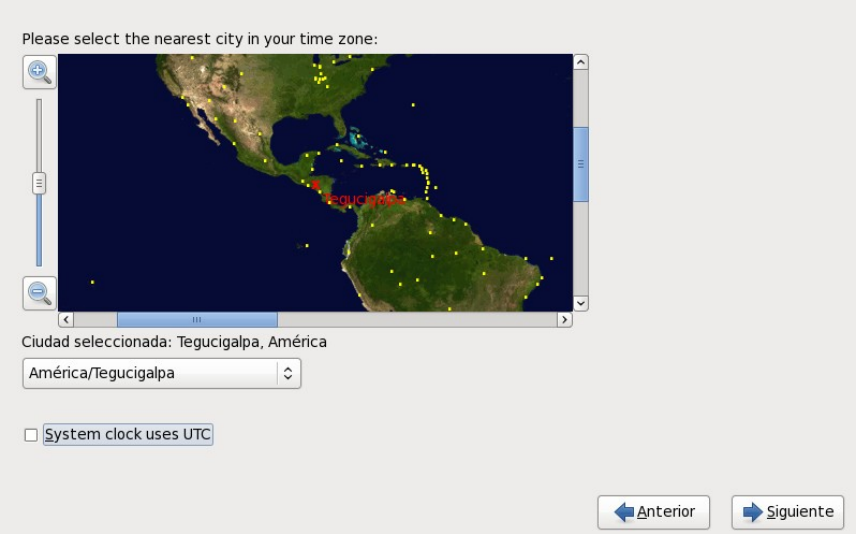


El configurador le pregunta un nombre de equipo y un nombre de dominio para esta computadora, en el formato nombredepc.nombrededominio. Muchas redes tienen el servicio DHCP (Protocolo de Configuración Dinámica de Equipo) que provee automáticamente la información de nombre de dominio a los sistemas, dejando al usuario ingresar el nombre de equipo. A no ser que tenga una necesidad puntual de modificar tanto el nombre de su equipo como el de su dominio, la configuración predeterminada lo define como localhost.localdomain, que para la mayoría de los usuarios es una opción aceptable.



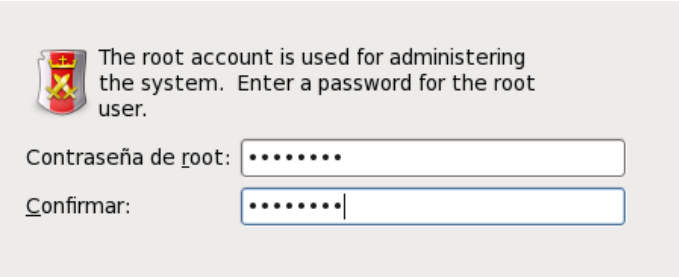
Configuración del uso de horario

Especifique la zona horaria aún si planea usar NTP (Protocolo de Hora de Red) para mantener la precisión del reloj de su sistema. Configure su huso horario seleccionando la ciudad más cercana a la ubicación física de su computador. Haga clic sobre el mapa para ampliar la región geográfica.



Poner la contraseña root

La configuración de la cuenta y la contraseña root es uno de los pasos más importantes durante la instalación. Su cuenta root es similar a la cuenta del administrador usada en las máquinas Microsoft Windows. La cuenta root es usada para instalar paquetes, actualizar RPMs y realizar la mayoría de las tareas de mantenimiento del sistema. Ingresando como root le da control completo del sistema.

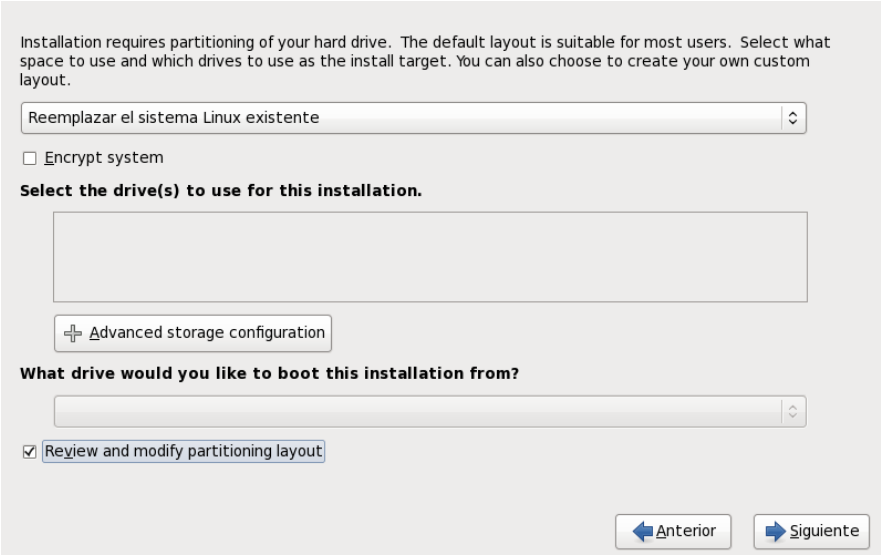


Utilice la cuenta de root tan sólo para la administración de su sistema. Cree una cuenta que no sea root para uso general y ejecute su - para actuar como root cuando

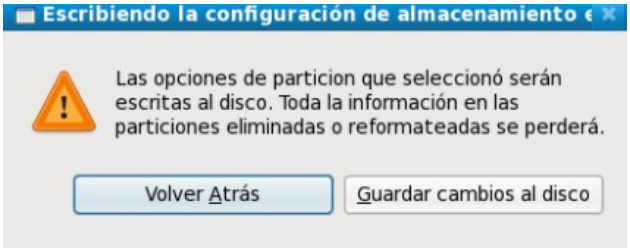
necesite configurar algo de forma rápida. Estas reglas básicas minimizarán las posibilidades de que un comando incorrecto o un error de tipografía puedan dañar su sistema.

Particionamiento del Disco Duro

En esta pantalla puede elegir entre crear una disposición predeterminada o realizar un particionamiento manual utilizando la opción Crear un diseño personalizado. Las primeras cuatro opciones le permiten realizar una instalación automatizada sin necesidad de que usted particione el disco. Si no se siente seguro durante la partición manual de su disco, se aconseja que no cree una disposición personalizada y que deje que el programa de instalación haga las particiones por usted.



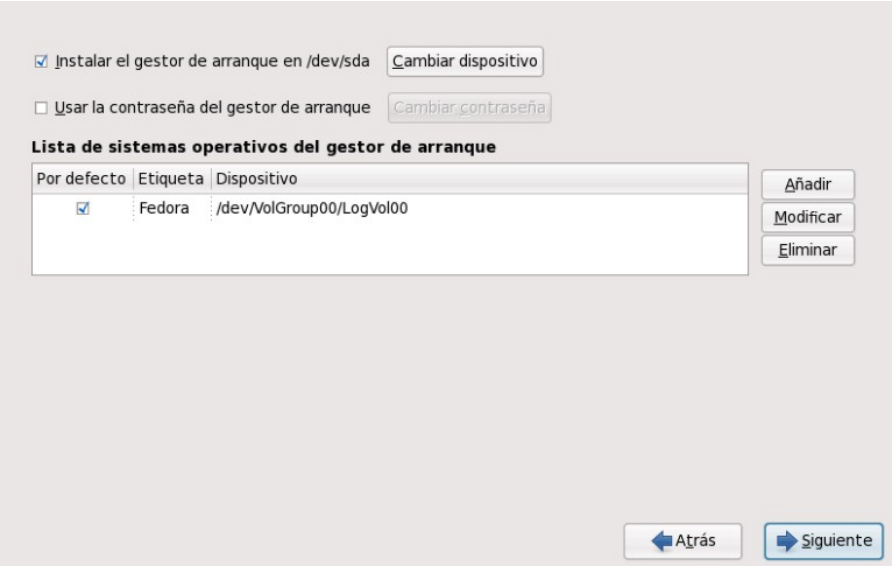
El instalador le pedirá que confirme las opciones de particionamiento elegidas. Haga clic en Guardar los cambios en el disco para permitir que el instalador realice las particiones elegidas en su disco rígido, e instale Fedora.



Configuración del Gestor de Arranque

GRUB (GRand Unified Bootloader), que se instala por defecto, es un gestor de arranque muy potente ya que puede cargar una gran variedad de sistemas

operativos gratuitos así como sistemas operativos propietarios con el sistema de cargado en cadena (el mecanismo para cargar sistemas operativos no soportados mediante la carga de otro gestor de arranque, tal como DOS o Windows).

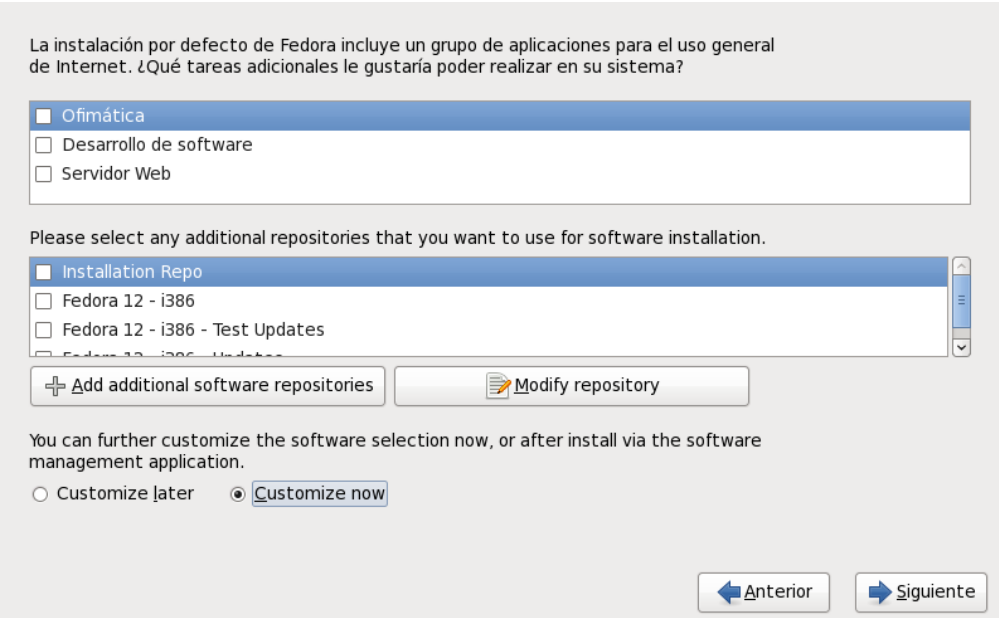


Si no hay ningún sistema operativo en su computadora, o está completando la eliminación de otros sistemas operativos, el programa de instalación instalará GRUB como su cargador de arranque sin ninguna intervención.

Selección de los paquetes

Ahora que ha realizado la mayoría de sus selecciones para la instalación, está listo para confirmar la selección predeterminada de paquetes o personalizar los paquetes para su sistema.

Primero, aparecerá la pantalla Instalación de Paquetes Predeterminados que detalla el conjunto de paquetes predeterminados configurados para la instalación de Fedora.



Por defecto, el proceso de instalación de Fedora carga una selección de software que es apropiado para un sistema de escritorio. Para incluir o quitar software para tareas comunes, seleccione los elementos de la lista:

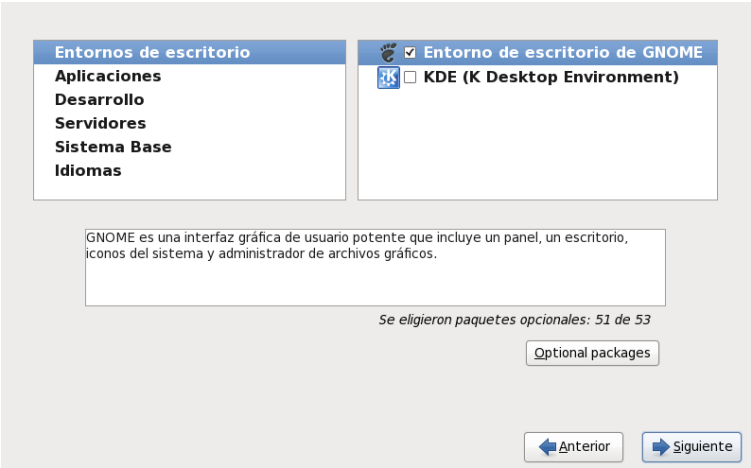
Oficina y Productividad
Esta opción ofrece la suite de productividad OpenOffice.org, la aplicación Planner para gestión de proyectos, herramientas gráficas como GIMP, y aplicaciones multimedia.

Software de Desarrollo
Esta opción provee las herramientas necesarias para compilar software en su sistema Fedora.

Servidor Web
Esta opción provee el servidor Web Apache

Para seleccionar un componente, haga clic en la casilla de verificación al lado de éste.

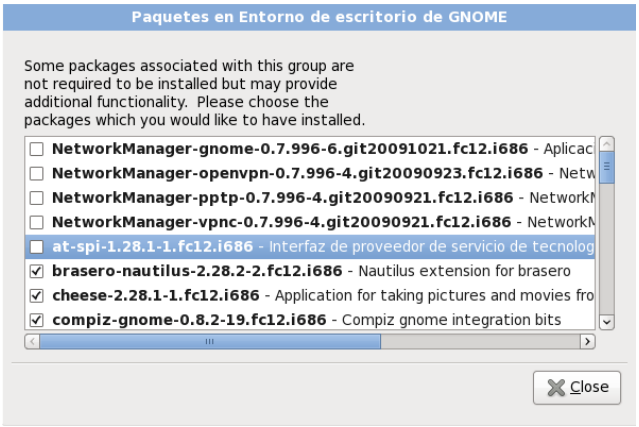
Para personalizar su grupo de paquetes aún más, seleccione la opción Personalizar ahora en la pantalla. Haga clic en Siguiente para ir a la pantalla Selección de Grupos de Paquetes.



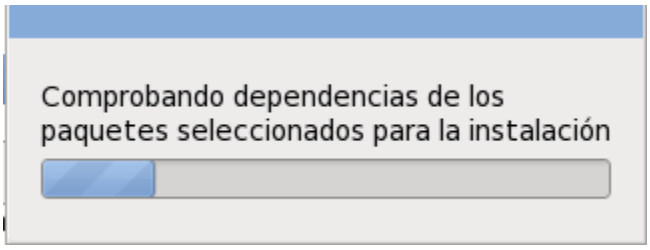
Para ver los grupos de paquetes por categoría, seleccione la categoria desde la lista a la izquierda. La lista a la derecha muestra los grupos de paquetes de la categoría seleccionada actualmente.

Para especificar un grupo de paquetes para su instalación, tilde la casilla que se encuentra junto al grupo que desea instalar. La casilla cerca del borde inferior de la pantalla muestra los detalles del grupo de paquetes que actualmente está seleccionado. Ninguno de los paquetes de un grupo serán instalados a menos que la casilla perteneciente a ese grupo sea tildada. Si selecciona un grupo de paquetes, Fedora automáticamente instala los paquetes imprescindibles y básicos de ese grupo. Para modificar los paquetes opcionales que de un grupo determinado serán instalados, seleccione el botón Paquetes Opcionales bajo la descripción de ese grupo. Luego utilice la casilla junto a los nombres de los paquetes individuales para cambiar la selección.

Después de haber elegido los paquetes deseados, seleccione Siguiente para continuar. Fedora verifica su selección, y automáticamente añade cualquier paquete extra que sea necesario para utilizar el software que usted ha seleccionado. Cuando finalice de elegir los paquetes, haga click sobre Cerrar para guardar su selección de paquetes optativos, y regrese a la pantalla principal de selección de paquetes.



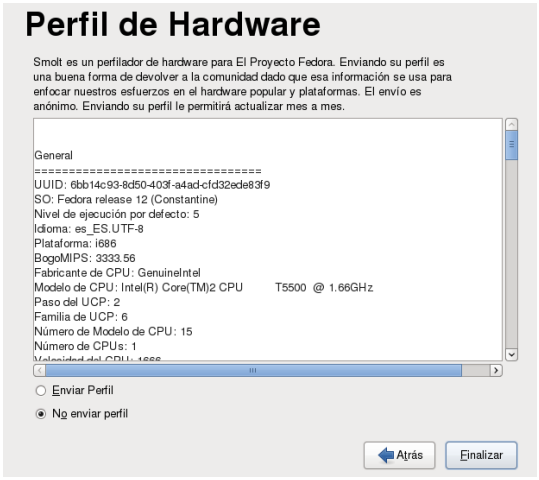
Una vez seleccionados los paquete comprobara las dependencias.



Luego de comprobar las dependencias empezara el proceso de instalación.

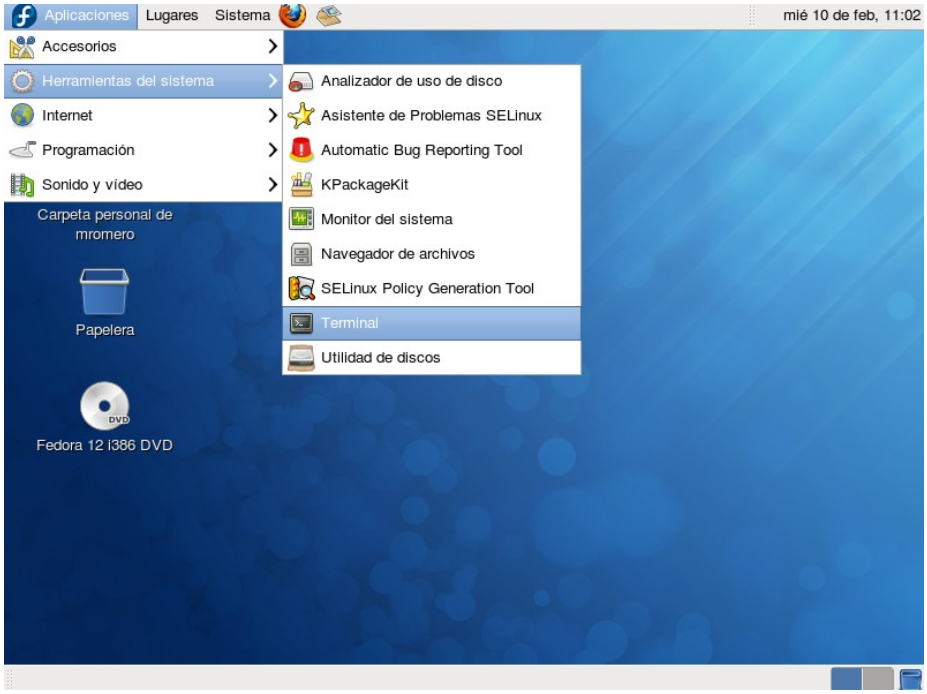
Al terminar le pedirá reiniciar el Sistema Operativo.

Luego ya estarás listo para usar Fedora, solo tienes que crear un usuario verificar que la fecha y hora concuerde con la actual y mandar la información de perfil de hardware para contribuir con la comunidad de Fedora.

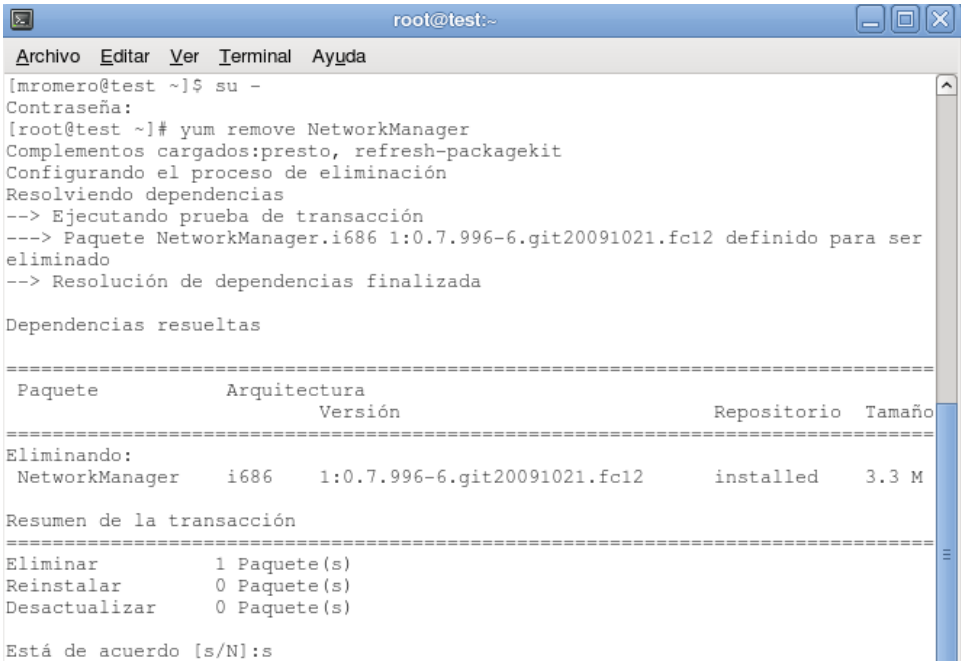


Configurando el Servidor de Correos

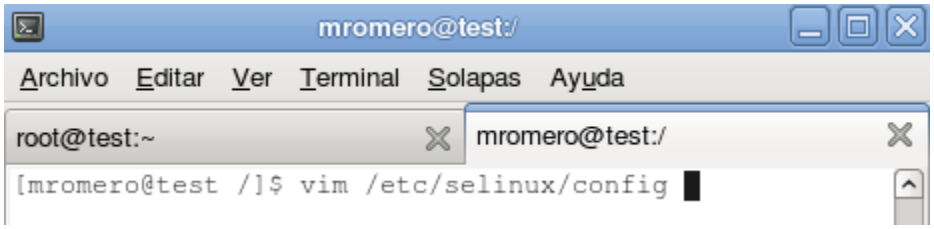
Iniciamos sesión y abrimos una terminal, ya que todo lo haremos mediante línea de comandos.



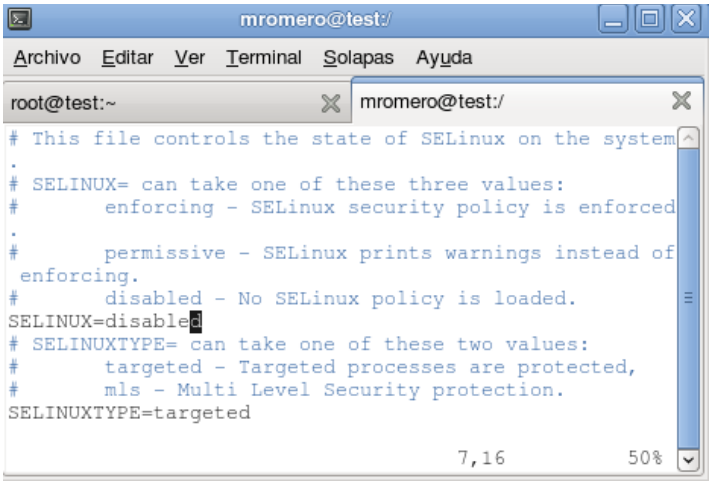
Desde el Terminal, lo primero que haremos será configurar la tarjeta de red para ello deberemos remover el NetworkManager esto lo haremos con el súper usuario (root) y con el comando yum remove tal como muestra la figura.



Editamos la configuración del selinux con el comando vim.



Y lo desactivos tal como se muestra en la figura.

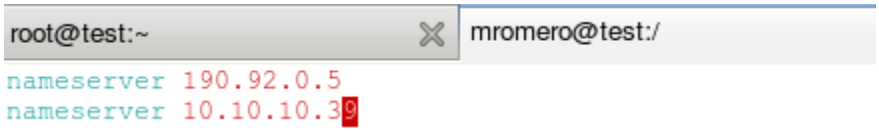


Ahora modificaremos el archivo de configuración para la interfaz eth0 con el comando vim.

El archivo de configuración deberá quedar similar al siguiente:

Editamos el archivo de configuración de los servidores de dominios con el comando vim.

El archivo de configuración deberá quedar igual al siguiente:



Agregar cuotas a las particiones var y home con el comando vim /etc/fstab como se muestra en la figura:

```
LABEL=/var      /var    ext3    defaults,usrquota,grpquota      1 2
LABEL=/home     /home   ext3    defaults,usrquota,grpquota      1 2
```

Debe remontar las particiones para que surtan efecto los cambios:

```
mount -o remount /var
mount -o remount /home
```

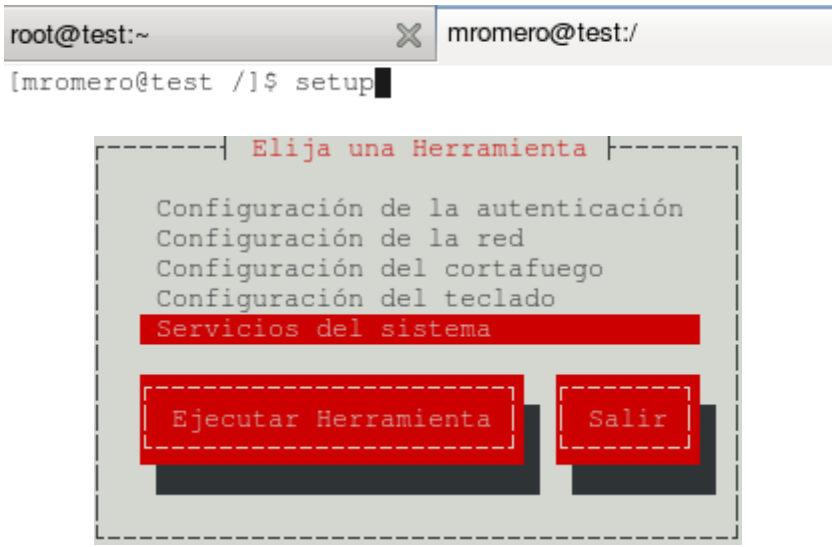
Se deben crear los ficheros aquota.user, aquota.group, quota.user y quota.group, los cuales se utilizarán en adelante para almacenar la información y estado de las cuotas en cada partición.

```
cd /var
touch aquota.user aquota.group quota.user quota.group
cd /home
touch aquota.user aquota.group quota.user quota.group
```

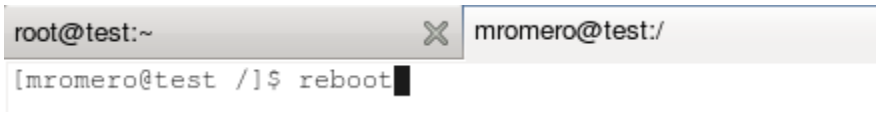
Para activar las cuotas de disco recién configuradas, solo bastará ejecutar los comandos:

quotaon /var
quotaon /home

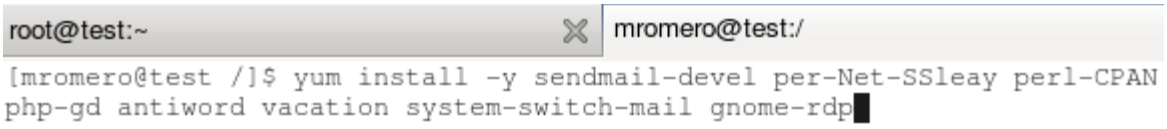
Agregar y quitar los servicios necesarios con el comando setup:



Después de haber hecho pruebas de conectividad reiniciamos el sistema con el comando reboot.

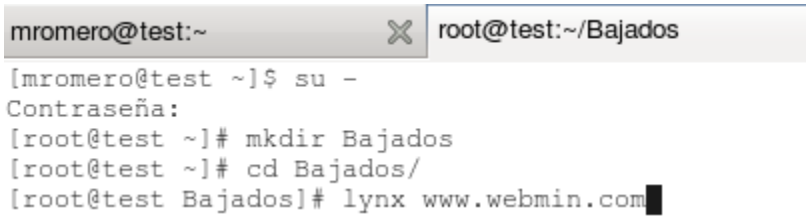


Instalar las dependencias con el comando yum:

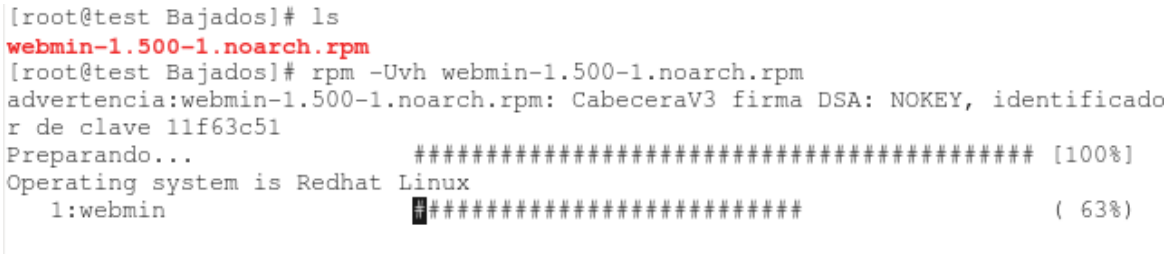


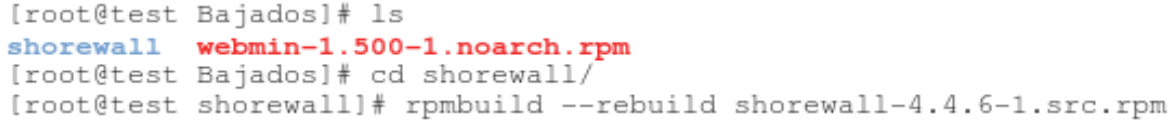
Cambiaremos al súper usuario (root) con el comando su, luego crearemos la carpeta de Bajados con mkdir hecho esto con el comando cd nos ubicamos dentro de la carpeta que acabamos de crear donde descargaremos los siguientes paquetes con el comando lynx:

- ✓ Webmin
- ✓ Shorewall



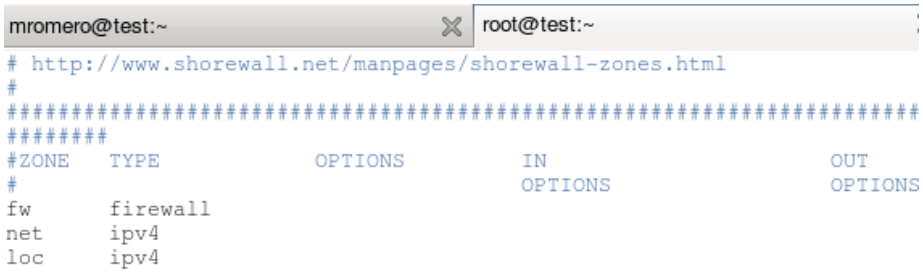
Luego con el comando rpm –Uvh instalamos los paquetes rpm que hemos bajado y con rpmbuid y rpm --rebuild reconstruimos los paquetes fuentes.



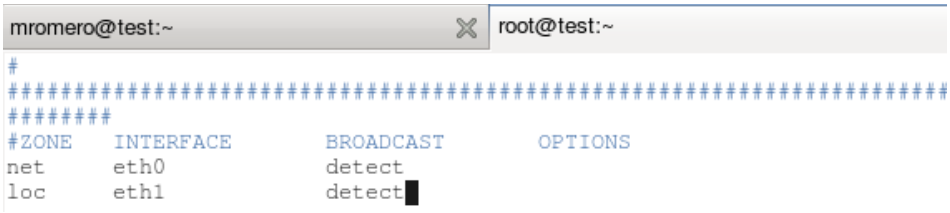


Una vez instalado el shorewall configuramos los ficheros básicos, con **vim etc/shorewall/shorewall.conf** activamos el shorewall :

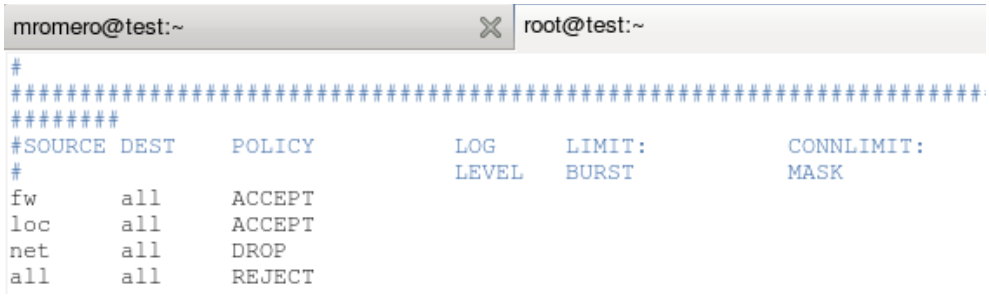
Con **vim /etc/shorewall/zones** agregamos las zonas:



Con **vim /etc/shorewall/interfaces** asignamos las zonas a las interfaces:

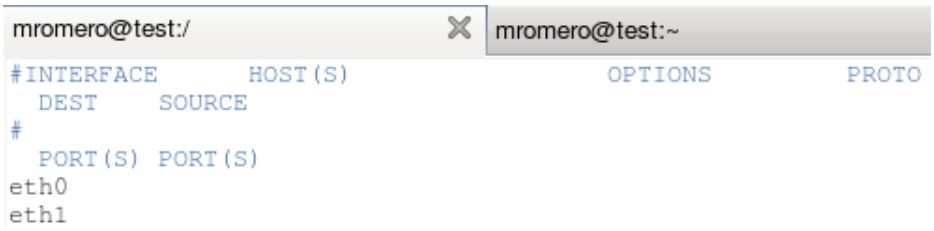


Luego definimos las políticas con **vim /etc/shorewall/policy**



Con **vim /etc/shorewall/rules** agregamos las reglas:

Con **vim /etc/shorewall/routestopped** configuramos que interfaces seguirán activas cuando se apague el shorewall.



Instalamos las dependencias con el comando yum install:
[mromero@test ~]# **yum install sendmail-devel perl-Net-SSLeay perl-CPAN php-gd php-pear system-switch-mail antiword vacation gnome-rdp php-xml php-dom php-mbstring* php-mcrypt* php-ftp**

Creamos una carpeta donde se descargaran los programas:
[mromero@test ~]# **mkdir /root/BAJADOS**
[mromero@test ~]# **cd /root/BAJADOS**
[mromero@test ~]# **mkdir MX**

Con el comando wget descargamos los programas que necesarios para el servidor de correos, instalamos y configuramos como se muestra:

Descompresor de Archivos Unrar:

[mromero@test ~]# **cd /root/BAJADOS/MX**
[mromero@test ~]# **wget http://dl.atrpms.net/all/unrar-3.8.4-1.src.rpm**
 # Con este comando creamos la paquetería y la reconstruimos:
[mromero@test ~]# **rpmbuild --rebuild unrar-3.8.4-1.src.rpm**
#Con rpm –Uvh instalamos el aplicativo del paquete que reconstruimos:
[mromero@test ~]# **rpm -Uhv /root/rpmbuild/RPMS/i586/unrar-3.8.4-1.fc11.i586.rpm**

Antivirus Clamav:
[mromero@test ~]# **cd /root/BAJADOS/MX**
[mromero@test ~]# **wget http://packages.sw.be/clamav/clamav-0.95.3-1.rf.src.rpm**
 # Con este comando creamos la paquetería y la reconstruimos:
[mromero@test ~]# **rpmbuild --rebuild clamav-0.95.3-1.rf.src.rpm**
[mromero@test ~]# **rpm -Uhv /root/rpmbuild/RPMS/i586/clam***
 # Para Actualizar la Base de Datos de virus se utiliza el comando:
[mromero@test ~]# **freshclam**

 # Instalamos los modulos perl:
[mromero@test ~]# **perl -MCPAN -e shell**
[mromero@test ~]# **vim /etc/clamd.conf**
SMTP Postfix
[mromero@test ~]# **cd /etc/**
[mromero@test ~]# **cp -r postfix postfix.Original**
[mromero@test ~]# **cd postfix**
[mromero@test ~]# **vim main.cf**
#Información de la versión del postfix y los dominios a administrar:
mail_version = 9999999
myorigin = sistelhn.net
mydestination = $myhostname, localhost.$mydomain, sistelhn.net
#Configuraciones para Bloquear SPAM:
smtpd_helo_required = yes
disable_vrfy_command = yes
strict_rfc821_envelopes = yes
#Para que rechacé direcciones, nombres, dominios desconocidos:
invalid_hostname_reject_code = 554
multi_recipient_bounce_reject_code = 554
non_fqdn_reject_code = 554
relay_domains_reject_code = 554
#Para que rechacé direcciones, clientes, nombres desconocidos:
unknown_address_reject_code = 554
unknown_client_reject_code = 554
unknown_hostname_reject_code = 554

```
        unknown_local_recipient_reject_code = 554
        unknown_relay_recipient_reject_code = 554
        unknown_sender_reject_code = 554
        unknown_virtual_alias_reject_code = 554
        unknown_virtual_mailbox_reject_code = 554
        unverified_recipient_reject_code = 554
        unverified_sender_reject_code = 554
#Opciones de autentificación:
        #smtpd_sasl_security_options = noanonymous
        smtpd_sasl_auth_enable = yes
        broken_sasl_auth_clients = yes
#Restricciones para correos:
        smtpd_recipient_restrictions =
                check_recipient_access hash:/etc/postfix/protected_destinations,
                        permit_sasl_authenticated,
                        permit_mynetworks,
                         reject_unauth_destination,
                        reject_invalid_hostname,
                        reject_unknown_recipient_domain,
                        reject_unknown_sender_domain,
                         reject_unauth_pipelining
        smtpd_restriction_classes = grupo2_only, grupo1_only

#Para que aplique las restricciones a los corres de los archivos grupo2 y grupo1:
        grupo2_only = check_sender_access hash:/etc/postfix/grupo2, reject
        grupo1_only = check_sender_access hash:/etc/postfix/grupo1, reject

#Numero de correos que estarán activos en cola:
        qmgr_message_active_limit = 1000
#El tiempo máximo que un correo estará en cola antes que sea entregado como imposible
enviar:
        maximal_queue_lifetime = 1d
        bounce_queue_lifetime = 1d
#Numero de entregas simultáneas:
        default_destination_concurrency_limit = 25
        smtpd_recipient_limit = 25
        message_size_limit = 409600000
        mailbox_size_limit = 409600000
        mynetworks = 127.0.0.1/32
# Límite de conexiones simultáneas podrá hacer el cliente a este servicio:
        smtpd_client_connection_count_limit  = 10
# Número máximo de intentos de conexión que podrá hacer el cliente a este servicio:
        smtpd_client_connection_rate_limit = 7
```

anvil_rate_time_unit = 1800s
 # Previene que se habrán múltiples cuentas:
local_destination_concurrency_limit = 2

#Mandar todo a Hold para que el Filtro MailScanner lo revise:
header_checks = regexp:/etc/postfix/header_checks

[mromero@test ~]# **vim header_checks**
/^Received:/ HOLD
#Creamos los archivos que tendrán las restricciones para las cuentas de correo:
[mromero@test ~]# **touch /etc/postfix/grupo2**
[mromero@test ~]# **touch /etc/postfix/grupo1**
[mromero@test ~]# **touch /etc/postfix/protected_destinations**
[mromero@test ~]# **cd /etc/postfix**
#Usamos el comando postmap para que aplique los cambios sin reiniciar el servicio:
[mromero@test ~]# **postmap protected_destinations**
[mromero@test ~]# **postmap grupo2**
[mromero@test ~]# **postmap grupo1**

Crear y generar Certificados:
[mromero@test ~]# **cd /etc/postfix**
[mromero@test ~]# **mkdir Certificados**
[mromero@test ~]# **cd Certificados/**
#Generamos los certificados usados por postfix, dovecot y apache.
[mromero@test ~]# **openssl req -new -nodes -newkey rsa:2048 -keyout sistelhn.net.key -out sistelhn.net.csr**
[mromero@test ~]# **openssl x509 -req -days 730 -in sistelhn.net.csr -signkey sistelhn.net.key -out sistelhn.net.crt**
[mromero@test ~]#
Configurar Apache:

[mromero@test ~]# **cd /etc/ httpd/conf/**
#Hacemos una copia del archivo de configuración del apache:
[mromero@test ~]# **cp -rp httpd httpd.Original**
[mromero@test ~]# **vim /etc/httpd/conf/httpd.conf**
NameVirtualHost 192.168.4.53:80
NameVirtualHost 192.168.4.53:443

#Configuración para la conexión al puerto 80 del webmail:
<VirtualHost 192.168.4.53:80>
DocumentRoot /var/www/html/roundcubemail
RewriteEngine On
RewriteRule ^/(.*)$ https://mail.sistelhn.net [R,NC]

```
        serverName test.sistelhn.net
        <Directory "/var/www/html/roundcubemail">
        allow from all
        Options +Indexes
        </Directory>
        </VirtualHost>

#Configuración para la conexión al puerto 443 del webmail:
        <VirtualHost 192.168.4.53:443>
        DocumentRoot /var/www/html/roundcubemail
        ServerName test.sistelhn.net
        SSLEngine on
        SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:
+SSLv2:+EXP
#Directorio donde se guardan los certificados:
        SSLCertificateFile /etc/postfix/Certificados/sistelhn.net.crt
        SSLCertificateKeyFile /etc/postfix/Certificados/sistelhn.net.key
        <Directory "/var/www/html/roundcubemail">
        allow from all
         Options +Indexes
         </Directory>
        </VirtualHost>

#Para que solo muestre el nombre del Servidor web instalado:
        ServerTokens ProductOnly
```

Configurar dovecot:

```
[mromero@test ~]#  cd /etc/
#Hacemos una copia del archivo de configuración del dovecot:
[mromero@test ~]#  cp -rp dovecot.conf dovecot.conf.Original
[mromero@test ~]#  vim dovecot.conf
#Habilitamos los protocolos y la opción para escuche en todas las interfaces:
        protocols = imap imaps pop3 pop3s
        listen = *, [::]
```

ssl = yes

#Opciones para el plugin de cuatos de disco del rouncubemail:

mail_plugins = quota imap_quota

quota = fs:INBOX:mount=/var

quota2 = fs:Others:mount=/home

#Agregamos la ruta de donde se encuentran los certificados:

ssl_cert_file = /etc/postfix/Certificados/sistelhn.net.crt

ssl_key_file = /etc/postfix/Certificados/sistelhn.net.key

[mromero@test ~]# **service dovecot restart**

Configurar MailScanner:

[mromero@test ~]# **cd /root/BAJADOS/MX**

#Descargamos el MailScanner con el comando wget:

[mromero@test ~]# **wget http://www.mailscanner.info/files/4/rpm/MailScanner-4.79.11-1.rpm.tar.gz**

#Descomprimimos el archivo que descargamos:

[mromero@test ~]# **tar xvfz MailScanner-4.79.11-1.rpm.tar.gz**

[mromero@test ~]# **cd MailScanner-4.79.11-1**

#Instalamos el MailScanner:

[mromero@test ~]# **./install.sh**

#Dejamos activo el MailScanner y desactivas el Sedmail ya que trabajaremos con postfix

[mromero@test ~]# **service sendmail stop**

[mromero@test ~]# **chkconfig sendmail off**

[mromero@test ~]# **chkconfig MailScanner on**

[mromero@test ~]# **vim /etc/MailScanner/MailScanner.conf**

%org-name% = Sistel

%org-long-name% = Sistemas Telemáticos

%web-site% = www.sistelhn.com

#Devuelve los mensajes en español:

%report-dir% = /etc/MailScanner/reports/es

#Usuario y grupo del SMTP:

Run As User = postfix

Run As Group = postfix

#Ubicación de la cola de correo entrante y saliente:

Incoming Queue Dir = /var/spool/postfix/hold

Outgoing Queue Dir = /var/spool/postfix/incoming

MTA = postfix

#Grupo que hará uso de la cuarentena con sus permisos para la interfaz web:

Quarantine Group = apache

Quarantine Permissions = 0660

#:

Use TNEF Contents = no

#Para que sea compatible con algunas versiones del Outlook:

```
        Deliver Unparsable TNEF = yes
        Virus Scanners = clamavmodule
#Formato que mostrara el nombre de los virus:
        Virus Names Which Are Spam = Sane*UNOFFICIAL HTML/*
        Allow Password-Protected Archives = yes
#Dirección de los archivos que contienen las reglas:
        Filename Rules = /etc/MailScanner/rules/GRUPOS.filename.rules
        Filetype Rules = /etc/MailScanner/rules/GRUPOS.filetype.rules
#Habilitar la cuarentena y guardar los mensajes o correo tal como lo recibimos:
        Quarantine Infections = yes
        Quarantine Whole Message = yes
        Quarantine Whole Messages As Queue Files = yes
#Incluir reportes del Spam Assassin:
        Always Include SpamAssassin Report = yes
        Hostname = the %org-name% ($HOSTNAME)
#No notificar a quienes nos mandaron un virus por correo:
        Notify Senders = no
#Personalización de los mensajes:
        Scanned Subject Text = Email Revisado!
        Virus Subject Text = Posible Virus!?
        Filename Subject Text = Nombre Archivo!?
        Content Subject Text = Contenido Peligroso!?
        Size Subject Text = Email Muy Grande, Revisar Archivos Adjuntos!?
        Disarmed Subject Text = Email Desarmado!
        Phishing Subject Text = Posible Fraude!?
        Spam Subject Text = Posible Spam!?
        High Scoring Spam Subject Text = Posible Spam!?
        Warning Is Attachment = no
        Send Notices = no
        Spam List = spamhaus-ZEN
        Is Definitely Not Spam = &SQLWhitelist
        Is Definitely Spam = &SQLBlacklist
#Puntaje para que un correo sea considerado como spam:
        Required SpamAssassin Score = 8
        High SpamAssassin Score = 12
        Check SpamAssassin If On Spam List = no
        Rebuild Bayes Every = 86400
#Almacena el mensaje en el directorio de cuarentena:
        Spam Actions = store
#Para eliminar el correo si tiene el puntaje máximo de spam:
        High Scoring Spam Actions = delete
#Directorio donde están los valores para el puntaje Spam Assassin:
        SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin
```

#Para que revise el contenido de los mensajes junto al valor requerido para que sea tomado como spam y la acción que tomara así como la ubicación de las listas:

MCP Checks = yes
MCP Required SpamAssassin Score = 2
MCP Actions = delete
High Scoring MCP Actions = delete
Is Definitely Not MCP = &SQLWhitelist
Definite MCP Is High Scoring = no
Always Include MCP Report = yes
Detailed MCP Report = yes

#Para obtener más información:

Always Looked Up Last = &MailWatchLogging

#Creamos la carpeta para el spamassassin:

[mromero@test ~]# **mkdir /var/spool/MailScanner/spamassassin**

#Le damos los permisos a las carpetas:

[mromero@test ~]# **chown postfix.postfix -R /var/spool/MailScanner/spamassassin**
[mromero@test ~]# **chown postfix.postfix -R /var/spool/MailScanner/incoming**
[mromero@test ~]# **chown postfix.postfix -R /var/spool/MailScanner/quarantine**

#Creamos el archivo donde se definen las reglas del grupo y lo editamos:

[mromero@test ~]# **touch /etc/MailScanner/rules/DEFINICION_GRUPOS.filename.rules**

#Usuarios Bloqueados
#Genoflexion:
From: jhazin@sistelhn.com and To: *@*
/etc/MailScanner/rules/grupox.filename.rules.conf
#
##
##
#Grupo 1: Acceso Abierto, Filtrado de tipo de Archivo casi nulo:
##
##

FromOrTo: mromero@sistelhn.net
/etc/MailScanner/rules/grupo1.filename.rules.conf

##
##########
##Grupo 2: Filtrado Estricto, Solo Archivos de Word, Adobe, Imagenes JPG:

```
#############################################################
##########

#FromOrTo:      xxxxxx@sistelhn.net
/etc/MailScanner/rules/grupo2.filename.rules.conf

#############################################################
##########
##Grupo 3: :
#############################################################
##########

FromOrTo: administrador@localhost.sistelhn.net
        /etc/MailScanner/rules/grupo3.filename.rules.conf
From:           127.0.0.1
        /etc/MailScanner/rules/grupo3.filename.rules.conf
FromOrTo:     localhost
        /etc/MailScanner/rules/grupo3.filename.rules.conf


################################################
#Grupo Por defecto para todos Filtrado Intermedio:
################################################

FromOrTo:     default                   /etc/MailScanner/filename.rules.conf

[mromero@test ~]#  touch
/etc/MailScanner/rules/DEFINICION_GRUPOS.filetype.rules
#Usuarios Bloqueados
#Genoflexion:
#  From: jhazin@sistelhn.net and To: *@*
/etc/MailScanner/rules/grupox.filetype.rules.conf
#
#############################################################
##
#Grupo 1: Acceso Abierto, Filtrado de tipo de Archivo casi nulo:
#############################################################
##

FromOrTo:     mromero@sistelhn.net
        /etc/MailScanner/rules/grupo1.filetype.rules.conf
```

```
#############################################################################
##Grupo 2: Filtrado Estricto, Solo Archivos de Word, Adobe, Imagenes JPG:
#############################################################################

#FromOrTo:   xxxxxx@sistelhn.net
        /etc/MailScanner/rules/grupo2.filetype.rules.conf

#############################################################################
##Grupo 3:
#############################################################################

FromOrTo:     administrador@localhost.sistelhn.net
        /etc/MailScanner/rules/grupo3.filetype.rules.conf
From:           127.0.0.1
        /etc/MailScanner/rules/grupo3.filetype.rules.conf
FromOrTo:     localhost
        /etc/MailScanner/rules/grupo3.filetype.rules.conf

################################################
#Grupo Por defecto para todos Filtrado Intermedio:
################################################

FromOrTo:     default                 /etc/MailScanner/filetype.rules.conf
```

#Creamos el archivo que contendrá la firma de la empresa:
[mromero@test ~]# **touch /etc/MailScanner/rules/Firma_Empresa-sig.text.rules**
[mromero@test ~]# **cd /etc/MailScanner**
#Copiamos los archivos para crear las reglas por archivo y tipo de los diferentes grupos:
[mromero@test ~]# **cp -rp filetype.rules.conf rules/grupo3.filetype.rules.conf**
[mromero@test ~]# **cp -rp filetype.rules.conf rules/grupo2.filetype.rules.conf**
[mromero@test ~]# **cp -rp filetype.rules.conf rules/grupo1.filetype.rules.conf**
[mromero@test ~]# **cp -rp filename.rules.conf rules/grupo1.filename.rules.conf**
[mromero@test ~]# **cp -rp filename.rules.conf rules/grupo2.filename.rules.conf**

[mromero@test ~]# **cp -rp filename.rules.conf rules/grupo3.filename.rules.conf**
#Añadimos los puntajes para spam:
[mromero@test ~]# **vim /etc/MailScanner/spam.assassin.prefs.conf**

```
score   TVD_SPACE_RATIO 1.50
score   RCVD_IN_XBL     2.80
score   RCVD_IN_BL_SPAMCOP_NET  1.50
score   BAYES_40        1.40
score   BAD_CREDIT      1.50
score   DEAR_SOMETHING  2.50
score   HTML_MESSAGE    0.80
score   BAYES_60        3.00
score   SUBJECT_NEEDS_ENCODING  0.60
score   FORGED_OUTLOOK_TAGS 0.40
score   RDNS_NONE       3.10
score   BAYES_99        4.20
score   BAYES_95        3.50
score   BAYES_50        2.70
score   URIBL_SBL       1.60
score   RDNS_DYNAMIC    3.20
score   RATWARE_MS_HASH 1.50
score   RATWARE_OUTLOOK_NONAME  0.50
score   SUBJ_ALL_CAPS   1.10
score   MIME_BASE64_TEXT        2.25
score   RCVD_NUMERIC_HELO       2.20
score   RCVD_IN_PB      1.90
score   RCVD_IN_SORBS_DUL       1.90
score   RCVD_IN_PBL     1.60
score   IMPOTENCE       2.50
score   HTML_SHORT_CENTER       1.20
score   MIME_HTML_ONLY  2.10
score   FUZZY_AMBIEN    2.10
score   TVD_RCVD_SINGLE 1.80
score   HTML_FONT_FACE_BAD      0.50
score   SUBJ_BUY        3.10
score   URI_NOVOWEL     1.50
score   URI_HEX 1.20
score   DATE_IN_FUTURE_03_06    1.00
score   INVALID_DATE    1.80
score   HTML_TAG_BALANCE_BODY   1.90
score   BAYES_80        3.50
score   STOX_REPLY_TYPE 1.25
score   BAYES_20        1.30
score   BAYES_05        1.00
```

score BAYES_00 0.00
[mromero@test ~]# **service spamassassin restart**

Mailwatch

#Con el comando wget descargamos el mailwatch:

[mromero@test ~]# **wget http://sourceforge.net/projects/mailwatch/files/mailwatch/1.0.5/mailwatch-1.0.5.tar.gz/download**

#Descomprimimos el archivo que descargamos:

[mromero@test ~]# **tar xvfz mailwatch-1.0.5.tar.gz**
[mromero@test ~]# **cd mailwatch-1.0.5**

#Movemos la carpeta mailscanner del mailwatch al directorio web:

[mromero@test ~]# **mv mailscanner /var/www/html/**
[mromero@test ~]# **cd /var/www/html/mailscanner/**
[mromero@test ~]# **cp -rp conf.php.example conf.php**

#Agregamos el usuario y contraseña para los siguientes archivos:

[mromero@test ~]# **vim conf.php**
define('DB_USER', 'usuario');
define('DB_PASS', 'contraseña');
[mromero@test ~]# **cd BAJADOS/mailwatch-1.0.5**
[mromero@test ~]# **vim MailWatch.pm**
my($db_user) = 'usuario';
my($db_pass) = 'contraseña';
[mromero@test ~]# **vim SQLSpamSettings.pm**
my($db_user) = 'usuario';
my($db_pass) = 'contraseña';
[mromero@test ~]# **vim SQLBlackWhiteList.pm**
my($db_user) = 'usuario';
my($db_pass) = 'contraseña';

#Creamos la base de datos mailscanner para mailwatch e insertamos un usuario con su respectiva contraseña para hacer uso del mailwatch vía web:

[mromero@test ~]# **mysql mailscanner -u mailcube –p**
mysql> INSERT INTO users VALUES ('mromero',md5('fernando1'),'Manuel Romero','A','','','','');
[mromero@test ~]# **cp -rp *.pm /usr/lib/MailScanner/MailScanner/CustomFunctions/**
[mromero@test ~]# **cd tools/**
[mromero@test ~]# **cp -rp db_clean.php /usr/local/bin/**
[mromero@test ~]# **service MailScanner restart && tail -f /var/log/maillog**

Configurar Roundcube:

[mromero@test ~]# **cd /root/BAJADOS/MX**
#Con el comando wget descargamos el roundcube:
[mromero@test ~]# **wget http://nightly.roundcube.net/trunk/roundcubemail-trunk-r3240-20100201.tgz**
#Descomprimimos el archivo que descargamos:
[mromero@test ~]# **tar xvfz roundcubemail-trunk-r3240-20100201.tgz**
#Movemos la carpeta del rouncube al directorio web:
[mromero@test ~]# **mv roundcubemail-trunk-r3240-20100201 /var/www/html/roundcubemail**
[mromero@test ~]# **cd /var/www/html/**
#Damos permiso a toda la carpeta para que el Servidor web pueda hacer uso de ella:
[mromero@test ~]# **chown apache.apache -R roundcubemail/**
#Creamos la base de datos para el rouncubemail:
[mromero@test ~]# # **mysql**
> CREATE DATABASE roundcubemail /*!40101 CHARACTER SET utf8 COLLATE utf8_general_ci */;
> GRANT ALL PRIVILEGES ON roundcubemail.* TO roundcube@localhost IDENTIFIED BY 'password';
> quit
#Ejecutamos el script:
[mromero@test ~]# **mysql roundcubemail < SQL/mysql.initial.sql**
[mromero@test ~]# **cd roundcubemail/config/**
[mromero@test ~]# **cp -rp db.inc.php.dist db.inc.php**
#Agregamos le usuario y contraseña de la base de datos que creamos para el roundcube:
[mromero@test ~]# **vim db.inc.php**
$rcmail_config['db_dsnw'] = 'mysql://usuario:clave@servidor/roundcubemail ';
[mromero@test ~]# **service httpd restart**
[mromero@test ~]# **cp -rp main.inc.php.dist main.inc.php**
#Editamos el archivo de configuración con las siguientes opciones:
[mromero@test ~]# **vim main.inc.php**
$rcmail_config['log_driver'] = 'file';
$rcmail_config['enable_caching'] = TRUE;
$rcmail_config['default_host'] = '127.0.0.1';
$rcmail_config['mail_domain'] = 'sistelhn.net';
$rcmail_config['smtp_server'] = '127.0.0.1';
$rcmail_config['language'] = es_ES;
$rcmail_config['create_default_folders'] = TRUE;
$rcmail_config['plugins'] = array('password','vacation');
$rcmail_config['logout_expunge'] = TRUE;

[mromero@test ~]# **service httpd restart**

#Plugin para cambiar contraseña del roundcubemail:
[mromero@test ~]# **cd /root/BAJADOS/MX**
[mromero@test ~]# **wget http://www.samera.net/rpm/poppassd-ceti-1.8.5-fc3.src.rpm**
[mromero@test ~]# **rpmbuild --rebuild poppassd-ceti-1.8.5-fc3.src.rpm**
#Forzamos la instalación del plugin poppassd:
[mromero@test ~]# **rpm -Uhv --nodeps /root/rpmbuild/RPMS/i586/poppassd-ceti-1.8.5-fc3.i586.rpm**
[mromero@test ~]# **cd /var/www/html/rouncubemail/plugins/password/**
[mromero@test ~]# **cp -rp config.inc.php.dist config.inc.php**
#Editamos el archivo de configuración con las siguientes opciones:
[mromero@test ~]# **vim config.ini.php**
```
$rcmail_config['password_driver'] = 'poppassd';
$rcmail_config['password_minimum_length'] = 8;
$rcmail_config['password_require_nonalpha'] = true;
```
[mromero@test ~]# cd /drivers

#Plugin para auto respuesta por vacaciones del rouncubemail:
[mromero@test ~]# **cd /BAJADOS/MX**
[mromero@test ~]# **wget http://downloads.sourceforge.net/project/rcubevacation/Version%201.6/vacation-1.6.5.zip?use_mirror=voxel**
[mromero@test ~]# **unzip vacation-1.6.5.zip**
#Damos permiso a toda la carpeta para que el Servidor web pueda hacer uso de ella:
[mromero@test ~]# **chown apache.apache -R vacation**
#Movemos la carpeta del vacation a la carpeto donde se encuentran los plugins del roundcube:
[mromero@test ~]# **mv vacation /var/www/html/roundcubemail/plugins/**
[mromero@test ~]# **cd /var/www/html/roundcubemail/plugins/vacation**
[mromero@test ~]# **cp -rp config.inc.php config.inc.php.Original**
[mromero@test ~]# **vim config.inc.php**
```
$rcmail_config['ftp']['server'] = '127.0.0.1';
```
[mromero@test ~]# **cd extra/vacation_binary/**
[mromero@test ~]# **make install**

[mromero@test ~]# **cp -rp squirrelmail_vacation_proxy /usr/bin/**
[mromero@test ~]# **chmod +x /usr/bin/squirrelmail_vacation_proxy**
[mromero@test ~]# **vim config.mk**
BINDIR = /usr/bin
WEBUSER = apache
[mromero@test ~]# **cd ../../**
[mromero@test ~]# **vim /etc/sudoers**
apache ALL = (ALL) NOPASSWD: /sbin/cbq,/sbin/tc,/sbin/ip
#Agregamos el plugin en el archivo de configuración del roundcube:
[mromero@test ~]# **vim /config/main.inc.pchp**
$rcmail_config['plugins'] = array('password','vacation');
[mromero@test ~]#

#Plugin para cambiar la apariencia del rouncubemail:
[mromero@test ~]# **cd /BAJADOS/MX**
[mromero@test ~]# **wget**
http://downloads.sourceforge.net/project/rcubevacation/Version%201.6/vacation-1.6.5.zip?use_mirror=voxel
[mromero@test ~]# **unzip air.zip**
[mromero@test ~]# **chown apache.apache -R air**
[mromero@test ~]# **mv air /var/www//html/roundcubemail/skins/**
#Agregamos el Skin para el rouncubemail en el archivo de configuración:
[mromero@test ~]# **vim /var/www/html/roundcubemail/config/main.inc.php**
$rcmail_config['skin'] = 'air';

Configuración de autentificación:

[mromero@test ~]# **vim /etc/pam.d/poppassd**

```
auth       required     pam_env.so
auth       sufficient   pam_unix.so nullok try_first_pass
auth       requisite    pam_succeed_if.so uid >= 500 quiet
auth       required     pam_deny.so

account    required     pam_unix.so
account    sufficient   pam_localuser.so
account    sufficient   pam_succeed_if.so uid < 500 quiet
account    required     pam_permit.so

#password    requisite  pam_cracklib.so try_first_pass retry=3
password    sufficient   pam_unix.so sha512 shadow nullok try_first_pass
password    required     pam_deny.so
```

Configuración de Servidor Ftp:

[mromero@test]# **vim /etc/vsftpd/vsftpd.conf**

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
xferlog_file=/var/log/vsftpd.log
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
```

[mromero@test]# **touch /etc/vsftpd/chroot_list**

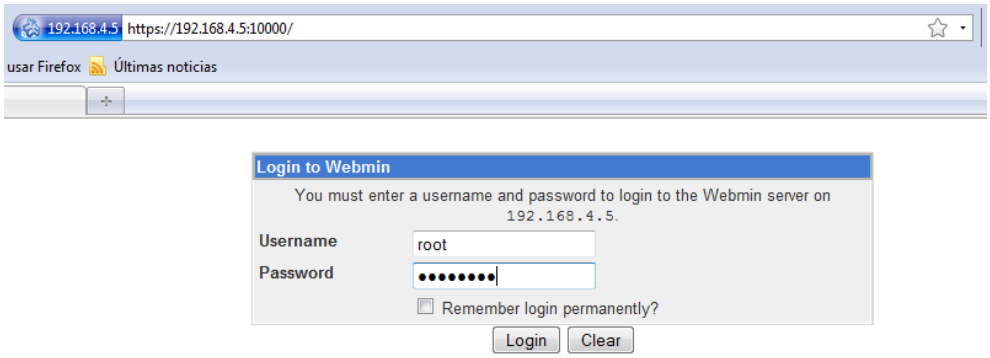
[mromero@test]# **service vsftpd restart**

Con el comando setup verificar que estén corriendo los siguientes servicios:

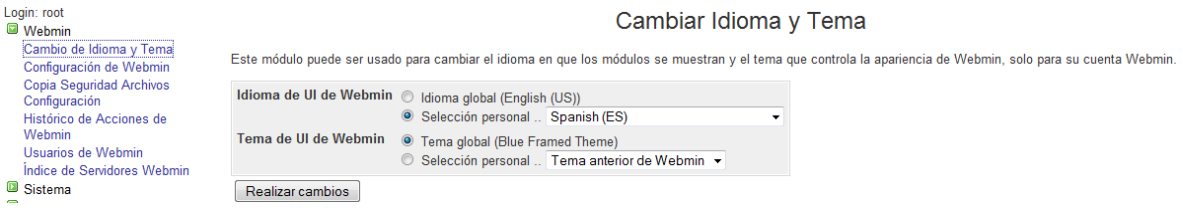
1. acpid
2. atd
3. clamd
4. cpuspeed
5. cron
6. dhcpd
7. dovecot
8. gpm
9. httpd
10. MailScanner
11. messagebus
12. mysqld
13. named
14. network
15. ntpd
16. ntpdate
17. poppassd
18. postfix
19. rsyslog
20. spamassassin
21. sshd
22. shorewall
23. vsftpd
24. webmin
25. xinetd

Personalización del Webmin

Para acceder a la interfaz de administración web colocamos en el url la dirección de nuestro servidor a través del puerto 10000 que usa el webmin https://192.168.4.5:10000/ donde introducimos el usuario y contraseña:



Lo primero que haremos será cambiar el idioma esto lo hacemos en webmin – Change Language and Theme y lo pasamos a español como se muestra en la imagen:

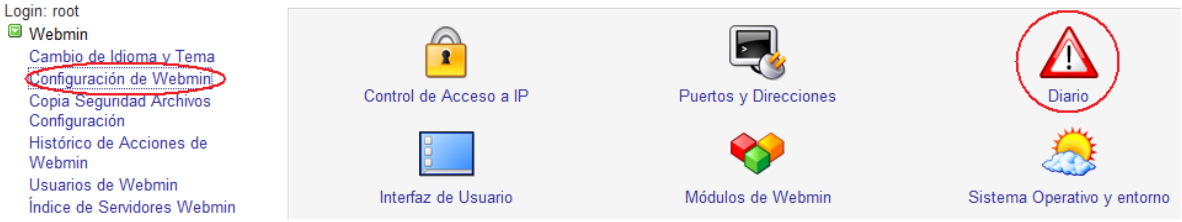


Luego nos vamos a configuración del webmin seleccionamos el icono de autentificación:

Hacemos los siguientes cambios:

1. opción Auto-logout after [ ] minutes of inactivity

Luego nos vamos a configuración del webmin seleccionamos el icono de diario:



Hacemos los siguientes cambios:

1. Utilizar formato combinado de histórico (incluyendo referenciador y agente de usuario) ( ) Si ( ) No
2. Periodically clear log files? ( ) Yes, every [600] hours ( ) No

3. Include Webmin logins and logouts in actions log? Si No
4. levar diario de los cambios hechos en archivos por cada acción Si No
5. Grabar todos los archivos modificados antes de las acciones, para permitir una vuelta atrás
   Si No
6. Also log to syslog? Si No

Luego nos vamos a Webmin – Usuarios de Webmin – Crear un nuevo grupo de Webmin:

Creamos el grupo Administrador y le damos acceso a los siguientes módulos:

1. Webmin:
    - Cambio de Idioma y Tema
    - Histórico de Acciones de Webmin
2. Sistema:
    - Arranque y Parada
    - Cambios de Contraseña
    - Cuotas de Disco
    - Usuarios y Grupos
3. Servidores:
    - Configuración de Postfix
    - Dansguardian Filtro de Contenidos Web
4. Red:
    - Configuración de Red
    - Cortafuegos Shorewall
5. Hardware:
    - Hora del Sistema
6. Otros:
    - Comandos Personalizados
    - Explorador de Archivos
    - Estado del Sistema y Servidor.

Luego creamos los usuarios y los añadimos al grupo de Administradores.