Escuela Superior Politécnica del Litoral

ADMINISTRACIÒN DE SERVICIOS DE RED BAJO LINUX | 1T 2019

MANUAL TÉCNICO



Contenido

[Overview 4](#_Toc17411857)

[Introducción 4](#_Toc17411858)

[Objetivo y alcances del sistema 4](#_Toc17411859)

[Normas, políticas y procedimientos 4](#_Toc17411860)

[Recursos de software 4](#_Toc17411861)

[OPENSWAN 4](#_Toc17411862)

[Nagios 4](#_Toc17411863)

[Paquete LAMP 5](#_Toc17411864)

[MYSQL 5](#_Toc17411865)

[Apache 5](#_Toc17411866)

[PHP 5](#_Toc17411867)

[GNS3 5](#_Toc17411868)

[Recursos de Simulación 6](#_Toc17411869)

[Caso de estudio 6](#_Toc17411870)

[Diagrama y Direccionamiento de la Red 6](#_Toc17411871)

[Servidor de archivos 7](#_Toc17411872)

[Configuración de Samba 7](#_Toc17411873)

[Instalación del servidor FTP 9](#_Toc17411874)

[Instalación de Nagios 11](#_Toc17411875)

[Instalación del Paquete LAMP 14](#_Toc17411876)

[Prerrequisitos 14](#_Toc17411877)

[Instalación de Apache Server 14](#_Toc17411878)

[Instalación de MySQL Server 14](#_Toc17411879)

[Instalación de PHP 15](#_Toc17411880)

[Permitir puerto en firewall 15](#_Toc17411881)

[Instalación de phpMyAdmin 15](#_Toc17411882)

[Configurar phpMyAdmin 16](#_Toc17411883)

[Firewall 18](#_Toc17411884)

[Instalacion de Squirrel Mail 18](#_Toc17411885)

[Deshabilitar Selinux 18](#_Toc17411886)

[Instalacion y Configuracion de Postfix 18](#_Toc17411887)

[Instalacion y Configuracion de dovecot 19](#_Toc17411888)

[Instalacion y configuracion de Squirrel Mail 20](#_Toc17411889)

[Crear un Usuario y accede a webmail 20](#_Toc17411890)

[Soporte 20](#_Toc17411891)

# Overview

## Introducción

OpenSwan es una implementación de Ipsec a nivel de código abierto la cual será utilizada para la comunicación de usuarios remotos en una empresa por medio de túneles VPN. Este proyecto involucra conceptos de bases de datos en MySql, iptables y manejo de servidores para la simulación de una red empresarial con sus respectivos servidores web y de correos además de visualizar información de los mismos a través de un aplicativo web para monitorear el rendimiento de los mismos llamado Nagios.

## Objetivo y alcances del sistema

* Realizar una conexión remota entre 2 usuarios por medio de OpenSwan
* Realizar la comunicación entre los dispositivos de capa 3 por medio del protocolo BGP.
* Configurar los entornos virtuales para que funciones como routers y servidores web y de correos.
* Realizar el modelo entidad-relación del sistema y poder observar adicionalmente el rendimiento de cada servidor.

## Normas, políticas y procedimientos

El ingreso a los respectivos servidores está controlado por una conexión ssh la cual mediante OpenSwan permitirá conectarse al ISP de la empresa y usando el protocolo BGP nos permitirá administrar cada uno de los servidores de manera remota.

Se espera que en todo momento la conexión sea estable por lo que se recomienda cerrar cualquier otro tipo de aplicación que realice conexiones de este tipo durante el aplicativo a excepción de un navegador en caso de querer monitorear a los servidores.

# **Recursos de software**

Dentro de esta sección se describen las librerías y frameworks de terceros usados durante la implementación del proyecto.

## OPENSWAN

Openswan es una implementación IPsec a nivel de kernel de código abierto en Red Hat Enterprise Linux. Emplea protocolos de establecimiento de llaves IKE (Internet Key Exchange) v1 y v2, implementadas como demonios de usuario.

## 

## Nagios

Nagios es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de estos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugin específicos para nuevos sistemas.

## Paquete LAMP

LAMP significa Linux, Apache, MySQL y PHP. Se utiliza para alojar sitios web escritos con lenguaje de programación PHP y usar MySQL como servidor de base de datos de fondo.

## MYSQL

MySQL es un sistema de gestión de bases de datos relacional desarrollado bajo licencia dual: Licencia pública general/Licencia comercial por Oracle Corporation y está considerada como la base de datos de código abierto más popular del mundo,1​2​ y una de las más populares en general junto a Oracle y Microsoft SQL Server, sobre todo para entornos de desarrollo web.

## Apache

Apache es la aplicación de servidor web más utilizada en sistemas operativos tipo Unix, pero se puede usar en casi todas las plataformas como Windows, OS X, OS / 2, etc.Es una aplicación de servidor web modular basada en procesos que crea un nuevo hilo con cada conexión simultánea. Es compatible con una serie de características; muchos de ellos se compilan como módulos separados y amplían su funcionalidad principal, y pueden proporcionar todo, desde soporte de lenguaje de programación del lado del servidor hasta el mecanismo de autenticación. El alojamiento virtual es una de esas características que permite que un único servidor web Apache sirva a varios sitios web diferentes

## PHP

PHP es un lenguaje de secuencias de comandos del lado del servidor de código abierto que originalmente significaba ‘Página de inicio personal ‘ahora significa ‘PHP: Preprocesador de hipertexto ‘, que es un acrónimo recursivo. Es un lenguaje de script multiplataforma que está muy influenciado por C, C ++ y Java.

## 

## GNS3

GNS3 es un software utilizado por cientos de miles de ingenieros de redes a nivel mundial para emular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, a aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube.

# **Recursos de Simulación**

Las pruebas de nuestro proyecto en su etapa de desarrollo fueron llevadas a cabo bajo el programa GNS3, el cual permite la simulación de sistemas de redes creando interfaces virtuales lo cual facilita al programador a testear configuraciones reales en un ambiente controlado.

Se utilizaron las máquinas virtuales con el SO Centos7 configuradas previamente como router para realizar las respectivas pruebas en GNS3 y los VPCS propio de GNS3 para la simulación de los usuarios remotos.

# Caso de estudio

## **Diagrama y Direccionamiento de la Red**

|  |
| --- |
|  |
| **Ilustración 1:** Diagrama de RED |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Puerta de enlace predeterminada |
| Internet | S0/1 | 10.0.1.1 | 255.0.0.0 | N/A |
| S0/2 | 10.0.2.1 | 255.0.0.0 | N/A |
| EdgeRouter1 | S2/0 | 10.0.1.2 | 255.0.0.0 | N/A |
| S1/0 | 172.16.0.1 | 255.240.0.0 | N/A |
| S1/1 | 172.16.1.1 | 255.240.0.0 | N/A |
| S1/2 | 172.16.2.1 | 255.240.0.0 | N/A |
| S1/3 | 172.16.3.1 | 255.240.0.0 | N/A |
| EdgeRouter2 | S2/0 | 10.0.2.2 | 255.0.0.0 | N/A |
| G0/0 | 192.168.4.1 | 255.255.255.0 | N/A |
| Quito | S1/0 | 172.16.0.2 | 255.240.0.0 | N/A |
| G0/0 | 192.168.0.1 | 255.255.255.0 | N/A |
| Guayaquil | S1/0 | 172.16.1.2 | 255.240.0.0 | N/A |
| G0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| Cuenca | S1/0 | 172.16.2.2 | 255.240.0.0 | N/A |
| G0/0 | 192.168.2.1 | 255.255.255.0 | N/A |
| Loja | S1/0 | 172.16.3.2 | 255.240.0.0 | N/A |
| G0/0 | 192.68.3.1 | 255.255.255.0 | N/A |
| Domain-srv | Eth1 | 192.168.0.100 | 255.255.255.0 | 192.168.0.1 |
| File-srv | Eth1 | 192.168.1.100 | 255.255.255.0 | 192.168.1.1 |
| Web-srv | Eth1 | 192.168.2.100 | 255.255.255.0 | 192.168.2.1 |
| Mail-srv | Eth1 | 192.168.3.100 | 255.255.255.0 | 192.168.3.1 |
| PC-1 | Eth1 | 192.168.4.101 | 255.255.255.0 | 192.168.4.1 |
| PC-2 | Eth1 | 192.168.4.102 | 255.255.255.0 | 192.168.4.1 |
| PC-3 | Eth1 | 192.168.4.103 | 255.255.255.0 | 192.168.4.1 |

**Tabla 1:** Tabla de Direccionamiento

# **Servidor de archivos**

## **Configuración de Samba**

1. **Procedemos a la instalación de Samba con el siguiente comando:**

|  |
| --- |
| yum install samba samba-client samba-common -y |

|  |
| --- |
| mv /etc/samba/smb.conf /etc/samba/smb.conf.bkp  vi /etc/samba/smb.conf |

1. **Editamos el archivo de configuración**

**y colocamos lo siguiente:**

|  |
| --- |
| [global]  workgroup = WORKGROUP  server string = Samba Server %v  netbios name = centos  security = user  map to guest = bad user  dns proxy = no  #===== Share Definitions=====  [Anonymous]  path = /samba/anonymous  browsable =yes  writable = yes  guest ok = yes  read only = no |

1. **Guardamos los cambios en el archivo de configuración y reiniciamos el servicio**

mkdir -p /samba/anonymous

systemctl enable smb.service

systemctl enable nmb.service

systemctl restart smb.service

systemctl restart nmb.service

1. **Realizamos los cambios respectivos en el firewall:**

|  |
| --- |
| firewall-cmd --permanent --zone=public --add-service=samba  firewall-cmd –reload |

1. **Cambiamos los permisos para compartir Samba**

|  |
| --- |
| chmod -R 0755 anonymous/  chown -R nobody:nobody anonymous/ |

1. **Permitimos las configuraciones de samba**

|  |
| --- |
| chcon -t samba\_share\_t anonymous/ |

1. **Creamos un usuario y contraseña para poder acceder a samba con las credenciales correspondientes.**

|  |
| --- |
| useradd rasho  groupadd smbgrp  usermod -a -G smbgrp rasho  smbpasswd -a rasho  [root@localhost]# smbpasswd -a rasho  New SMB password: YOUR SAMBA PASS  Retype new SMB password: REPEAT YOUR SAMBA PASS  Added user rasho. |

1. **Establecemos nuevos permisos**

|  |
| --- |
| mkdir /home/secure  chown -R rasho:smbgrp /home/secure/  chmod -R 0770 /home/secure/  chcon -t samba\_share\_t /home/secure/ |

1. **Editamos el archivo de configuración de nuevo y escribimos lo siguiente:**

|  |
| --- |
| [Secure]  path = /home/secure  valid users = @smbgrp  guest ok = no  writable = yes  browsable = yes |

1. **Finalmente reiniciamos los servicios**

|  |
| --- |
| systemctl restart smb.service  systemctl restart nmb.service |

## **Instalación del servidor FTP**

1. **Instalamos el paquete vsftpd.**

|  |
| --- |
| sudo yum install vsftpd |

1. **Habilitamos, empezamos y confirmamos si el servicio está activo**

|  |
| --- |
| sudo systemctl start vsftpd  sudo systemctl enable vsftpd  sudo systemctl status vsftpd |

1. **Abrimos el archivo de configuración en /etc/vsftpd/vsftpd.conf y escribimos lo siguiente:**

|  |
| --- |
| anonymous\_enable=NO  local\_enable=YES  write\_enable=YES  local\_umask=022  dirmessage\_enable=YES  xferlog\_enable=YES  connect\_from\_port\_20=YES  xferlog\_std\_format=YES  chroot\_local\_user=YES  listen=NO  listen\_ipv6=YES  pam\_service\_name=vsftpd |

|  |
| --- |
| userlist\_enable=YES  userlist\_file=/etc/vsftpd/user\_list  userlist\_deny=NO  tcp\_wrappers=YES  user\_sub\_token=$USER  local\_root=/home/$USER/ftp  pasv\_min\_port=30000  pasv\_max\_port=31000  rsa\_cert\_file=/etc/vsftpd/vsftpd.pem  rsa\_private\_key\_file=/etc/vsftpd/vsftpd.pem  ssl\_enable=YES |

1. **Habilitamos los puertos respectivos**

|  |
| --- |
| sudo firewall-cmd --permanent --add-port=20-21/tcp  sudo firewall-cmd --permanent --add-port=30000-31000/tcp  firewall-cmd –reload |

1. **Creamos las credenciales de un nuevo usuario y lo añadimos a la lista de usuarios de FTP.**

|  |
| --- |
| sudo adduser newftpuser  sudo passwd newftpuser  echo "newftpuser" | sudo tee -a /etc/vsftpd/user\_list |

1. **Creamos un directorio y establecemos los permisos correspondientes.**

|  |
| --- |
| sudo mkdir -p /home/newftpuser/ftp/upload  sudo chmod 550 /home/newftpuser/ftp  sudo chmod 750 /home/newftpuser/ftp/upload  sudo chown -R newftpuser: /home/newftpuser/ftp |

1. **Ejecutamos los siguientes comandos para crear el shell / bin / ftponly y hacerlo ejecutable:**

|  |
| --- |
| echo -e '#!/bin/sh\necho "This account is limited to FTP access only."' | sudo tee -a /bin/ftponly  sudo chmod a+x /bin/ftponly |

1. **Agregamos el nuevo shell a la lista de shells válidos en el archivo / etc / shells**

|  |
| --- |
| echo "/bin/ftponly" | sudo tee -a /etc/shells |

1. **Cambiamos el shell del usuario a / bin / ftponly**

sudo usermod newftpuser -s /bin/ftponly

# **Instalación de Nagios**

1. **Instalamos las librerias correspondientes:**

|  |
| --- |
| yum install httpd  yum install gcc  yum install glibc\*  yum install gd\* |

1. **Creamos un usuario y grupo para Nagios**

|  |
| --- |
| useradd nagios  passwd nagios  groupadd nagcmd  usermod -G nagcmd nagios  usermod -G nagcmd apache |

1. **Descargas:**

Creamos el siguiente directorio:

|  |
| --- |
| mkdir NagiosSetup  cd NagiosSetup |

Descargamos nagios

|  |
| --- |
| wget -X Get "http://sourceforge.net/projects/nagios/files/nagios-3.x/nagios-3.2.1/nagios-3.2.1.tar.gz/download" |

Descargamos los plugins de nagios:

|  |
| --- |
| wget -X Get "http://sourceforge.net/projects/nagiosplug/files/nagiosplug/1.4.15/nagios-plugins-1.4.15.tar.gz/download" |

1. **Instalamos Nagios**

|  |
| --- |
| tar -xzvf nagios-3.2.1.tar.gz  cd nagios-3.2.1  ./configure --with-command-group=nagcmd  make all  make install  make install-config  make install-commandmode  make install-init  chkconfig --add nagios |

1. **Instalamos los plugins**

|  |
| --- |
| tar xvf nagios-plugins-1.4.11.tar.gz  cd nagios-plugins-1.4.11  ./configure --with-nagios-user=nagios --with-nagios-group=nagios  make  make install |

1. **Verificamos la instalaciòn y posterior a esto inicializamos el servicio de nagios**

|  |
| --- |
| service nagios start  En el navegador escribimos: http://IP-ADDRESS/nagios |

1. **Descargamos, extraemos e instalamos los plugins de MySql:**

|  |
| --- |
| wget http://labs.consol.de/wp-content/uploads/2010/10/check\_mysql\_health-2.1.3.tar.gz  tar -zxvf check\_mysql\_health-2.1.3.tar.gz  cd check\_mysql\_health-2.1.3  ./configure --prefix=/usr/local/nagios --with-nagios-user=nagios --with-nagios-group=nagios --with-perl=/usr/bin/perl  make  make install |

1. **Creamos la base de datos de usuario:**

|  |
| --- |
| grant usage, replication client on \*.\* to 'nagios'@'localhost' identified by 'nagios'; |

1. **Configuramos Nagios para monitorear el servidor de MySql**

|  |
| --- |
| vi /usr/local/nagios/etc/nagios.cfg  añadimos la siguiente linea:  cfg\_file=/usr/local/nagios/etc/objects/mysqlmonitoring.cfg  Definimos el comando check\_mysql\_health como se muestra a continuacion:  vi /usr/local/nagios/etc/objects/commands.cfg  define command{  command\_name check\_mysql\_health  command\_line $USER1$/check\_mysql\_health -H $ARG4$ --username $ARG1$ --password $ARG2$ --port $ARG5$ --mode $ARG3$  } |

**Ingresamos los servicios a ser monitoreados en mysqlmonitoring.cfg:**

|  |
| --- |
| vi /usr/local/nagios/etc/objects/mysqlmonitoring.cfg  Añadimos:  define service{  use local-service  host\_name localhost  service\_description MySQL connection-time  check\_command check\_mysql\_health!nagios!nagios!connection-time!127.0.0.1!3306!  }  define service{  use local-service  host\_name localhost  service\_description MySQL slave-io-running  check\_command check\_mysql\_health!nagios!nagios!slave-io-running!127.0.0.1!3306!  }  define service{  use local-service  host\_name localhost  service\_description MySQL slave-sql-running  check\_command check\_mysql\_health!nagios!nagios!slave-sql-running!127.0.0.1!3306!  } |

**Finalmente reiniciamos el servicio de nagios**

service nagios restart

# **Instalación del Paquete LAMP**

## **Prerrequisitos**

Los dos repositorios rpm más populares REMI y EPEL tienen la mayoría de los paquetes actualizados. También están proporcionando los últimos paquetes para la configuración de LAMP. Habilite ambos repositorios en su sistema utilizando los siguientes comandos en su sistema CentOS 7.

rpm -Uvh http://dl.fedoraproject.org/pub/epel/7/x86\_64/Packages/e/epel-release-7-11.noarch.rpm

rpm -Uvh http://rpms.famillecollet.com/enterprise/remi-release-7.rpm

## **Instalación de Apache Server**

Apache o HTTP es el servidor web más popular utilizado en sistemas basados en Linux. Instalemos el servidor web Apache usando el siguiente comando habilitando los repositorios EPEL y REMI yum.

yum --enablerepo=epel,remi install httpd

Ahora inicie el servicio httpd y habilítelo para iniciar el arranque con comandos.

systemctl enable httpd.service

systemctl start httpd.service

## **Instalación de MySQL Server**

1. Primero, agregue el repositorio MySQL yum en su sistema usando el siguiente comando. También puede visitar repo.mysql.com para encontrar los rpms del repositorio para otros sistemas operativos. El siguiente comando funcionará con CentOS y RedHat 7.

rpm -Uvh <https://repo.mysql.com/mysql80-community-release-el7-1.noarch.rpm>

1. El repositorio predeterminado de MySQL 8 está habilitado para la instalación. Para cambiar, edite el archivo de configuración del repositorio (/etc/yum.repos.d/mysql-community.repo) y habilite / deshabilite los repositorios según los requisitos.
2. Luego instale el servidor MySQL y otros paquetes de dependencia.

yum install mysql-server

Después de la instalación, habilite el servicio MySQL e inícielo.

systemctl enable mysqld.service

systemctl start mysqld.service

1. El instalador generó una contraseña temporal para el usuario root de MySQL y la copió al archivo de registro. Puede encontrar esta contraseña con el siguiente comando.

grep "A temporary password" /var/log/mysqld.log | tail -n1

[Some text hidden] A temporary password is generated for root@localhost: Eif;=YpBy2h#

1. Aplique seguridad en el servidor MySQL recién instalado. Esto también le pedirá que cambie la contraseña temporal con una nueva contraseña.

mysql\_secure\_installation

Le saldrá las siguientes opciones:

Change the password for root? - y

Remove anonymous users? - y

Disallow root login remotely? - y

Remove test database and access to it? - y

Reload privilege tables now? - y

# **Instalación de PHP**

1. Ahora, instale paquetes PHP habilitando repositorios EPEL y REMI usando el siguiente comando.

yum --enablerepo=epel,remi-php73 install php

1. Luego instale los módulos PHP requeridos. Use el siguiente comando para enumerar los módulos disponibles e instalarlo.

yum --enablerepo=remi-php73 list php-\*

yum --enablerepo=remi-php73 install php-mysql php-xml php-xmlrpc php-soap php-gd

1. Después de instalar php y otros módulos php, reinicie el servicio Apache.

systemctl restart httpd.service

## **Permitir puerto en firewall**

Finalmente, abra los puertos de firewall para los servicios HTTP (80) y HTTPS (443) con el siguiente comando.

firewall-cmd --permanent --zone=public --add-service=http

firewall-cmd --permanent --zone=public --add-service=https

firewall-cmd --reload

## Instalación de phpMyAdmin

Instalar phpMyAdmin es muy simple. Puede instalar phpMyAdmin utilizando el comando yum.

LAMP Stack with PHP 7.3

yum install --enablerepo=remi-php73 phpmyadmin

### Configurar phpMyAdmin

De manera predeterminada, phpMyAdmin es accesible solo para localhost, lo que significa que no puede acceder a la interfaz web de phpMyAdmin desde máquinas externas. Tenemos que editar el archivo phpMyAdmin.conf ya que phpMyAdmin coloca los archivos de configuración en el directorio /etc./httpd/conf. d ya que tiene reglas y permisos para acceso remoto.

vi /etc/httpd/conf.d/phpMyAdmin.conf

La configuración predeterminada se verá a continuación:

Alias /phpMyAdmin /usr/share/phpMyAdmin

Alias /phpmyadmin /usr/share/phpMyAdmin

<Directory /usr/share/phpMyAdmin/>

AddDefaultCharset UTF-8

<IfModule mod\_authz\_core.c>

|  |
| --- |
| # Apache 2.4  <RequireAny>  Require ip 127.0.0.1  Require ip ::1  </RequireAny>  </IfModule>  <IfModule !mod\_authz\_core.c>  # Apache 2.2  Order Deny,Allow  Deny from All  Allow from 127.0.0.1  Allow from ::1  </IfModule>  </Directory>  <Directory /usr/share/phpMyAdmin/setup/>  <IfModule mod\_authz\_core.c>  # Apache 2.4  <RequireAny>  Require ip 127.0.0.1  Require ip ::1  </RequireAny>  </IfModule>  <IfModule !mod\_authz\_core.c>  # Apache 2.2  Order Deny,Allow  Deny from All  Allow from 127.0.0.1  Allow from ::1  </IfModule>  </Directory> |

Elimine o comente Requerir ip 127.0.0.1 y Requerir ip :: 1. Luego agregue Requerir todo otorgado al archivo de configuración. Finalmente obtendremos lo siguiente, en el archivo de configuración.

|  |
| --- |
| Alias /phpMyAdmin /usr/share/phpMyAdmin  Alias /phpmyadmin /usr/share/phpMyAdmin  <Directory /usr/share/phpMyAdmin/>  AddDefaultCharset UTF-8  <IfModule mod\_authz\_core.c>  # Apache 2.4  <RequireAny>  Require all granted  </RequireAny>  </IfModule>  <IfModule !mod\_authz\_core.c>  # Apache 2.2  Order Deny,Allow  Deny from All  Allow from 127.0.0.1  Allow from ::1  </IfModule>  </Directory>  <Directory /usr/share/phpMyAdmin/setup/>  <IfModule mod\_authz\_core.c>  # Apache 2.4  <RequireAny>  Require all granted  </RequireAny>  </IfModule>  <IfModule !mod\_authz\_core.c>  # Apache 2.2  Order Deny,Allow  Deny from All  Allow from 127.0.0.1  Allow from ::1  </IfModule>  </Directory> |

Reiniciar el servidor web

|  |
| --- |
| systemctl restart httpd |

### Firewall

Configure el firewall para permitir solicitudes web HTTP desde redes externas.

|  |
| --- |
| firewall-cmd --permanent --add-service=http  firewall-cmd --reload |

# Instalacion de Squirrel Mail

## Deshabilitar Selinux

Esta no es la mejor opción para deshabilitar el firewall por motivos de seguridad, pero lo estamos haciendo localmente. en su caso, permite que el tráfico supere las reglas de cmd del firewall.

|  |
| --- |
| # vi /etc/selinux/config  set SELINUX=disabled |

## Instalacion y Configuracion de Postfix

Debe instalar Epel Repository usando el siguiente comando

|  |
| --- |
| yum install epel-release -y |

Ahora, la instalación de Postfix

|  |
| --- |
| yum install postfix -y |

Ahora realice los siguientes cambios en el archivo postfix usando el siguiente comando al final.

|  |
| --- |
| vi /etc/postfix/main.cf |

Los cambios que debe de realizar son los siguientes:

|  |
| --- |
| ## Ingrese su hostname  myhostname = ejemplo.localhost.local  ## Ingrese su nombre de dominio  mydomain = ejemplo.localhost.local  inet\_interfaces = all  myorigin = $mydomain  ##Configure su direccion ip  mynetworks = 192.168.130.138/24, 127.0.0.0/8  ## Configure su directorio de mail  home\_mailbox = Maildir/  ## Ir a la linea 164, y agregar $domain al final  mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain |

Se debe de guardar los cambios antes de salir. Y como siguiente paso se debe de reiniciar postfix.

|  |
| --- |
| systemctl restart postfix  systemctl enable postfix |

## Instalacion y Configuracion de dovecot

|  |
| --- |
| yum install dovecot  systemctl start dovecot  systemctl enable dovecot |

Ahora modifique los archivos a continuación uno por uno. realice los siguientes cambios al final del archivo /etc/dovecot/dovecot.conf

|  |
| --- |
| vi /etc/dovecot/dovecot.conf  protocols = imap pop3 lmtp |

Realice los siguientes cambios al final del archivo /etc/dovecot/conf.d/10-mail.conf

|  |
| --- |
| vi /etc/dovecot/conf.d/10-mail.conf  mail\_location = maildir:~/Maildir |

Realice los siguientes cambios al final del archivo /etc/dovecot/conf.d/10-auth.conf

|  |
| --- |
| vi /etc/dovecot/conf.d/10-auth.conf  disable\_plaintext\_auth = yes  auth\_mechanisms = plain login |

Realice los siguientes cambios en el archivo /etc/dovecot/conf.d/10-master.conf

|  |
| --- |
| vi /etc/dovecot/conf.d/10-master.conf  unix\_listener auth-userdb {  #mode = 0600  user = postfix ## uncomment line 91 and enter postfix  group = postfix ## uncomment line 92 and enter postfix |

Reiniciar dovecot.

|  |
| --- |
| systemctl restart dovecot  systemctl enable dovecot |

## Instalacion y configuracion de Squirrel Mail

Primero, instalar squirrel mail.

|  |
| --- |
| yum install squirrelmail -y |

Ahora vaya a la carpeta squirrelmail y configúrelo de acuerdo con su servidor.

|  |
| --- |
| cd /usr/share/squirrelmail/config/  # ./conf.pl |

Ahora agregue las siguientes líneas al final del archivo httpd.conf.

|  |
| --- |
| vi /etc/httpd/conf/httpd.conf  Alias /webmail /usr/share/squirrelmail  <Directory /usr/share/squirrelmail>  Options Indexes FollowSymLinks  RewriteEngine On  AllowOverride All  DirectoryIndex index.php  Order allow,deny  Allow from all  </Directory> |

Reinicar el servicio de apache y dovecot.

|  |
| --- |
| systemctl restart httpd  restart dovecot |

## Crear un Usuario y accede a webmail

|  |
| --- |
| adduser ejemplo  passwd ejemplo |

# Soporte

Para más información o algún problema comunicarse con el equipo de soporte del software.

* [msegarra@espol.edu.ec](mailto:msegarra@espol.edu.ec)
* [anivmart@espol.edu.ec](mailto:anivmart@espol.edu.ec)
* groque@espol.ed.ec
* cesanava@espol.edu.ec