GUÍA DE ADMINISTRACIÓN DE SERVICIOS GNU/LINUX CENTOS7

El texto muestra herramientas que permiten llevar de mejor forma la administración de un sistema operativo basado en GNU/Linux, con especial énfasis en CentOS, para lo cual se han considerado siete capítulos que profundizan en temas relacionados con la gestión de cuentas de usuario, de tareas administrativas, de Servicios en GNU/LINUX Administración TCP/IP, en FTP, NSCA Implementación, así como la configuración de estos. La necesidad de contar con un control que permita llevar a cabo la monitorización en tiempo real de todos los equipos y dispositivos conectados a una red es de suma importancia dentro de las organizaciones, de ahí que se considere esta obra de pertinencia social en la contemporaneidad.

Alfonso Aníbal Guijarro Rodríguez: Máster en Docencia y Gerencia en Educación Superior. Máster Universitario en Modelado Computacional en Ingeniería. Ingeniero en Computación. Ha tutorado tesis de pregrado y posgrado. Posee varias publicaciones de artículos regionales y libros de alto impacto, en áreas de tecnología de la información. Es director de proyectos de investigación. Docente investigador de la Universidad de Guayaquil,.

Verónica Mendoza Morán: Máster Universitaria en Software y Sistemas. Máster en Educación Superior. Ingeniera en Sistemas Informáticos y Computación. Ha tutorado tesis de grado y realizado publicaciones de artículos científicos y libros. Gestora Pedagógica Curricular en las carreras de Software e Ingeniería en Sistemas Computacionales. Docente de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, Ecuador.

Ángel Humberto Veloz Rodríguez: Máster en Gestión y Diseño Web. Analista de Sistemas. Licenciado en Sistemas de Información. Ha tutorado varias tesis de grado y realizado publicaciones de artículos científicos y libros. Docente de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, Ecuador.

Angélica María Cruz Chóez: Máster en Sistemas Integrados de Gestión. Analista de Sistemas. Licenciada en Sistemas de Información. Ha tutorado tesis de grado y realizado publicaciones de artículos científicos y libros. Docente de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, Ecuador.

Tatiana Verónica Gutiérrez Quiñónez: Doctorando en Gestión y Planificación Pública y Privada. Máster en Sistemas Integrados de Gestión de Calidad, Seguridad y Medio Ambiente. Ingeniera Industrial. Ha tutorado tesis de grado y realizado publicaciones de artículos científicos y libros. Docente de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, Ecuador.

ISBN: 978-959-7225-77-5

EDACUN
EDITORIAL ACADÉMICA UNIVERSITARIA

GUÍA DE ADMINISTRACIÓN DE SERVICIOS GNU/LINUX CENTOS7

GUÍA DE ADMINISTRACIÓN DE SERVICIOS GNU/LINUX CENTOS7

Alfonso Aníbal Guijarro Rodríguez
Verónica Mendoza Morán
Ángel Humberto Veloz Rodríguez
Angélica María Cruz Chóez
Tatiana Verónica Gutiérrez Quiñónez

EDITORIAL ACADÉMICA UNIVERSITARIA

EDITORIAL ACADÉMICA UNIVERSITARIA

GUÍA DE ADMINISTRACIÓN DE SERVICIOS GNU/LINUX CENTOS7

Alfonso Aníbal Guijarro Rodríguez

Verónica Mendoza Morán

Ángel Humberto Veloz Rodríguez

Angélica María Cruz Chóez

Tatiana Verónica Gutiérrez Quiñónez

Diseño y Edición: MSc. Osmany Nieves Torres. As.
Corrección: MSc. Miriam Gladys Vega Marín. As.
Dirección General: Dr. C. Ernan Santiesteban Naranjo. P.T.

978-959-7225-77-5

Editorial Académica Universitaria (Edacun)
Universidad de Las Tunas
Ave. Carlos J. Finlay s/n
Código postal: 75100
Las Tunas, 2020

ÍNDICE

Nota al lector

El texto muestra herramientas que permiten llevar de mejor forma la administración de un sistema operativo basado en GNU/Linux, con especial énfasis en CentOS, para lo cual se han considerado siete capítulos, descritos a continuación:

Capítulo 1: Gestión de cuentas de usuario y tareas administrativas, aborda el uso de las cuentas de usuarios, desde aquellas que llevan privilegios especiales como el root, y las que se encuentran restringidas, por el sistema. Su creación, eliminación y la personalización de sus parámetros, además se tratan tareas administrativas como encender y apagar el sistema operativo, gestionar los grupos de usuarios, respaldo y restauración del sistema y la automatización de tareas programadas, además de servicios esenciales, como red, proxy, firewall, etc.

Capítulo 2: Configuración y Gestión de Servicios en GNU/LINUX Administración TCP/IP. Su enfoque principal es revisar el protocolo TCP/IP, su modelo en capas, la configuración que requiere Linux para la ejecución correcta de los servicios a nivel de redes Ethernet e inalámbricas, servicios de DNS, correo.

Capítulo 3: Gestión de Servicios FTP, NSCA Implementación. Se aborda el manejo del protocolo ftp. Enfoca el proceso técnico de cómo instalar, configurar y habilitar el servicio de ftp, y un apartado especial de Acceso por NCSA de proxy.

Capítulo 4: Administración de Restricciones - Restricción de Acceso a Sitios de Internet. Los proxy ayudan a la gestión de sitios web, lo que se debe permitir o no en una organización, denegar palabras, extensiones,

horario, música, entre otros, son muchas de las cosas que se muestran en esta unidad.

Capítulo 5: VLANs en GNU/Linux - Configurar VLANs en GNU/Linux. La información que se refiere es la utilización del sistema operativo linux como si fuera un switch de capa 2 que puede gestionar redes virtuales VLAN, lo cual es compatible con varias de las versiones basadas en red hat, centos, fedora.

Capítulo 6: Quagga en Centos 7 Configuración de Quagga en Centos 7: Ruteo estático, RIP y OSPF. La información que se presenta lleva a utilizar el sistema operativo linux como si fuera un router de capa 3 que puede gestionar protocolos como enrutamiento estático, dinámico con RIP y OSPF. Aunque soporta otros estos no fueron abordados, sin embargo, estas configuraciones son compatibles con varias de las versiones basadas en red hat, centos, fedora.

Capítulo 7: ZABBIX. Introducción ZABBIX. La necesidad de contar con un control que permita llevar a cabo la monitorización en tiempo real de todos los equipos y dispositivos conectados a una red es de suma importancia dentro de las organizaciones. Este capítulo se enfocado en presentar una herramienta que facilite la labor del administrador.

Capítulo 1

CAPÍTULO 1: GESTIÓN DE CUENTAS DE USUARIO Y TAREAS ADMINISTRATIVAS

Una cuenta de usuario regular posee restricciones que imposibilitan ejecuciones que puedan afectar la configuración de los servicios y la ubicación de los archivos de los archivos en el sistema operativo. Por lo contrario, la cuenta del usuario root dispone de privilegios y únicamente se emplea para llevar a cabo tareas de administración de este como lo indica Barrios (2016).

1.1 Creación de cuentas de usuario

Para establecer una nueva cuenta de usuario de manera sencilla se aplica el comando: *useradd con la opción -m*.

Esta opción (-m) sirve para crear el directorio de inicio dentro de /home y adicionalmente se coloca el nombre del usuario como complemento. De este modo se determina un grupo de igual nombre y se destina al usuario un UID (User Identification) con un número a partir del 1000 y usará /bin/bash como intérprete de mandatos.

1.1.1 Asignación o cambio de contraseñas

En este sentido, se coincide con la siguiente afirmación “Si la cuenta del usuario carece de contraseña, esta

automáticamente está deshabilitada. Para asignar una contraseña ejecute passwd con el nombre del usuario como argumento" (Barrios, 2016).

Los usuarios regulares están obligados a definir siempre una contraseña segura y que carezca de palabras del diccionario del sistema. Mientras que el usuario root solo puede asignar contraseñas débiles y presentar un aviso en caso de estas. Si existen errores de tecleado se puede pulsar la tecla de retroceso las ocasiones necesarias antes de continuar a oprimir la tecla ENTER. El sistema nunca mostrará los caracteres digitados en pantalla e informará siempre la falla en la confirmación de contraseña.

1.1.2 Eliminación de cuentas de usuario

- Ejecute userdel con un nombre de usuario como argumento para eliminar este.
- Ejecute userdel con la opción -r y el nombre del usuario como argumento para eliminar también el directorio de inicio, junto con su contenido, y el buzón de correo correspondiente.

1.1.3 Gestión de Grupos

Existen grupos de usuarios y de sistema, los cuales funcionan para organizar los mismos. Los grupos de usuarios están compuestos por usuarios regulares y emplean un número de GIP (Group Identification) encima del 1000 y los grupos de sistema son usados por programas y servicios con un número de GID por debajo del 1000. Estos grupos funcionan para organizar a los usuarios.

Para la creación de grupos de sistemas se realizan los siguientes pasos:

- Ejecute groupadd con la opción -r y un nombre como argumento para crear un grupo de sistema.
- Para la eliminación de grupos de sistemas se realizan los siguientes pasos:
- Simplemente ejecute groupdel con el nombre del grupo como argumento para eliminar este.
- Para la asignación de usuarios existentes a grupos existentes, se deben ejecutar los siguientes comandos:
- *Usermod -G* con el nombre del grupo y el nombre del usuario como argumentos para asignar usuarios a grupos.
- *Gpasswd -a* con el nombre del usuario seguido por el nombre del grupo como argumentos para asignar usuarios a grupos.
- *Gpasswd -M* y una lista de usuarios separada por comas para agregar varios usuarios simultáneamente.
- *Gpasswd -d* con el nombre del usuario seguido por el nombre del grupo como argumentos para eliminar al usuario del grupo.
- *Gpasswd -A* con el nombre del usuario seguido por el nombre del grupo como argumentos con el que se puede definir un usuario regular para que administre el grupo.
- *Gpasswd* con el nombre del grupo como argumento para eliminar la contraseña.

Se recomienda no utilizar contraseñas que tengan palabras existentes en algún diccionario de cualquier idioma o datos vinculados con el usuario o la empresa. De igual manera, memorizar las contraseñas y no escribirlas en medios físicos. Si no se puede lograr esto, usar contraseñas sencillas, pero cambiarlas constantemente. Además, no compartir estas con terceros y si es necesario almacenar las contraseñas en un archivo con un buen cifrado, es lo más seguro.

Una buena contraseña se compone de una combinación de números y letras mayúsculas y minúsculas y que contiene como mínimo 8 caracteres, al menos tres caracteres en mayúscula, al menos tres números y al menos tres caracteres especiales. También es posible utilizar pares de palabras con puntuación insertada y frases o secuencias de palabras o bien acrónimos de estas.

1.2 Configuración de valores por defecto para cuentas de usuario

Procedimientos:

Los comandos para la configuración de los valores por defectos para cuentas de usuarios son los mostrados a continuación: Archivo /etc/default/useradd

Como root edite el archivo /etc/default/useradd: vim /etc/default/useradd

Encontrará, invariablemente, el siguiente contenido:

 # useradd defaults file

GROUP=100

HOME=/home

INACTIVE=-1

EXPIRE=

SHELL=/bin/bash

SKEL=/etc/skel

CREATE_MAIL_SPOOL=yes

1.2.1 Variable HOME

El valor de esta variable puede ser cambiado según las prioridades del administrador. Conforme al Estándar de Jerarquía de Sistema de Archivos (Filessystem Hierarchy Estándar) el inicio del usuario se creará dentro de /home.

1.2.2 Variable SHELL

La variable SHELL establece el intérprete mandatos, para las cuentas creadas. El sistema determina /bin/bash (BASH/Bourne Again Shell) para interpretar mandatos, pero si el sistema es servidor se le asigna otro valor (Barrios, 2016).

Los posibles valores para la variable SHELL pueden ser:

- */sbin/nologin*, programa que de forma cortés rechaza el ingreso en el sistema (login).
- */bin/false*, programa que realiza salida inmediata e indica falla. Es decir, que impide el acceso al sistema y además devuelve falla.
- */dev/null*, el dispositivo nulo descarta todos los datos escritos sobre este y para cualquier proceso que lo utilice.
- */bin/bash*, intérprete de mandatos desarrollado por el proyecto GNU. Es el intérprete de mandatos predeterminado en GNU/Linux.
- /*bin/sh*, un enlace simbólico que apunta hacia /bin/bash y ofrece una versión simplificada de Bash muy similar a Bourne Shell (sh).

- */bin/tcsh*, una versión mejorada del intérprete de mandatos de C (csh).
- */bin/ash*, un clon de Bourne hell (sh) que utiliza menos memoria.
- */bin/zsh*, una versión mejorada de sh con funciones útiles encontradas en Bash y tcsh.

1.2.3 Directorio /etc/skel

Es empleado como plantilla para el directorio de inicio de los usuarios del sistema. Este habitualmente en sistemas establecidos sobre CentOS, engloba los siguientes archivos:

.bash_logout .bash_profile .bashrc

mkdir -m 0700 /etc/skel/mail/

touch /etc/skel/mail/Drafts

touch /etc/skel/mail/Junk

touch /etc/skel/mail/Sent

touch /etc/skel/mail/Trash

*chmod 600 /etc/skel/mail/**

1.3 Tareas administrativas del sistema

Al introducirnos en el mundo de Linux, se puede apreciar que es posible dividir las tareas administrativas en dos grupos: la administración del sistema y la administración de la red. Administrar estos sistemas demanda una serie de conocimientos y técnicas.

1.3.1 Arranque y apagado del sistema

Todos los sistemas de Unix cuentan con un sistema de arranque y apagado que se puede ajustar a preferencia del administrador del sistema. Así se podrán elegir los servicios

del arranque, en qué momento detenerlos y en qué momento el sistema se apaga.

En relación con ello, es válido retomar la siguiente idea:

> Todas las particiones primarias y extendidas comienzan con lo que se llama sector de arranque. El IPL por defecto, únicamente pasa el control al sector de arranque de la partición marcada con el flag (bandera) activo, también llamado flag de arranque. Como se puede suponer, sólo debería haber una partición con el flag de activo marcado. De esta manera se controla la partición de arranque. En el sector de arranque se encuentra otro programa que es el encargado de arrancar el sistema operativo. En el caso de Linux, estos programas son Lilo y Grub. (Junta de Andalucia, 2019, p. 2)

1.3.2 Gestión de Usuarios y Grupos

Administrar los usuarios es parte fundamental de esta tarea, saber a qué usuario darle acceso al sistema, los permisos para cada uno, la gestión de los grupos en general. Podemos identificar tres tipos de usuarios: los usuarios root, también conocidos como administrador; los usuarios especiales o llamados cuentas del sistema; usuarios normales, que son los usuarios que usan individualmente el sistema. En el archivo */etc/logins.defs* están definidas las variables para la creación de usuarios y de los campos shadows usadas por defecto. El *etc/shadow* es un archivo del sistema que almacena las contraseñas encriptadas, que solo pueden ser leídas por el usuario root.

1.3.3 Backup y restauración del sistema

Para cualquier sistema, es necesario crear copias de seguridad periódicamente. Jorba (2019) afirma que “se deben establecer periodos de copia que permitan salvaguardar nuestros datos de fallos del sistema (o factores externos) que puedan provocar pérdidas o corrupción de datos” (p.35).

Para sacar un backup se deben seguir los siguientes pasos:

1. Crear el directorio para los scripts y backups de un directorio: *mkdir /scripts /opt, mkdir /backup/*
2. Crear el script que genere un backup de tipo semanal, mediante el uso de manera automática de los scripts:

TIME=$(date +%y%m%d) # Este comando agregará fecha en nombre de archivo.

FILENAME=backup-$TIME.tar.gz # Aquí defino el formato y nombre de archivo.

SRCDIR=/data # Ubicación del directorio de backup.

DESDIR=/backup # Destino del archivo de copia de seguridad.

tar -cpzf $DESDIR/$FILENAME $SRCDIR #END

3. Programar la ejecución del script:

vim /etc/crontab # Ejecutar el script cada domingo a la media noche

0 0 * * 0 root /opt/script/backup.sh

1.3.4 Automatización de tareas rutinarias

En el uso habitual de la computadora se pueden automatizar ciertas tareas, ya sea por ser simples como por su temporalización. Las automatizaciones de las tareas se suelen hacer mediante scripts como Shell, perl. Para la automatización de las tareas se usan dos programas: Cron y At.

El Cron se trata de unos de los servicios básicos de los sistemas GNU/Linux. De hecho, el dominio cron siempre está

arrancado y en funcionamiento. La función básica de cron es la de ejecutar tareas programadas para un determinado momento, y por un usuario con los privilegios necesarios para poder programarlas.

En el At, a diferencia de Cron, las tareas que le son encomendadas (y su dominio, atd) solo se realizarán una vez. Es decir, la utilidad At se utiliza para programar una tarea que se llevará a cabo en un momento determinado, y no se volverá a ejecutar.

1.4 Tareas administrativas de red

1.4.1 Interfaz de red y conectividad

Se utiliza como el acceso a una red local, la conexión a una red mayor, o conexiones de ancho de banda con tecnología ADSL, RDSI o fibra óptica por cable.

NFS (*network fylesystem*)

Estos sistemas de archivos permiten compartir de forma transparente los ficheros por parte de todos o algunos de los usuarios, independientemente de nuestra situación en la red. En algunos casos, como Samba/CIFS, se nos ofrecen soportes para el acceso por parte de plataformas hardware/softwares diferentes (como por ejemplo Windows y Mac OS), e independientes de las configuraciones de clientes o servidores.

1.4.2 Impresión remota

Se trata de permitir el acceso a servidores de impresión remotos, impresión de forma transparente para el usuario, directo a impresoras remotas o a equipos que ofrecen servicios de impresión local.

1.5 Servicios esenciales

1.5.1 Mantener la hora del sistema

Es importante y esencial mantener la hora del sistema en Linux, ya que, a diferencia de otros sistemas operativos, el sistema de Linux depende mucho de la hora. Por ello es importante tener conocimientos acerca de cómo definir la zona horaria, cómo configurar el tiempo y cómo mantener la precisión del reloj. También es importante mantener actualizado el paquete de las zonas horarias.

Para verificar actualizaciones en ALDOS, CentOS o Red Hat™ Enterprise Linux usa el siguiente comando: *yum -y update tzdata,* y en openSUSE™ o SUSE™ Linux Enterprise: *yast -i timezone*.

1.5.2 Configurar la zona horaria

Por lo general la zona horaria es establecida desde el programa de instalación. Para volver a ajustarla se debe consultar el contenido del directorio /usr/share/zoneinfo y buscar una zona horaria apropiada para nuestra región.

El directorio *ls /usr/share/zoneinfo* contiene los archivos que corresponden a las zonas horarias de todo el mundo. Para evitar problemas, se respalda el archivo */etc/localtime* utilizado por el sistema: *cp /etc/localtime /etc/localtime.bak*

Se genera un enlace simbólico que apunta hacia el archivo de zona que corresponda a su localidad sobre-escribiendo al archivo: *ln -sf../usr/share/zoneinfo/Continente/region /etc/localtime*

1.5.3 Establecer hora y fecha exacta

Para ello se debe tener instalado el paquete *ntp: yum -y install ntp.* Luego se ejecuta el comando ntpdate utilizando como argumento el nombre o dirección IP de cualquier servidor NTP

ntpdate nombre_o_direccionIp. Esto debe devolver una salida similar a la siguiente: *28 Aug 12:28:51 ntpdate[29180]: adjust time server direccion_Ip offset -0.023721 sec.* Es necesario activar e iniciar el servicio correspondiente a NTP para que el sistema siempre este en la hora exacta.

Ejecute lo siguiente, si utiliza ALDOS 1.4, CentOS 6 o Red Hat™ Enterprise Linux 6 o versiones anteriores de estos: *chkconfig ntpd on && service ntpd start.*

Ejecute lo siguiente, si utiliza CentOS 7, Fedora™ o Red Hat™ Enterprise Linux 7 o versiones posteriores de estos: *systemctl enable ntpd && systemctl start ntpd.*

Ejecute lo siguiente, si utiliza openSUSE™ o SUSE™ Linux Enterprise: *insserv ntp on && rcntp start.*

Se activa e inicia el servicio ntpdate para forzar el ajuste de la hora junto con cada inicio del sistema. Editar el archivo */etc/sysconfig/ntpdate, vim /etc/sysconfig/ntpdate*

Se encuentra el siguiente contenido:

OPTIONS="-p 2" # Options for ntpdate

RETRIES=2 # Number of retries before giving up

SYNC_HWCLOCK=no # Set to 'yes' to sync hw clock after successful ntpdate

Añadir la opción -u a la variable OPTIONS:

OPTIONS="-p 2 -u" # Options for ntpdate

RETRIES=2 # Number of retries before giving up

SYNC_HWCLOCK=no # Set to 'yes' to sync hw clock after successful ntpdate

Ejecutar lo siguiente, si utiliza ALDOS, CentOS 6 o Red Hat™ Enterprise Linux 6 o versiones anteriores de estos: *chkconfig ntpdate on && service ntpdate start*

Ejecutar lo siguiente, para CentOS 7 o Red Hat™ Enterprise Linux 7 o versiones posteriores de estos: *systemctl enable ntpdate && systemctl start ntpdate*

Ejecutar lo siguiente, si utiliza openSUSE™ o SUSE™ Linux Enterprise: *insserv ntpdate on && rcntpdate start*

1.5.4 Login del Sistema

Es el servicio encargado de verificar a un usuario, si existe dentro del archivo de registro, para poder acceder al sistema. Para crear un usuario deben seguirse los siguientes pasos:

- Ingresar a la consola de Linux como root desde la consola.
- Crear la nueva cuenta de usuario, para ello, escribir el siguiente comando: # *useradd nombre_usuario*.
- Crear un password para ese usuario: # *passwd nombre_usuario*. El sistema pedirá ingresar la contraseña dos veces para confirmar. Una vez completado el proceso con éxito, la cuenta estará creada.

1.5.5 Servicios de impresión

Es muy diferente a otros sistemas operativos, ya que no utiliza un sistema de instalación de drivers o reconocimiento de la impresora. Para poder agregar una impresora en un sistema Linux podemos hacerlo por medio de CUPS (Sistema de Impresión Común en Unix, por sus siglas en inglés), que es un sistema de impresión modular para sistemas operativos de tipo Unix, el cual nos va a permitir usar la impresora como un

servidor para aceptar tareas de impresión de otras computadoras clientes.

Para agregar una impresora por medio de CUPS se debe tener la impresora conectada y configurada en la red donde va a ser usada. Ello requiere los siguientes pasos:

- Abrir el navegador y en la barra de búsqueda escribir lo siguiente: localhost:631
- Aparece una interfaz gráfica de CUPS que hace más fácil el proceso.
- Clic en la pestaña Administración.
- Ir a Add Printer para añadir la nueva impresora.
- Ingresar nuestro usuario y contraseña de administrador y pulsar intro.
- Seleccionar Discovered Network Printers para encontrar las impresoras en red o selecciona Internet Printing Protocol para agregarlas manualmente y damos a continuar.
- Si se selecciona Internet Printing Protocol ahora será el momento de introducir la dirección de la impresora en red en la caja de texto que aparece en pantalla. La URL será la IP de la impresora tipo “http://192.168.1.11” y pulsamos Connection y Continue.
- Escribir el nombre de la impresora, la descripción y localización en las cajas de texto correspondientes. Finalmente pulsamos “Add Printer” y “Continue”.
- Elegir el fabricante de la impresora en Makes y pulsamos Continue.

- Elegir el modelo de nuestra impresora para seleccionar los drivers de la lista y pulsar “Add Printer”.
- Finalmente, se agregará una impresora y en red, podrá ser usada.

1.6 Implementación del firewall

En la segunda práctica de esta guía se realizará la implementación para la seguridad de nuestro servidor CentOS 7, integrar el Firewall y el proxy en nuestra distribución Linux.

El tema más importante que se debe tener en mente es la forma de cómo proteger la integridad y disponibilidad de los archivos almacenados, de los servicios y roles del servidor y evitar el acceso no autorizado a los equipos.

Una de las soluciones más prácticas es implementar un sistema de firewall que brinde la posibilidad de llevar un control centralizado sobre el acceso y desarrollo del día a día. Se realizará la práctica prevista, la cual consiste en instalar y configurar un firewall, en este caso se utilizará Firewall CSF en CentOS 7 con el afán de obtener un nivel de seguridad mucho mayor al acostumbrado. Las siglas CSF proviene ConfigServer Security & Firewall.

1.6.1 Csf Firewall

Es una herramienta básica de seguridad, muy versátil y reconocida en el ámbito de los servidores web. Es un cortafuego a nivel de software, muy fácil de gestionar a diferencia de otras soluciones, que bloqueará el tráfico malicioso que se reciba en el servidor. Detecta todas las intrusiones y protege nuestro servidor Linux de números ataques de accesos indebidos e intentos de acceso por fuerza bruta.

CSF ofrece muchas ventajas sofisticadas con el afán de ofrecer una alta calidad de seguridad, dentro de estas se encuentran:

- Detectar accesos no autorizados a través de conexiones SSH.
- Intentos de inicio de sesión usando el comando su para adquirir potestad sobre el sistema.
- Analiza y comprueba fallos de autenticación.
- Integrado a la interfaz gráfica de WebAdmin y Cpanel.
- Puede autoconfigurar el puerto SSH si aún no es estándar durante su instalación.
- Bloquea el tráfico del direccionamiento IP no usado con frecuencia.
- Genera reportes sobre accesos sospechosos, uso excesivo de procesos por parte de los usuarios, entre otros.
- Alerta cuando un usuario envía demasiados scripts por hora, lo que evita spam en los scripts.
- Protege paquetes BOGON.
- Compatible con diversos dispositivos Ethernet.
- Realiza comprobaciones periódicas de seguridad al servidor con el fin de analizar vulnerabilidades.
- Permite direcciones IP de DNS dinámicos.
- Puede bloquear direcciones IP de forma permanente o temporal usando TTL.
- Soporta direcciones IPv6.

- Hace seguimiento a los cambios en las distintas cuentas del sistema.
- Detecta el uso excesivo de puertos.
- Puede detectar ataques con acceso distribuido.
- Puede bloquear códigos de acceso por país.
- Soporta Ipset para grandes listas de direcciones IP.

1.6.2 Configuración del FIREWALL

En esta práctica se procederá a montar la parte de seguridad a nuestro servidor web, para ello se ha elegido el FIREWALL CSF y el PROXY SQUID.

Como paso inicial se procede a descargar las dependencias, mediante el comando: *yum install wget vim perl-libwww-perl.noarch perl-Time-HiRes*

En nuestro caso ya se cuenta con dichas dependencias instaladas cuando se realizó la instalación en CentOS 7, por tal motivo, luego de ingresar el comando y ejecutarlo muestra un mensaje en el que indica que nada para hacer por lo que ya se encuentra instalado.

A continuación, es necesario ubicarse en la ruta *cd /usr/src/*

Luego ingresar el comando wget https://download.configserver.com/csf.tgz, mediante este se procederá a iniciar la descarga de la configuración que permitirá posteriormente configurar CSF (ver figura 1).

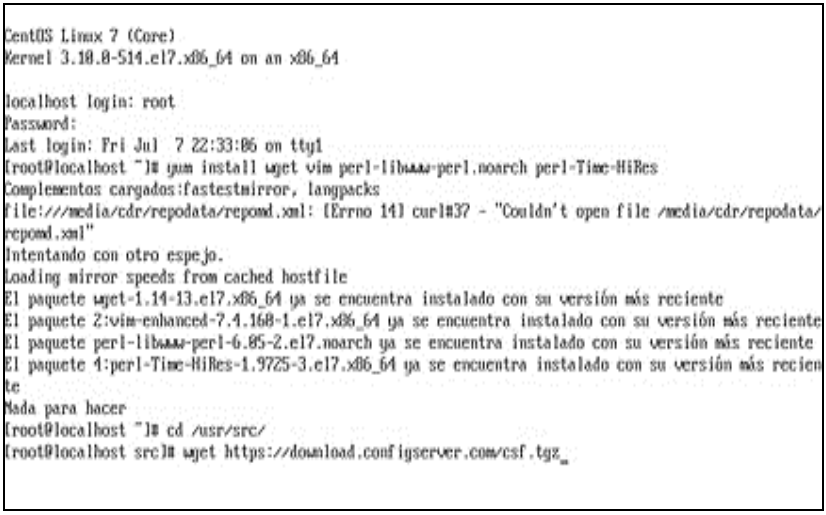


Figura 1. Inicio de descarga de la configuración de CSF.

Se procede a esperar que la descarga de la configuración culmine para extraer el contenido mediante el comando: *tar -xzf csf.tgz*

Luego se procede al directorio csf mediante el comando: *cd csf*

Para proceder a instalar lo que hemos extraído, se lo hará mediante el comando: *sh install.sh*

Ahora queda esperar que la instalación siga su curso y culmine el proceso de instalación (ver figura 2).

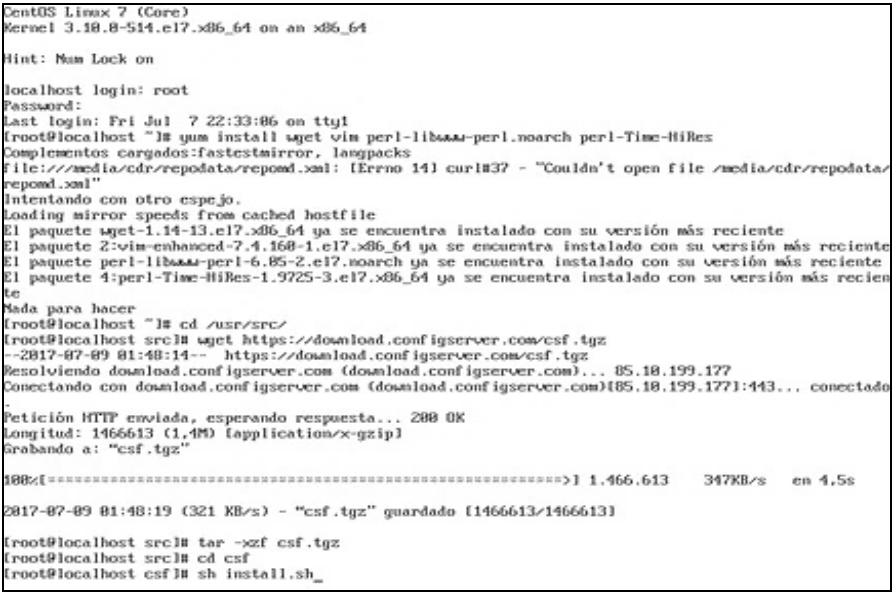


Figura 2. Inicio de instalación de CSF.

Luego que el proceso de instalación culmine, CSF debe funcionar en nuestro servidor. Para comprobarlo, se procedes a realizar un test mediante los siguientes comandos*: cd /usr/local/csf/bin/perl* y *csftest.pl* (ver figura 3).

```
«csf/bootstrap/fonts/glyphicons-halflings-regular.eot» -> «webmin/csf/images/bootstrap/fonts/glyphic
ons-halflings-regular.eot»
«csf/bootstrap/fonts/glyphicons-halflings-regular.woff2» -> «webmin/csf/images/bootstrap/fonts/glyph
icons-halflings-regular.woff2»
«csf/bootstrap/fonts/glyphicons-halflings-regular.svg» -> «webmin/csf/images/bootstrap/fonts/glyphic
ons-halflings-regular.svg»
«csf/bootstrap/fonts/glyphicons-halflings-regular.ttf» -> «webmin/csf/images/bootstrap/fonts/glyphic
ons-halflings-regular.ttf»
«csf/bootstrap/fonts/glyphicons-halflings-regular.woff» -> «webmin/csf/images/bootstrap/fonts/glyphi
cons-halflings-regular.woff»
«csf/configserver.css» -> «webmin/csf/images/configserver.css»
«csf/csf-loader.gif» -> «webmin/csf/images/csf-loader.gif»
«csf/csf_small.png» -> «webmin/csf/images/csf_small.png»
«csf/csf.svg» -> «webmin/csf/images/csf.svg»
«csf/jquery.min.js» -> «webmin/csf/images/jquery.min.js»
«csf/LICENSE.txt» -> «webmin/csf/images/LICENSE.txt»
«csf/loader.gif» -> «webmin/csf/images/loader.gif»
«/etc/csf/csfwebmin.tgz» -> «/usr/local/csf/csfwebmin.tgz»

Installation Completed

[root@localhost csf]# cd /usr/local/csf/bin
[root@localhost bin]# perl csftest.pl
Testing ip_tables/iptable_filter...OK
Testing ipt_LOG...OK
Testing ipt_multiport/xt_multiport...OK
Testing ipt_REJECT...OK
Testing ipt_state/xt_state...OK
Testing ipt_limit/xt_limit...OK
Testing ipt_recent...OK
Testing xt_connlimit...OK
Testing ipt_owner/xt_owner...OK
Testing iptable_nat/ipt_REDIRECT...OK
Testing iptable_nat/ipt_DNAT...OK

RESULT: csf should function on this server
[root@localhost bin]# _
```

Figura 3. Instalación completa y test para comprobar el funcionamiento.

Después de haber realizado el test de funcionalidad a CSF, se realizará la configuración dentro del sistema en CentOS 7. Lo primero es detener el servicio de firewall por defecto, luego deshabilitar el arranque automático del firewall y acceder a la ruta requerida y así poder editar el fichero. Para ello se utilizarán los siguientes comandos: *systemctl stop firewalld, systemctl disable firewalld*, *cd /etc/csf y nano csf.conf* (ver figura 4).

```
[root@localhost bin]# systemctl stop firewalld
[root@localhost bin]# systemctl disable firewalld
[root@localhost bin]# cd /etc/csf
[root@localhost csf]# nano csf.conf
```

Figura 4. Detención y desactivación del firewall por defecto.

Se abrirá el fichero seleccionado, una vez dentro nos ubicamos en la línea TESTING=”1” en este punto, cambiar el valor por el de 0. Guardar el cambio realizado mediante las teclas Ctrl+O (ver figura 5).

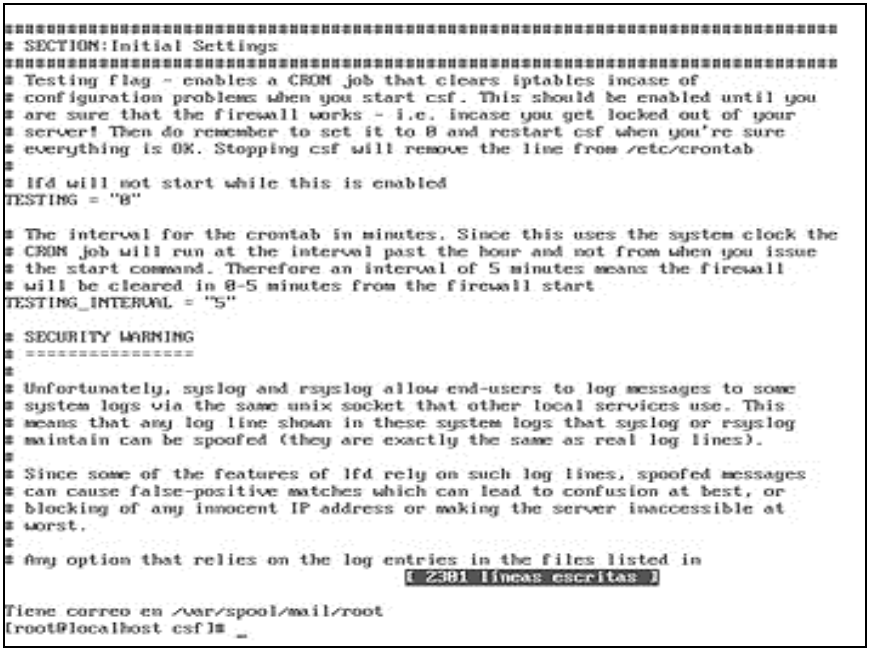


Figura 5. Edición del fichero csf.conf.

Por defecto, CSF habilita el tráfico entrante y saliente por el puerto SSH. Ahora iniciar los servicios de CSF y LDF mediante la ejecución de comandos como: *systemctl start csf y systemctl start lfd.*

1.7 Squid Proxy

Un proxy de conexión a Internet es un servidor que hace de intermediario entre los PCs de la red y el router de conexión a Internet, de forma que cuando un usuario quiere acceder a

esta, su PC realiza la petición al servidor proxy y este es quien realmente accede.

Squid es un servidor intermediario de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy una muy popular solución ampliamente utilizada entre los sistemas operativos como GNU/Linux y derivados de Unix. Puede funcionar como Servidor Intermediario y caché de contenido de Red para los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario. Entre sus ventajas están:

- Ahorro de tráfico.
- Mejoras en la productividad de la organización.
- Velocidad de tiempo de respuesta.
- Políticas de acceso y filtrado de contenido.
- Asegura la red local al no permitir acceso a contenido inseguro.
- Modificación de contenido.

1.8 Configuración de proxy squid

1.8.1 Instalación de SQUID

Acceder a la terminal de CentOS, desde aquí se realizarán las configuraciones que se describen en cada una de las secciones siguientes. Es necesario acceder al super usuario, que tiene todos los privilegios para realizar todas las configuraciones. Se ejecuta: su ➔ y después se ingresa la contraseña correspondiente. El $ cambia por # cuando se accede.

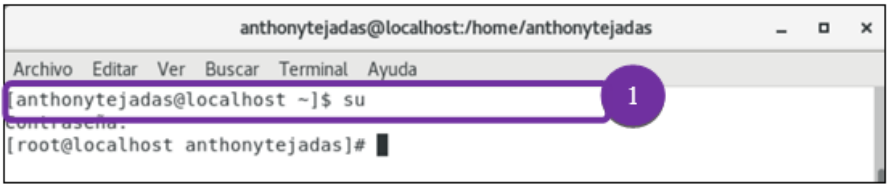


Figura 6. Instalación SQUID paso 1

Antes de instalar cualquier paquete, se recomienda actualizar el sistema y los paquetes con el siguiente comando: *yum -y update.*

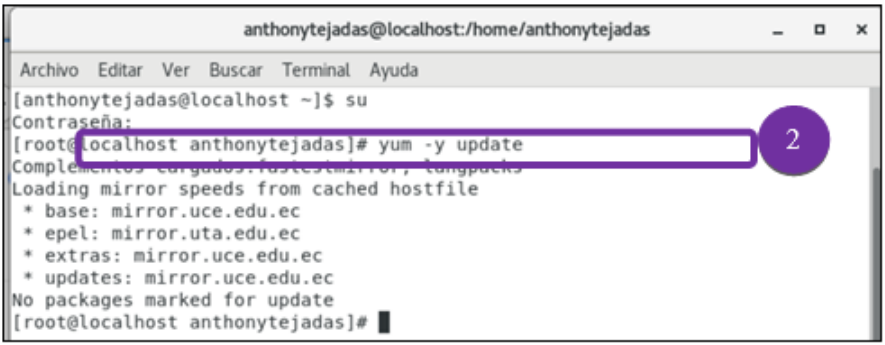


Figura 7. Instalación SQUID paso 2

Ahora deberá instalar el repositorio EPEL en su sistema, ya que Squid no está disponible en el repositorio predeterminado de yum. Ejecutar el siguiente comando para instalar el repositorio de EPEL en su servidor.

3.1. *yum -y install epel-release*

3.2. *yum -y update*

3.3. *yum clean all*

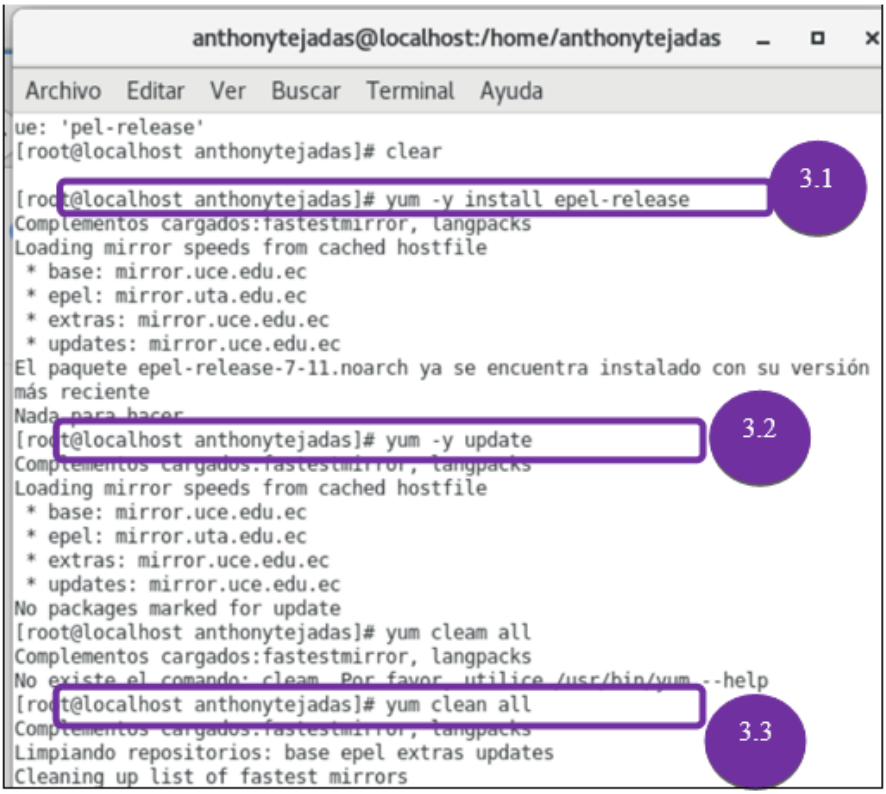


Figura 8. Instalación SQUID paso 3

Instalación de Squid a través de yum. Es necesario que el computador esté conectado a Internet, en caso contrario se deben descargar los paquetes de instalación. Para instalar el paquete de Squid Ejecutar: *yum -y install squid*

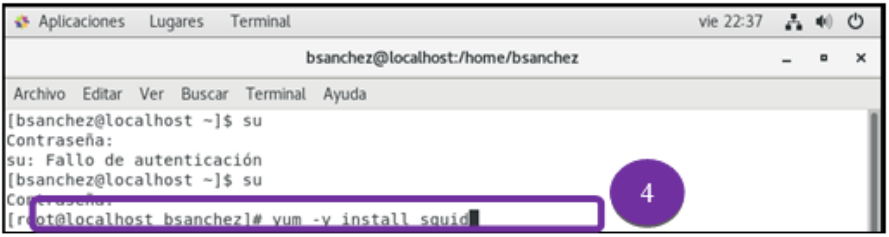


Figura 9. Instalación SQUID paso 4.1

Si la descarga se realiza correctamente, se mostrará un mensaje al finalizar "¡Listo!".

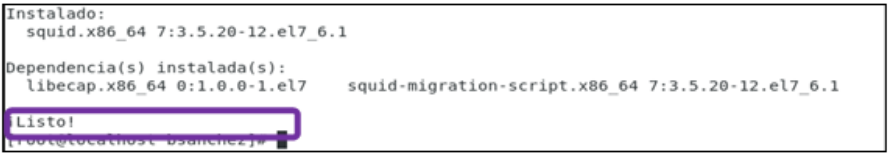


Figura 10. Instalación SQUID paso 4.2

Para comprobar qué versión de squid se instaló y corroborar la existencia de este se ejecuta la siguiente línea de comando: *rpm –q squid*

Figura 11. Instalación SQUID paso 5

Una vez que instale Squid, se puede iniciar el programa inmediatamente usando el siguiente comando: *systemctl start squid*; y para iniciar automáticamente Squid en el momento del arranque, se puede ejecutar el siguiente comando: *systemctl enable squid*

Para ver el estado del servicio Squid, se ejecuta el siguiente comando: *systemctl status squid*

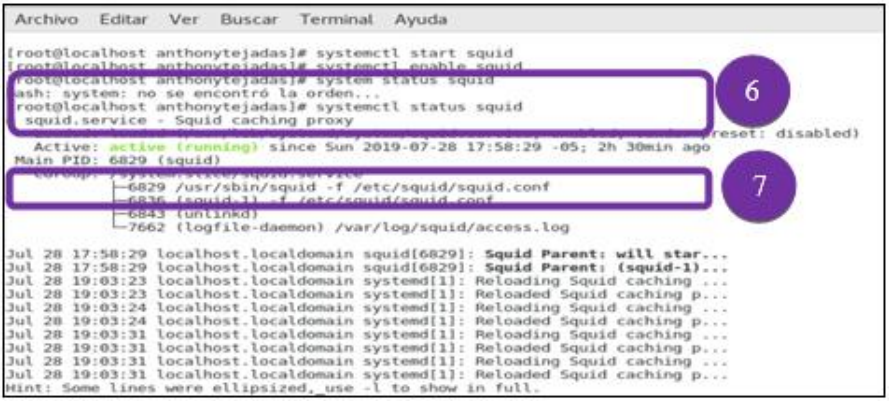


Figura 12. Instalación SQUID paso 7

Para ver la versión de Squid y las opciones de configuración, se ejecuta el siguiente comando: *squid -h*

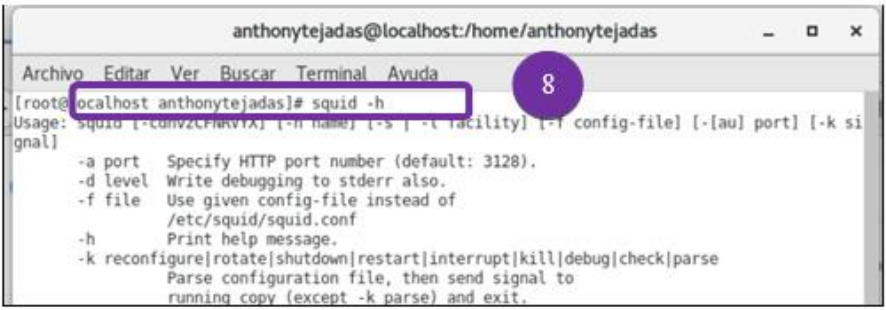


Figura 13. Instalación SQUID paso 8

Se pueden verificar los registros de errores de Squid usando el siguiente comando: *tail -f /var/log/squid/access.log*

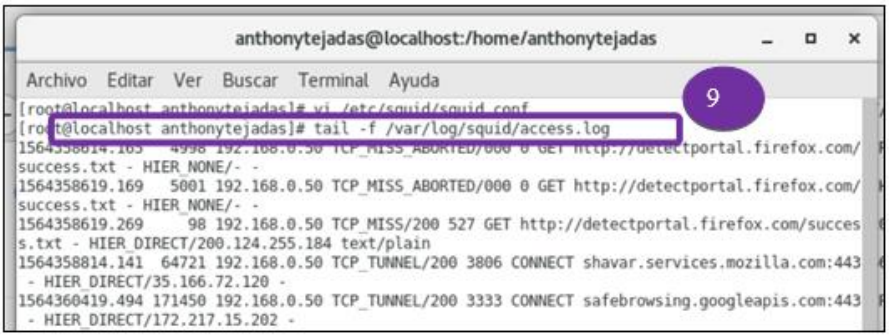


Figura 14. Instalación SQUID paso 9

Para configurar el squid se deberá ejecutar la siguiente línea de comando: *vi /etc/squid/squid.conf*. Localizar las líneas correspondientes a *cache_dir* y el *cache_men*

En caso de estar comentado el *cache_dir* con el numeral al inicio "#", borrar el numeral y definir 1024 en lugar de 100. Para la línea del *cache_men* en caso de no existir, agregar la línea *cache_men* 48 MB. Reiniciar el squid para hacer los cambios efectivos.

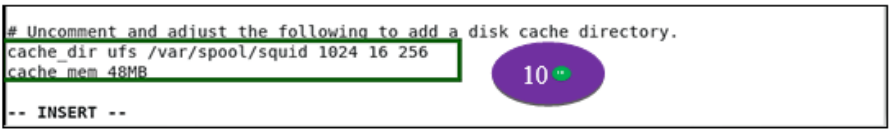


Figura 15. Instalación SQUID paso 10

Para ingresar desde el cliente al server por Telnet es necesario que el servicio de firewalle este desactivado, se hace mediante las líneas: *iptables –F, iptables –t nat –F*

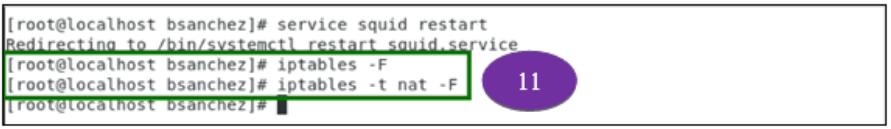


Figura 16. Instalación SQUID paso 11

1.8.2 Desde el cliente

Configurar el navegador de internet, Internet Explorer, para que sea posible la conexión.

Abrir internet Explorer > hacer clic en el ícono de engranaje (1.1) > Opciones de Internet > Seleccionar la pestaña de Conexión (1.2).

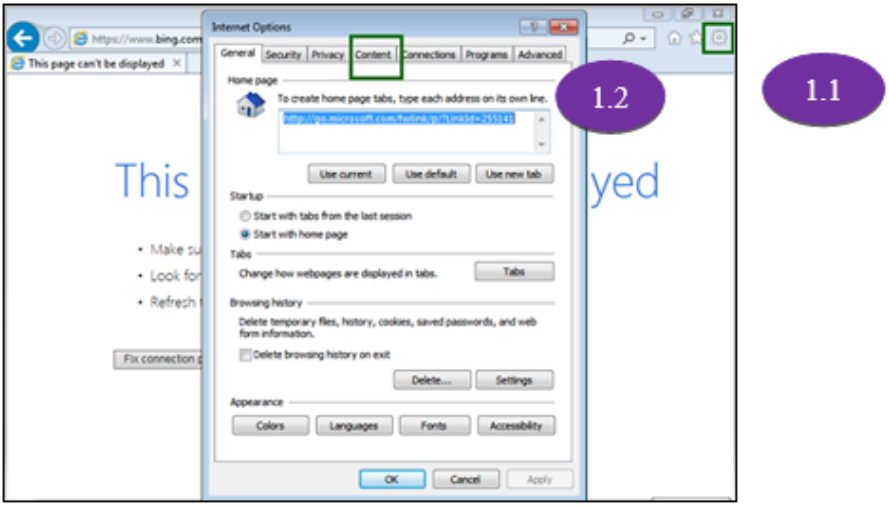


Figura 17. Configuración internet desde cliente paso1

Acceder a Configuraciones de LAN (2.1) y Activar “Usar Proxy Server” (2.2.), escribir la dirección IP del Servidor CentOS y el puerto del squid.

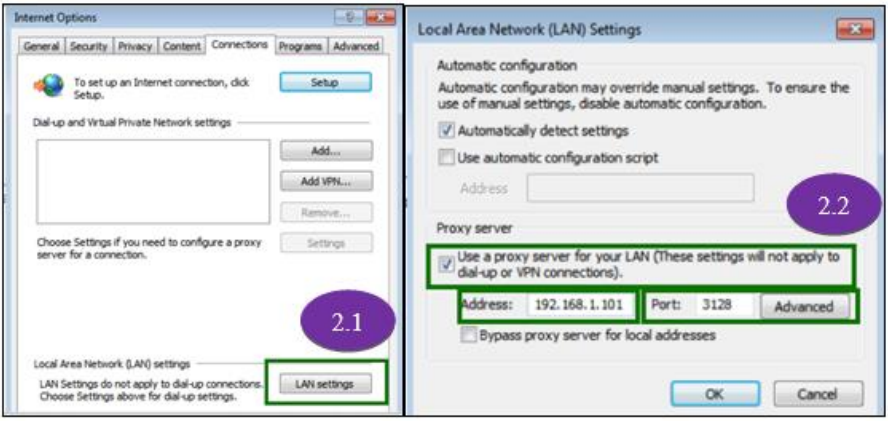


Figura 18. Configuración internet desde cliente paso2.1 y 2.2

Figura 19. Prueba de navegación de la máquina cliente.

Capítulo 2

CAPÍTULO 2: CONFIGURACIÓN Y GESTIÓN DE SERVICIOS EN GNU/LINUX

2.1 Administración TCP/IP

TCP/IP es una agrupación de protocolos accesible para la comunicación entre computadoras, la cual corresponde a una red. La abreviatura TCP/IP representa al Protocolo de control de transmisión/Protocolo de Internet. Procede de la asignación de protocolos fundamentales incluidos en el conjunto TCP/IP, esto es, del protocolo TCP y del protocolo IP.

En ciertos aspectos, TCP/IP significa todas las reglas de comunicación para Internet y se asienta en la noción de dirección IP, es decir, en la idea de proponer una dirección IP a cada unidad de la red para poder enrutar paquetes de datos. Debido a que el vínculo de protocolos TCP/IP originalmente se creó con resultados militares, está diseñado para efectuar con una cierta cantidad de criterios, entre ellos, dividir mensajes en paquetes, usar un procedimiento de direcciones, enrutar datos por la red y detectar errores en las transmisiones de datos.

La idea del conjunto de protocolos TCP/IP no es notable para un simple usuario, de la misma manera que un asistente no necesita saber cómo funciona su red audiovisual o de televisión. En cambio, para las personas que desean gestionar

o brindar soporte técnico a una red TCP/IP, su conocimiento es fundamental.

2.1.1 La diferencia entre estándar e implementación

En general, TCP/IP relaciona los siguientes dos elementos:

Los elementos de estándar: el protocolo TCP/IP representa la manera en la que se realizan las comunicaciones en una red.

Los elementos de implementación: la designación TCP/IP generalmente se extiende a software basado en el protocolo TCP/IP. En realidad, TCP/IP es un modelo cuya aplicación de red utilizan los desarrolladores. Las aplicaciones son, por lo tanto, implementaciones del protocolo TCP/IP.

2.1.2 TCP/IP modelo de capas

Para poder emplear el modelo TCP/IP en cualquier equipo, independientemente del sistema operativo, el sistema de protocolos TCP/IP se ha fragmentado en diversos módulos. Cada uno de estos ejecuta una tarea específica y realizan sus trabajos uno a continuación del otro en una disposición específica, es decir que existe un sistema estratificado.

La palabra capa se utiliza para mostrar el hecho de que los datos que recorren por la red atraviesen distintos niveles de protocolos. Así, cada capa sentencia continuamente los datos (paquetes de información) que transitan por la red, les agrega un elemento de información (llamado encabezado) y los envía a la capa siguiente.

El modelo TCP/IP es muy conforme al modelo OSI (modelo de 7 capas) que fue desarrollado por la Organización Internacional para la Estandarización (ISO) para estandarizar las comunicaciones entre equipos.

2.1.3 El modelo TCP/IP

El modelo TCP/IP, influenciado por el modelo OSI, también utiliza el enfoque modular (utiliza módulos o capas), pero solo contiene cuatro: acceso a la red, Internet, transporte y aplicación.

Las ocupaciones de las diferentes capas son las siguientes:

- Capa de acceso a la red: define la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizado.
- Capa de Internet: es responsable de proveer el paquete de datos (datagrama).
- Capa de transporte: brinda los datos de enrutamiento, inmediato con los mecanismos que permiten conocer el estado de la transmisión.
- Capa de aplicación: incorpora aplicaciones de red estándar (Telnet, SMTP, FTP, etc.).

2.1.4 Encapsulación de datos

Durante una entrega, los datos cruzan cada una de las capas en el nivel del equipo remitente. En cada capa, se le agrega información al paquete de datos. Esto se llama encabezado, es decir, una recopilación de información que garantiza la transmisión. En el nivel del equipo receptor, cuando se atraviesa cada capa, el encabezado se lee y después se elimina. Entonces, cuando se recibe, el mensaje se encuentra en su estado original:

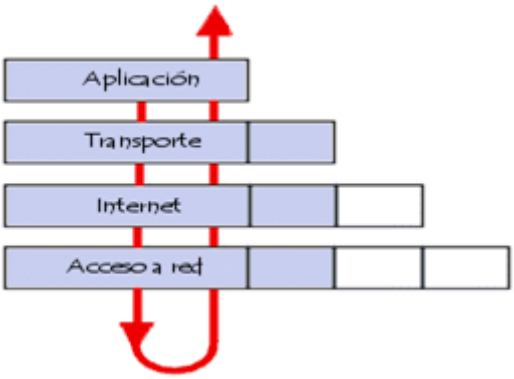


Figura 20 Niveles de encapsulado de paquetes

En cada nivel, el paquete de datos cambia su aspecto porque se le agrega un encabezado. Por lo tanto, las designaciones cambian según las capas: el paquete de datos se denomina mensaje en el nivel de la capa de aplicación. El mensaje después se encapsula en forma de segmento en la capa de transporte y toma el nombre de datagrama. Finalmente, se habla de trama en el nivel de capa de acceso a la red

2.1.5 Capa de acceso a la red

Es la primera capa de la pila TCP/IP. Ofrece la capacidad de acceder a cualquier red física, es decir, brinda los recursos que se deben implementar para transmitir datos a través de la red. Por lo tanto, contiene especificaciones relacionadas con la transmisión de datos por una red física, cuando es una red de área local (red en anillo, Ethernet, FDDI), conectada mediante línea telefónica u otro tipo de conexión a una red. Afortunadamente, todas estas especificaciones son invisibles al ojo del usuario, ya que en realidad es el sistema operativo el que realiza estas tareas, mientras los controladores de hardware permiten la conexión a la red (por ejemplo, el controlador de la tarjeta de red).

2.1.6 Capa de Internet

Es la capa "más importante" (si bien todas son importantes a su manera), ya que es la que define los datagramas y administra las nociones de direcciones IP. Permite el enrutamiento de datagramas (paquetes de datos) a equipos remotos junto con la administración de su división y ensamblaje cuando se reciben. Contiene 5 protocolos: IP, ARP, ICMP, IGMP y RARP. Los primeros tres protocolos son los más importantes para esta capa.

2.1.7 Capa de transporte

Los protocolos de las capas anteriores permiten enviar información de un equipo a otro. La capa de transporte permite que las aplicaciones que se ejecutan en equipos remotos puedan comunicarse. Esta contiene dos protocolos que permiten que dos aplicaciones puedan intercambiar datos independientemente del tipo de red (es decir, de las capas inferiores). Los dos protocolos son el TCP y UDP, que se diferencian por el tipo de servicio que ofrecen. TCP, es un protocolo orientado a conexión que brinda detección de errores. En cambio, UDP es un protocolo no orientado a conexión en el que la detección de errores es obsoleta.

2.1.8 Capa de aplicación

Se encuentra en la parte superior de las capas del protocolo TCP/IP. Contiene las aplicaciones de red que permiten la comunicación mediante las capas inferiores. Por lo tanto, el software en esta capa se comunica mediante uno o dos protocolos de la capa inferior (la capa de transporte), es decir, TCP o UDP. Se pueden clasificar según los servicios que brindan: administración de archivos e impresión (transferencia), conexión a la red, conexión remota, diversas utilidades de Internet.

2.1.9 Introducción IPv4 e IPv6

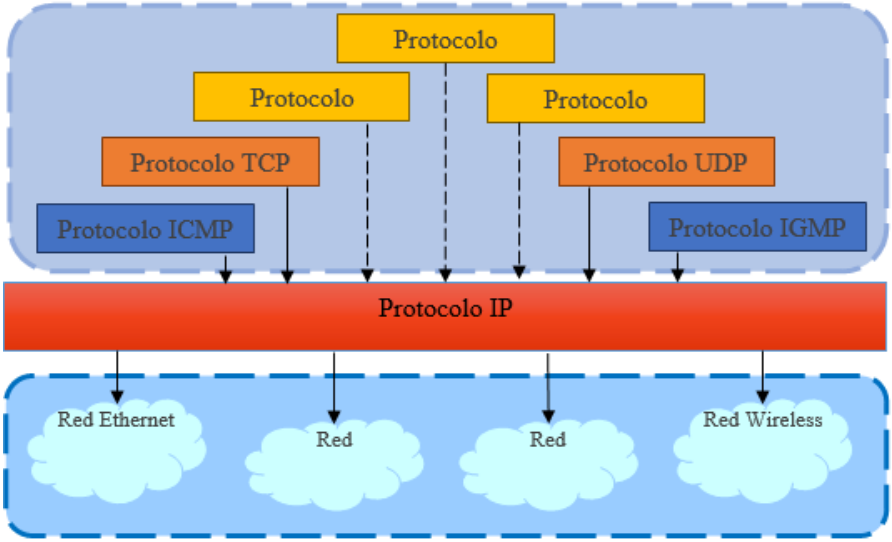


Figura 21. Protocolo IP

El protocolo TCP/IP es el utilizado para gestionar el tráfico de datos en la red. Este protocolo en realidad está formado por dos protocolos diferentes y que realizan acciones diferentes. Por un lado, está el protocolo TCP, que es el encargado del control de transferencia de datos y por otro está el protocolo IP, que es el encargado de la identificación de la máquina en la red un código único como el número de cédula de un ciudadano (EcuRed, 2017).

El direccionamiento es una función clave de los protocolos de capa de red que permite la comunicación de datos entre hosts, independientemente de si los hosts se encuentran en la misma red o en redes diferentes. Tanto el protocolo de Internet versión 4 (IPv4) como el protocolo de Internet versión 6 (IPv6) proporcionan direccionamiento jerárquico para los paquetes que transportan datos.

El diseño, la implementación y la administración de un plan de direccionamiento IP adecuado asegura que las redes puedan operar de manera eficaz y eficiente. Se examina detalladamente la estructura de las direcciones IP y su aplicación en la construcción y la puesta a prueba de redes y subredes IP (Cisco Networking, 2014) direcciones únicas, muchas de las cuales están dedicadas a redes locales LAN. Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos, ya hace varios años se vio que escaseaban las direcciones IPv4.

Esta limitación ayudó a estimular el impulso hacia Ipv6, que está actualmente en las primeras fases de implantación, y se espera que termine reemplazando a IPv4 y a su vez, poder abastecer la demanda existente. IPv6 es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual del IPv4. En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no lo son o se usan con poca frecuencia, se quitaron o se hicieron opcionales, y se agregaron nuevas características.

2.1.10 Configuración de la Red en GNU/LINUX

- Indicar la dirección IP y la máscara de red de cada una de las interfases que dispone la máquina.
- Deshabilitar la interfaz de la tarjeta de red anterior.
- Configurar la dirección IP de la interfaz de red operativa del equipo Linux a 172.16.1equipo.
- Modificar la dirección IP de la interfaz operativa de 172.16.1equipo a 100.210.aula.1equipo.

- Realizar un ping a la dirección IP. Enviar únicamente 4 paquetes.
- Listar todos los comandos necesarios para configurar la ruta estática de enrutamiento del PC LINUX del siguiente esquema de tal manera que tenga acceso a toda la red. Listar la tabla de enrutamiento final.

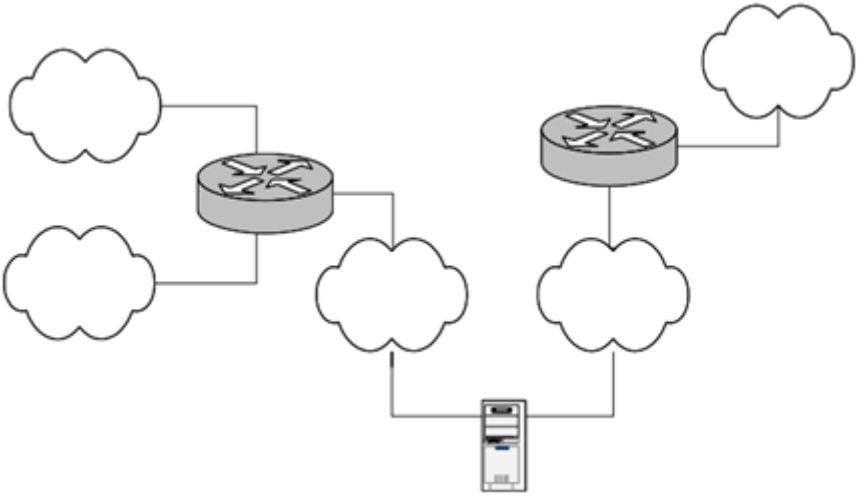


Figura 22. Representación de configuración de Red

- Cambiar el nombre de la máquina de forma cuando se inicie el sistema.
- Cambiar la dirección IP de la interfaz de red a 192.168.1.10, a través del fichero de red (etc/network/interfaces)
- Modificar la configuración del sistema para añadir un gateway por defecto con dirección IP 192.168.1.1. Indicar qué archivo es necesario modificar y la sintaxis empleada.

- Reinicializar la red del equipo mediante comando.
- Comprobar que los parámetros de red del equipo modificados son los esperados (interfaz, tabla de routing).

2.1.11 Conexión a redes inalámbricas (Wifi) desde terminal

Configurar y conectarse a una red Wifi desde la interfaz gráfica es un procedimiento relativamente trivial, al dejarse que todos los procedimientos los realicen NetworkManager o Connman. Sin embargo, hay circunstancias en las cuales puede ser necesario conectarse a una red Wifi desde una terminal. A continuación, se describen los procedimientos para conectarse a los dos tipos de redes Wifi más utilizados, WEP y WPA, con configuraciones básicas utilizadas en dispositivos como serían los puntos de acceso de los modem ADSL de Prodigy Infinitum.

¿Qué es WPA? ¿Por qué debería usarlo en lugar de WEP?

WPA (Wi-Fi Protected Access) y WPA2 es una clase de sistemas para el aseguramiento de redes inalámbricas. WPA fue creado en respuesta a las serias debilidades de otros protocolos como WEP (Wired Equivalent Privacy). Implementa la mayoría de lo que conforma el estándar IEEE 802.11i y fue diseñado para funcionar con todas los dispositivos para redes inalámbricas, excepto los puntos de acceso de primera generación. WPA2 implementa todo el estándar IEEE 802.11i, pero no funciona con muchos dispositivos viejos. WPA fue creado por el grupo industrial y comercial Alianza Wi-Fi, dueños de la marca registrada Wi-Fi y certificadores de los dispositivos que ostenten dicho nombre.

Los datos utilizan el algoritmo RC4 con una clave de 128 bits y un vector de inicialización de 48 bits. Una de las mejoras más

sobresalientes sobre su predecesor, WEP, es TKIP (Temporal Key Integrity Protocol o Protocolo de integridad de clave temporal), el cual consiste en el cambio dinámico mientras se utiliza el sistema. Cuando se combina con Vectores de Inicialización mayores, hace considerablemente más difícil realizar ataques para la obtención de llaves, como ocurre con WEP.

Además de proporcionar autenticación y ciframiento, WPA proporciona mejor integridad de la carga útil. La verificación de redundancia cíclica (CRC o Cyclic Redundancy Check) utilizada en WEP es insegura porque permite alterar la carga útil y actualizar el mensaje de verificación de redundancia cíclica sin necesidad de conocer la clave WEP.

En cambio, WPA utiliza un Código de Integridad de Mensaje (MIC o Message Integrity Code) que es en realidad un algoritmo denominado «Michael», que fue el más fuerte que se pudo utilizar con dispositivos antiguos para redes inalámbricas a fin de no dejar obsoletos a estos. El Código de Integridad de Mensaje de WPA incluye un mecanismo que contrarresta los intentos de ataque para vulnerar TKIP y bloques temporales.

En resumen, WPA hace más difícil vulnerar las redes inalámbricas al incrementar los tamaños de las claves y Vectores de Inicialización, al reducir el número de paquetes enviados con claves relacionadas y añadir un sistema de verificación de mensajes. Además de poder utilizar una clave compartida (PSK o Pre-Shared Key), lo cual suple la complejidad de implementación de un servidor de autenticación 802.1X en hogares y oficinas pequeñas, WPA puede utilizar Protocolos Extensibles de Autenticación (EAP o (Extensible Authentication Protocol), como los siguientes:

- EAP-TLS

- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM
- EAP-LEAP

Entre los diversos servidores que pueden utilizarse para este tipo de implementaciones, está FreeRADIUS. Alcance Libre cuenta con un modesto documento para la configuración de esta implementación.

2.1.12 Equipamiento lógico necesario

Instalación a través de yum.

Se requieren los paquetes *wireless-tools* y *wpa_supplicant*. Para instalar o actualizar el equipamiento lógico necesario en CentOS, Fedora o Red Hat™ Enterprise Linux y versiones posteriores de estos, solo se necesita ejecutar como root lo siguiente: *yum -y install wireless-tools wpa_supplicant*

Si utiliza openSUSE o SUSE Linux Enterprise, solo se necesita ejecutar lo siguiente para instalar o actualizar el equipamiento lógico necesario, en caso de que este estuviese ausente: *yast -i wireless-tools wpa_supplicant*

Si utiliza Debian o Ubuntu y versiones posteriores, solo se necesita ejecutar lo siguiente para instalar o actualizar el equipamiento lógico necesario, en caso de que este estuviese ausente: *sudo apt-get install wireless-tools wpa_supplicant*

Preparativos

En sistemas operativos basados sobre CentOS, Fedora, Red Hat Enterprise Linux, openSUSE y SUSE Linux Enterprise, el primer paso consiste en cambiarse al usuario root: *su -l*

Se debe utilizar sudo para todos los procedimientos en sistemas operativos basados sobre Ubuntu. Ejemplos:

sudo ifup lo

sudo iwconfig wlan0

sudo iwlist wlan0 scan

Debido a que seguramente el servicio NetworkManager hará conflicto con los procedimientos, se debe detener este: *service NetworkMananger stop*

Muchos componentes del sistema requieren que este activa la interfaz de retorno del sistema (loopback), por lo que es importante iniciarla: *ifup lo*

Se ejecuta iwconfig con el nombre de la interfaz como argumento para comenzar a utilizar la interfaz Wifi. Ejemplo: *iwconfig wlan0*

Es buena idea realizar un escaneado de las redes Wifi disponible para asegurarse de que se puede acceder a la red Wifi deseada y para determinar el protocolo a utilizar: *iwlist wlan0 scan*

2.1.13 Autenticar en el punto de acceso

- A través de redes WEP

Para redes inalámbricas con autenticación a través de cifrado WEP, que se caracterizan por tener una seguridad muy pobre, el procedimiento es simple. Se ejecuta lo siguiente para definir el nombre del punto de acceso a utilizar: *iwconfig wlan0 essid punto-de-acceso*

Luego, para definir la contraseña a utilizar —puede ser de 64 o 128 bits: *iwconfig wlan0 key contraseña*

Si se utiliza una clave WEP tipo ASCII, se define de la siguiente manera: *iwconfig wlan0 key s: contraseña*

- A través de redes WPA

Se procede a determinar el nombre de la red Wifi a utilizar y la contraseña. Ejecute *wpa_passphrase* con el nombre del punto de acceso y la contraseña cambiando la salida estándar para generar al archivo */root/wpa.conf: wpa_passphrase punto-de-acceso contraseña > /root/wpa.conf*

Si se realiza el procedimiento desde Ubuntu, lo anterior fallará debido a limitaciones de seguridad de sudo. En su lugar ejecute lo siguiente: *sudo bash -c "wpa_passphrase punto-de-acceso contraseña > /root/wpa.conf"*

Ejecute wpa_supplicant con las opciones -B, para enviar los procesos a segundo plano -D, para especificar el controlador a utilizar y -c para especificar el archivo de configuración creado en el paso anterior e iniciar la autenticación hacia la red Wifi: *wpa_supplicant -B -Dwext -iwlan0 -c/root/wpa.conf*

2.1.14 Configuración de valores de la interfaz de red

Utilizando dhclient

Lo más común es utilizar dhclient para dejar que el servidor DHCP del punto de acceso o la LAN se encargue de asignar los valores de red para la interfaz. Es buena idea indicar a dhclient que libere el préstamo que estuviera asignado en el servidor DHCP: *dhclient -r*

Se ejecuta dhclient con el nombre de la interfaz WiFi como argumento para obtener una nueva dirección IP. Ejemplo: *dhclient wlan0*

2.1.15 Asignación manual de los valores de la interfaz de red

Si se conocen los datos para la configuración de red, también es posible asignarlos manualmente. En el siguiente ejemplo, se asigna a la interfaz wlan0 la dirección IP 192.168.70.50, con máscara de subred 255.255.255.128 (25 bit) y puerta de enlace 192.168.70.1: *ip addr add 192.168.70.50/25 dev wlan0 y ip route add default via 192.168.70.1 dev wlan0*

Se edita el archivo */etc/resolv.conf* y añade o modifica nameserver con la dirección IP del servidor DNS a utilizar como argumento. En el siguiente ejemplo se define 192.168.70.1 como servidor DNS: *echo "nameserver 192.168.70.1" > /etc/resolv.conf*

Si se realiza el procedimiento desde Ubuntu, lo anterior fallará debido a limitaciones de seguridad de sudo. En su lugar se ejecuta lo siguiente: *sudo bash -c "echo 'nameserver 192.168.70.1' > /etc/resolv.conf"*

Para la asignación permanente de valores de la interfaz de red en CentOS, Fedora y Red Hat Enterprise Linux, solo es necesario crear el archivo de interfaz, dentro de */etc/sysconfig/network-scripts/* mediante el siguiente formato: *ifcfg-Auto_punto-de-acceso*

Como ejemplo, si se desea conectar el sistema a un punto de acceso denominado alcance2, se debe crear el archivo */etc/sysconfig/network-scripts/ifcfg-Auto_alcance2: vim /etc/sysconfig/network-scripts/ifcfg-Auto_alcance2*

Si se va a conectar a través de DHCP y utilizar cifrado WEP, se ubica el siguiente contenido:

NAME="Auto alcance2"

ONBOOT=yes

TYPE=Wireless

BOOTPROTO=dhcp

ESSID=alcance2

MODE=Managed

SECURITY_MODE=open

DEFAULTKEY=1

PEERDNS=yes

PEERROUTES=yes

DHCP_CLIENT_ID=nombre-equipo

DHCP_HOSTNAME=nombre-equipo

Si se va a conectar a través de DHCP y utilizar cifrado WPA, se escribe el siguiente contenido:

NAME="Auto alcance2"

ONBOOT=yes

TYPE=Wireless

BOOTPROTO=dhcp

ESSID=alcance2

MODE=Managed

KEY_MGMT=WPA-PSK

PEERDNS=yes

PEERROUTES=yes

DHCP_CLIENT_ID=nombre-equipo

DHCP_HOSTNAME=nombre-equipo

Para la contraseña del punto de acceso, es necesario crear el archivo */etc/sysconfig/network-scripts/keys-Auto_alcance2:vim/etc/sysconfig/network-scripts/keys-Auto_alcance2*

Si se va a conectar por WEP, se escribe el siguiente contenido: *KEY_PASSPHRASE1=contraseña*

Si se va a conectar por WPA, se ubica el siguiente contenido: *WPA_PSK=clave-de-acceso*

Se ejecuta lo siguiente para iniciar la interfaz: *ip link set wlan0 up*

Se ejecuta lo siguiente solo si necesita detener la interfaz*: ip link set wlan0 down*

2.2 Instalación del DNS

En este apartado se comenzarán a realizar los pasos para implementar el servicio de DNS, Correo y Antispam en CentOS 7. Con las configuraciones de esta práctica se aumenta el grado de dificultad para un buen funcionamiento de nuestro servidor.

DNS (Domain Name System) es una base de datos distribuida y jerárquica, que almacena la información necesaria para los nombres de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio.

2.2.1 Configuración de DNS

BIND (acrónimo de Berkeley Internet Name Domain) es una implementación del protocolo DNS y provee una implementación libre de los principales componentes del Sistema de Nombres de Dominio, los cuales incluyen:

- Un servidor de sistema de nombres de dominio (named).
- Una biblioteca resolutoria de sistema de nombres de dominio.
- Herramientas para verificar la operación adecuada del servidor DNS (bind-utils).

Paquete	**Descripción**
bind	Incluye el servidor DNS (named) y herramienta para verificar su funcionamiento.
bind-libs	Bibliotecas compartidas, que consisten en rutinas para aplicaciones para utilizarse cuando se interactúe con servidores DNS.
bind-chroot	Contiene un árbol de archivos que puede ser utilizado como una jaula *chroot* para named, lo que añade seguridad adicional al servicio.
bind-utils	Colección de herramientas para consultar servidores DNS.

Cuadro 1 Descripción paquete BIND

Para comenzar con la implementación de DNS se procede a instalar el paquete yum mediante el siguiente comando: *yum -y install bind bind-chroot bind-utils (ver figura 23).*

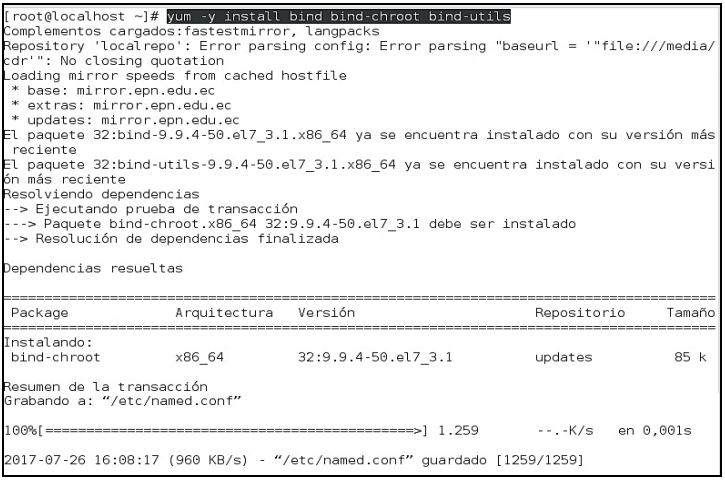


Figura 23. Instalación del paquete yum.

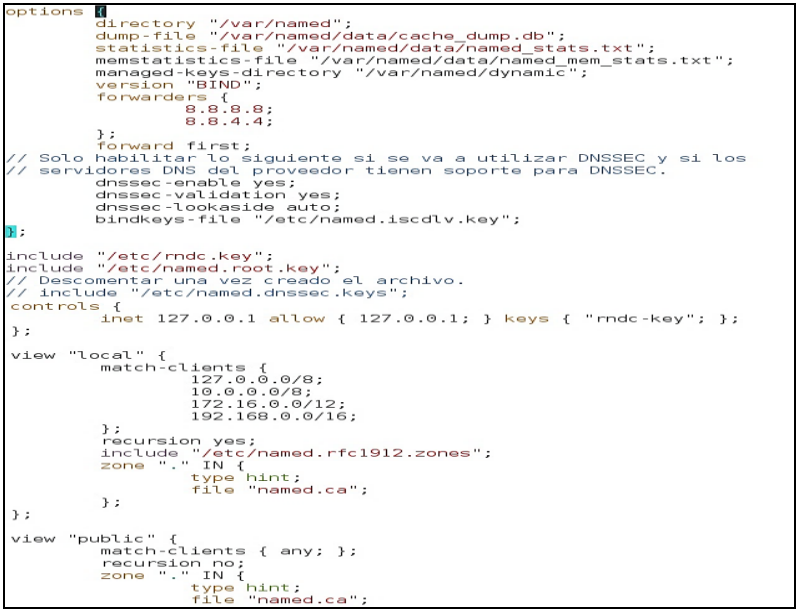
2.2.2 SElinux y el servicio named

SElinux nos protege al servicio named contra las vulnerabilidades de falsificaciones de tráfico DNS al contaminar la cache de los servidores. Se debe cuidar que el archivo tenga los contextos de SELinux correcto, al ejecutar lo siguiente: *restorecon -v /etc/named.conf*

El archivo debe pertenecer a root y el grupo named: *chown root:named /etc/named.conf*

Asignar permiso de lectura y escritura para usuario, solo lectura para grupo y nada para otros (rw-r-----), *chmod 640 /etc/named.conf*

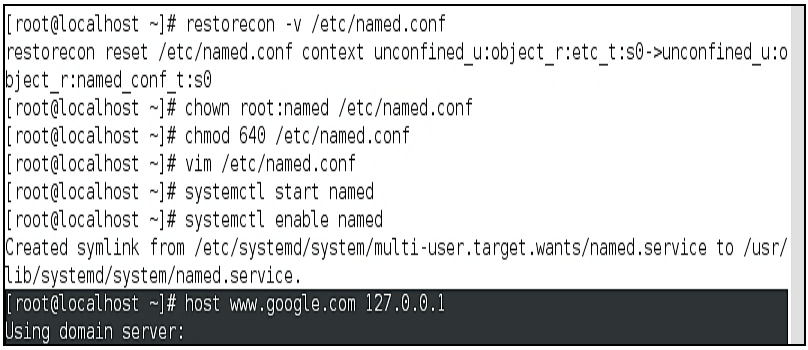
Editar el archivo */etc/named.conf: vim /etc/named.conf* (ver figura 24).



```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        managed-keys-directory "/var/named/dynamic";
        version "BIND";
        forwarders {
                8.8.8.8;
                8.8.4.4;
        };
        forward first;
// Solo habilitar lo siguiente si se va a utilizar DNSSEC y si los
// servidores DNS del proveedor tienen soporte para DNSSEC.
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        bindkeys-file "/etc/named.iscdlv.key";
};

include "/etc/rndc.key";
include "/etc/named.root.key";
// Descomentar una vez creado el archivo.
// include "/etc/named.dnssec.keys";
controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

view "local" {
        match-clients {
                127.0.0.0/8;
                10.0.0.0/8;
                172.16.0.0/12;
                192.168.0.0/16;
        };
        recursion yes;
        include "/etc/named.rfc1912.zones";
        zone "." IN {
                type hint;
                file "named.ca";
        };
};

view "public" {
        match-clients { any; };
        recursion no;
        zone "." IN {
                type hint;
                file "named.ca";
```

Figura 24. Edición del archivo named.conf

Para iniciar el servicio y arranque del sistema, se escriben los siguientes comandos en el terminal: *Systemctl start named.conf y systemctl enable named* (ver figura 25).



```
[root@localhost ~]# restorecon -v /etc/named.conf
restorecon reset /etc/named.conf context unconfined_u:object_r:etc_t:s0->unconfined_u:o
bject_r:named_conf_t:s0
[root@localhost ~]# chown root:named /etc/named.conf
[root@localhost ~]# chmod 640 /etc/named.conf
[root@localhost ~]# vim /etc/named.conf
[root@localhost ~]# systemctl start named
[root@localhost ~]# systemctl enable named
Created symlink from /etc/systemd/system/multi-user.target.wants/named.service to /usr/
lib/systemd/system/named.service.
[root@localhost ~]# host www.google.com 127.0.0.1
Using domain server:
```

Figura 25. Inicio y habilitación del sistema.

Se comprueba que el servidor DNS recién configurado es capaz de resolver nombres por sí mismo. Se ejecuta el siguiente comando: *host www.google.com 127.0.0.1* (ver figura 26).

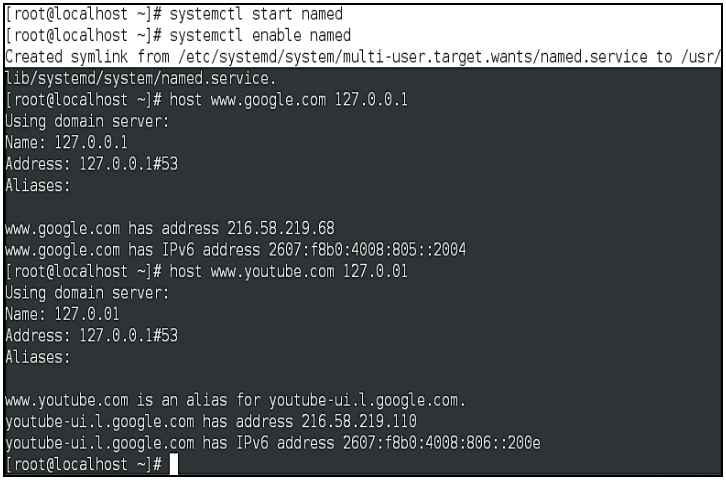


Figura 26. Verificación del funcionamiento de servidor DNS.

Se procedemos a configurar 127.0.0.1 como único DNS del sistema.

Si lo anterior funciona, comienza a editar el archivo */etc/resolv.conf: vi /etc/resolv.conf*

Establezca a 127.0.0.1 como único servidor DNS. Ejemplo: *search admincc.com* y *nameserver 127.0.0.1*

Nota: Si la interfaz está configurada por DHCP, añada la opción PEERDNS con valor no y DNS1 con valor 127.0.0.1.

Se edita el archivo de configuración de la interfaz principal de su servidor: *vi /etc/sysconfig/network-scripts/ifcfg-enp0s3* (ver figura 27).

```
DEVICE=ens33
TYPE=Ethernet
NAME="ens33"
BOOTPROTO=none
ONBOOT=yes
IPV4_FAILUERE_FATAL=yes
IPV6INIT=no
UUID=cae53305-d966-4dba-a8a4-1e1a42b275e3
DEFROUTE=no
NM_CONTROLLED=no
HWADDR=00:0c:29:df:f9:98
PEERDNS=no
DOMAIN=admincc.com
DNS1=127.0.0.1
```

Figura 27. Edición de la interfaz del servidor.

Reinicie el servicio de red para aplicar los cambios: *service network restart*

Para verificar si el DNS predeterminado del sistema puede resolver nombres. Ejecute el siguiente comando: host www.google.com (ver figura 28).

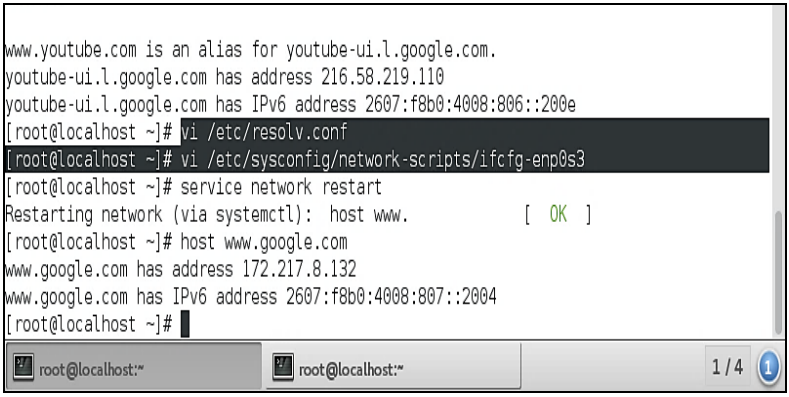


Figura 28. Comprobación del funcionamiento DNS.

2.3 Servidor de correo

Un servidor de correo es una aplicación informática que tiene como objetivo, enviar, recibir y gestionar mensajes a través de las redes de transmisión de datos existentes, con el fin de que los usuarios puedan mantenerse comunicados con una velocidad muy superior a la que ofrecen otros medios de envío de documentos.

2.3.1 Configuración de correo

Para comenzar con el procedimiento se utiliza Postfix. Este es un servidor de correo de software libre y código abierto, que se lo utiliza normalmente para el enrutamiento y envío de correo electrónico. Fue creado como una alternativa más rápida, fácil de administrar y segura, ampliamente utilizado es Sendmail.

Primero se deben instalar los paquetes de postfix: *yum -y install postfix**

Se comprueba si el servicio se está ejecutando correctamente, a través del siguiente comando: *systemctl status postfix.service*

Luego corresponde configurar el archivo de postfix: *gedit /etc/postfix/main.cf*

Dentro de archivo postfix varios de los comandos se encuentran comentados con el signo #, se deben descomentar algunos comandos entre ellos están: *myhostname= accserver.localdomain.com*

En el comando “mydomain” se escribe el nombre del servidor que se utiliza, para hacer la cuenta de los usuarios de quienes van a pertenecer al servicio.

mydomain= accserver.com

myorigin= $mydomain

inet_interfaces= all

Por defecto trae la interfaz de manera local y se comenta tal comando: *#inet_interfaces= localhost*

Por defecto trae la configuración de destino descomentada y no se usará, por lo tanto, se vuelve a comentar de esta manera: *#mydestination= $myhostname, localhost.$mydomain, localhost*

Luego se descomenta al comando que sí se va a utilizar: *mydestination= $myhostname, localhost.$mydomain, localhost, $mydomain*

Se procede a descomenta el siguiente comando: *home_mailbox= Maildir/*

En “mynetworks” se descomenta y luego se coloca una dirección de red válida para nuestro servidor: *mynetworks= 192.168.43.0/24 127.0.0.0/8*

Una vez realizado todo esto, se presiona el botón” Guardar” de la terminal y se cierra el archivo.

Para el siguiente paso, se reinicia el servicio de postfix, a través del comando: *systemctl restart postfix.service*

Ahora con los siguientes comandos, se creans los usuarios netamente en CentOS para los cuales se va a utilizar en nuestro servicio de postfix: *useradd danny* (ver figura 29).

Se asigna una contraseña: *passwd danny*

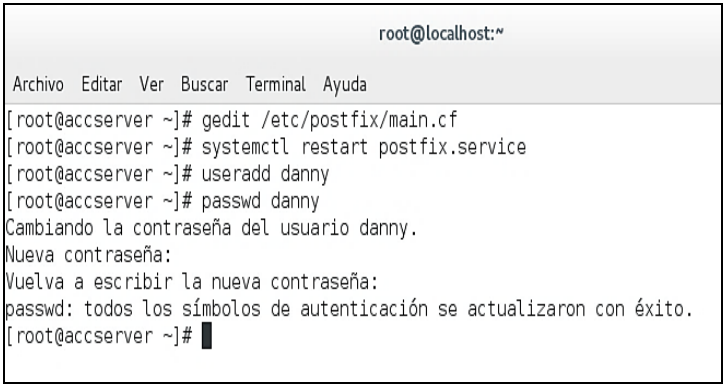


Figura 29. Creación de usuario.

Ahora se hace un envío de mensaje de prueba, en donde se utiliza el comando telnet y luego se procede a escribir los siguientes parámetros: *telnet localhost smtp* (ver figura 30).

Nota: Con el parámetro punto "." Se hace la terminación del texto. Con el parámetro "quit" se da por terminado el servicio.

Figura 30. Mensaje de prueba.

Para verificar si el mensaje ha llegado al otro usuario, se digita el siguiente comando: *cd /home/alex/Maildir/new y ls -l*

Para el siguiente paso, se debe utilizar el servicio llamado “Dovecot”, es un servidor de POP3 e IMAP de fuente abierta que funciona en Linux y sistemas basados sobre Unix™ y diseñado con la seguridad como principal objetivo. Dovecot puede utilizar tanto el formato mbox como maildir y es compatible con las implementaciones de los servidores UW-IMAP y Courier IMAP.

Se instala con el siguiente comando: *yum -y install dovecot**

Se configura el archive dovecot: *gedit /etc/dovecot/dovecot.conf*

Se procede a descomentar el comando relacionado con el postfix para el respectivo funcionamiento y después de ello, se da click en el botón “Guardar” y se cierra la terminal del archivo*: protocols= imap pop3 lmtp* (ver figura 31).

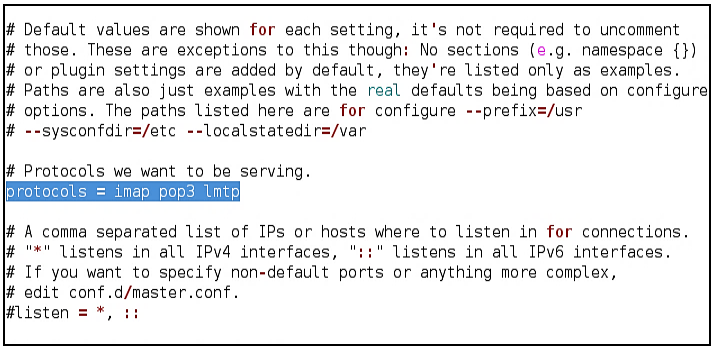


Figura 31. Configuración archivo dovecot.

Se coloca el siguiente comando para modificar algunos archivos y luego se digita con el comando *ls* para observar los archivos pertenecientes*: cd /etc/dovecot/conf.d* (ver figura 32).

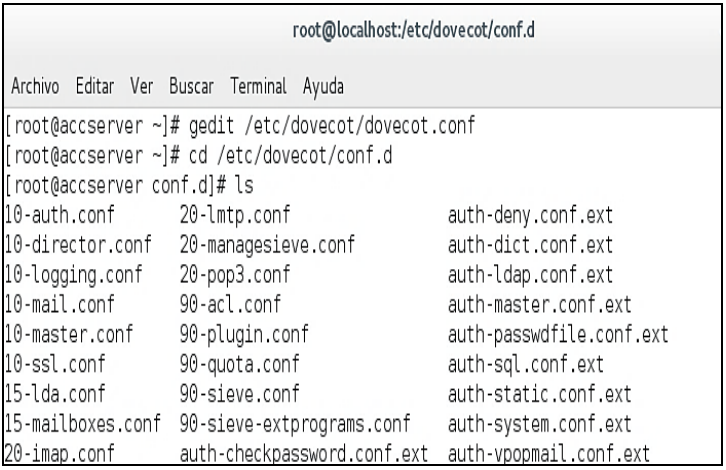


Figura 32. Acceso a dovecot/conf.d

Se comienzan a escribir los comandos de los archivos a modificar:

- Primer archivo: *gedit 10-auth.conf*

Una vez que se escribe el comando, se abrirá una ventana del archivo para lo cual se descomentará disable_plaintext_auth= no luego se guarda y cierra.

- Segundo archivo: *gedit 10-mail.conf*

Se abrirá una ventana donde se descomentará *disable_plaintext_auth= yes*. Seguido a esto, se cambia el valor del parámetro a un valor no. Por lo tanto, quedará de esta forma: *disable_plaintext_auth= no* luego se guardan los cambios y cierra la ventana del archivo.

- Tercer archivo: *gedit 10-email.conf*

Se descomentarán las siguientes opciones, y luego se guarda: *mail_location= maildir:~/Maildir*

Aquí se colocan los siguientes valores: *mail_uid= vmail y mail_gid=vmail*

- Cuarto archivo: *gedit 20-pop3.conf*

Se descomentarán las siguientes opciones, y luego se guarda: *pop3_uidl_format = %08Xu%08Xv*

Se reinicia y comprueba el estado del servicio de dovecot: *systemctl restart dovecot.service y systemctl start dovecot.service* (ver figura 33).

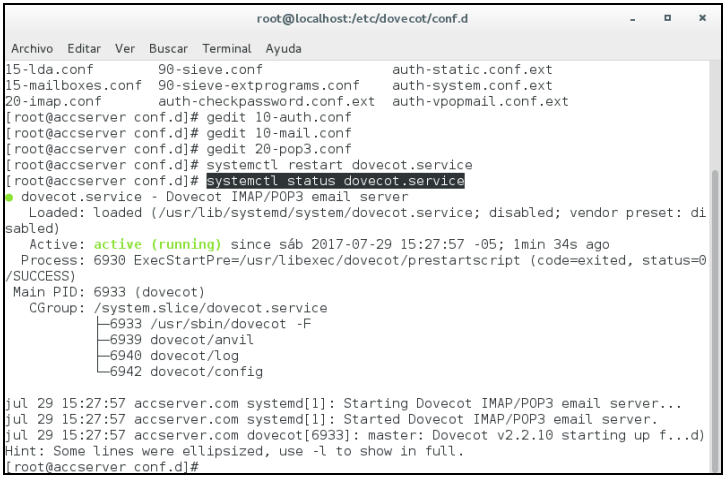


Figura 33. Comprobación del servicio dovecot

Se debe descargar Thunderbind, a través del siguiente enlace: https://centos.pkgs.org/7/centos-86_64/thunderbird-45.4.0-1.el7.centos.x86_64.rpm.html

Se accede a la carpeta descarga y comprueba que el programa este allí. Se presiona sobre el programa y procede a instalarlo (ver figuras 34 y 35.

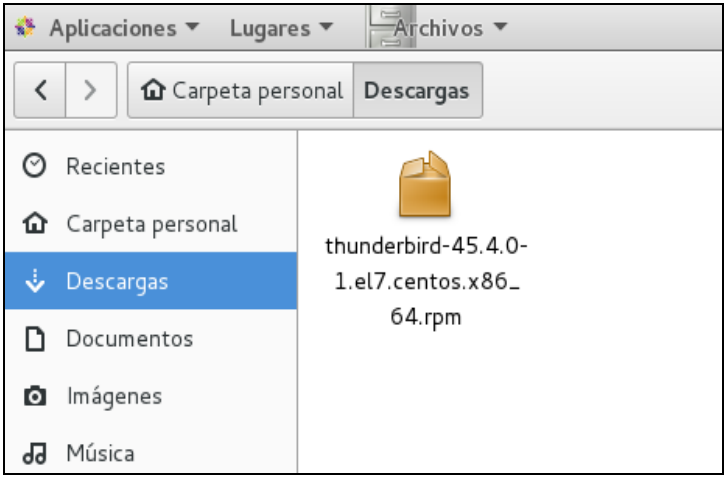


Figura 34. Programa Thunderbird

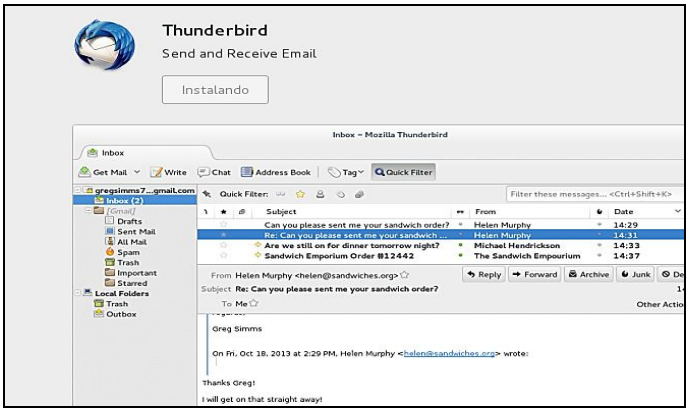


Figura 35. Instalación de Thunderbird

Para abrir el programa se siguen los siguientes pasos: *Aplicaciones>Thunderbird*

Se crean las cuentas de usuario (ver figura 36).

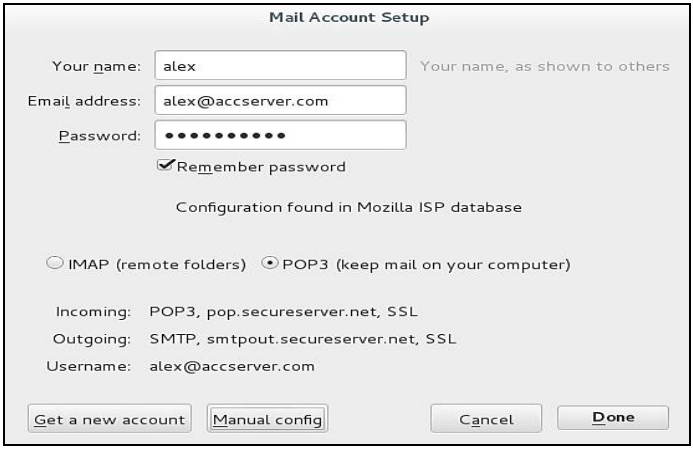


Figura 36. Creación de usuario.

Se configura manualmente, para eso click en el botón Manual Config. (ver figura 37).

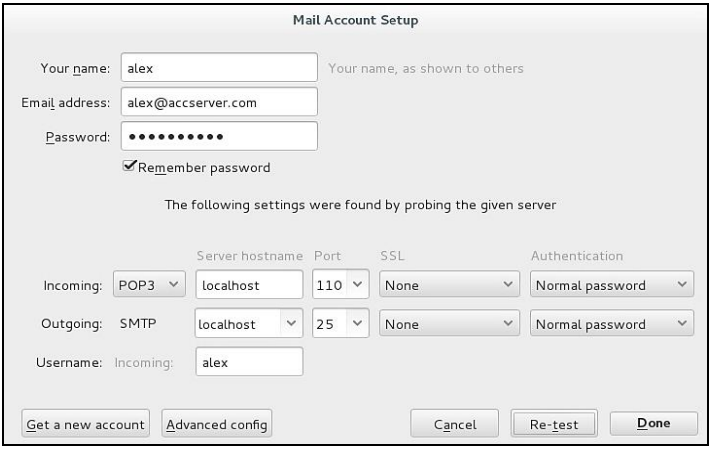


Figura 37. Configuración de cuenta usuario.

Aparece un aviso de peligro ante el cual se presiona *check I understand the risks, click* en Done (ver figura 38).

Figura 38. Ventana de alerta.

Verificar que se ha creado correctamente (ver figura 39).

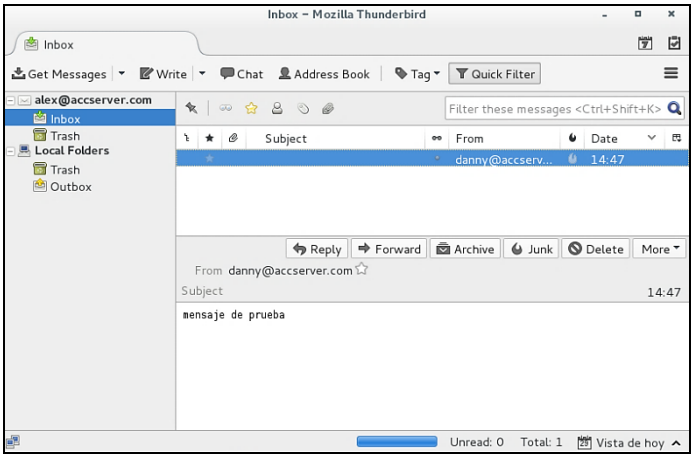


Figura 39. Verificación del usuario creado.

Se crea el usuario 2, *click* en el botón *Skip this and use my existing email* (ver figura 40).

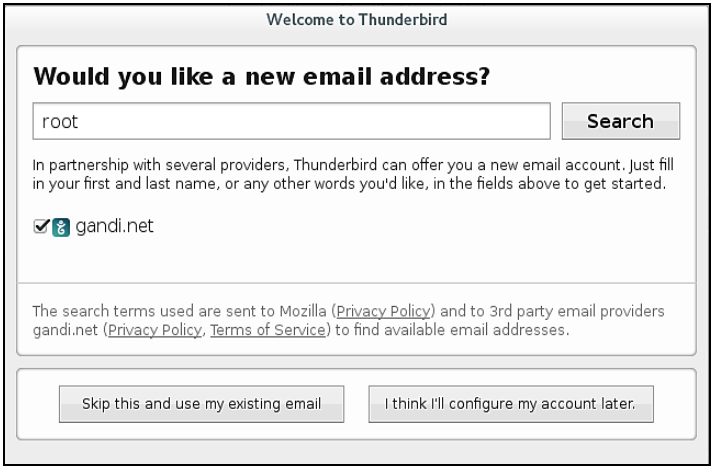


Figura 40. Creación de usuario 2.

Seguir los pasos anteriormente indicados (ver figuras 41, 42 y 43).

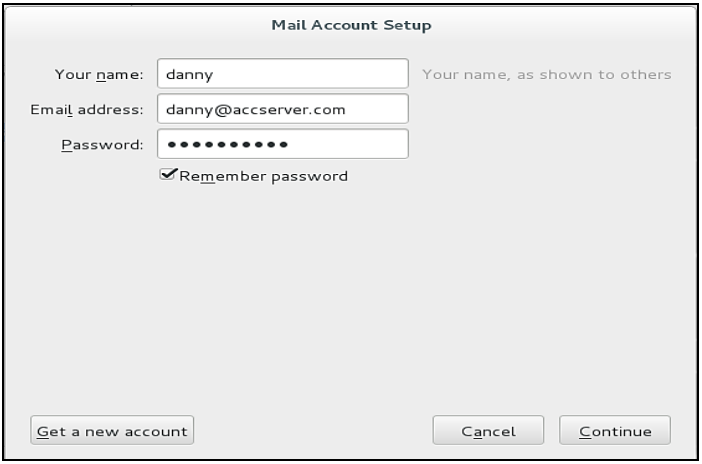


Figura 41. Creación usuario 2. Paso 1.

Figura 42. Creación usuario 2. Paso 2.

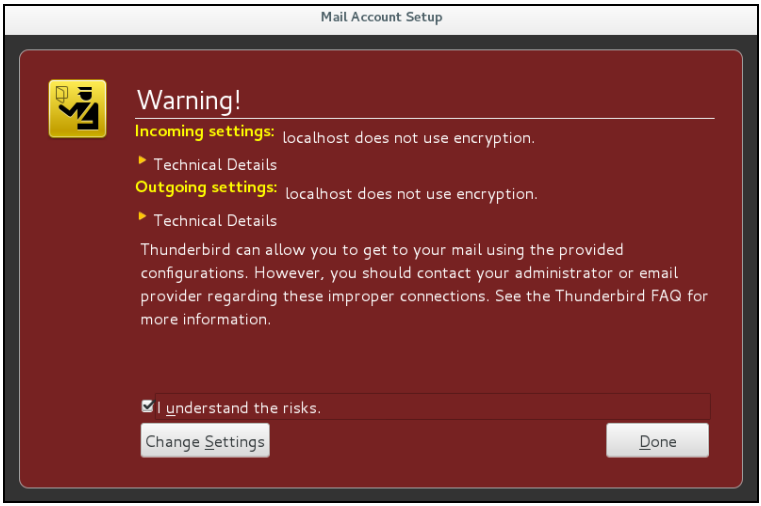


Figura 43. Creación usuario 2. Paso 3.

Una vez finalizada la creación de los dos usuarios, se realiza una prueba de envío de mensaje para comprobar su funcionamiento (ver figura 44).

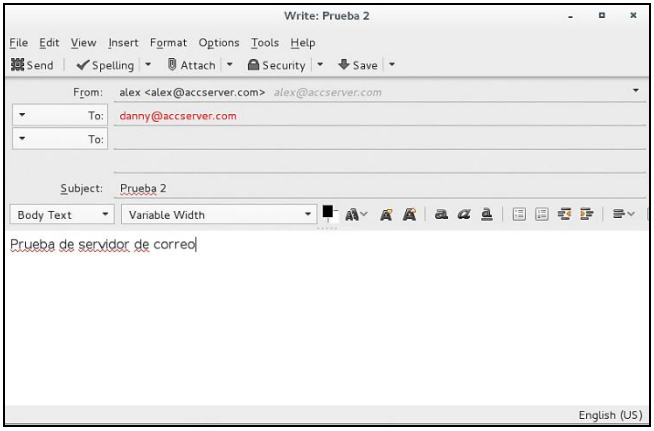


Figura 44. Prueba de mensaje

Se verifica el envío correcto, ejemplo: el mensaje del primer usuario Alex hacia el segundo usuario Danny (ver figura 45).

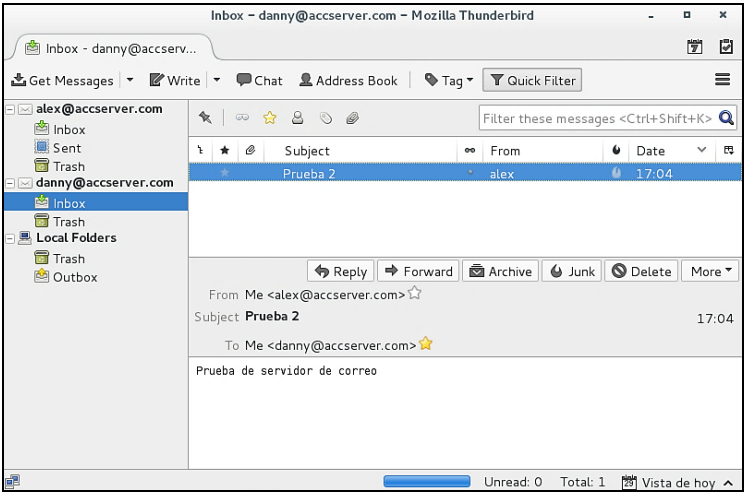


Figura 45. Comprobación de mensaje recibido.

Capítulo 3

CAPÍTULO 3: GESTIÓN DE SERVICIOS FTP, NSCA

3.1 Implementación FTP

3.1.1 FTP (File Transfer Protocol)

Esta herramienta permitirá, a través de la red, copiar ficheros de un ordenador a otro basado en el proyecto como Cliente-servidor. No importa en absoluto dónde están localizados estos ordenadores, o si es que usan el mismo sistema operativo, basta que estén conectados a Internet se podrán compartir los ficheros.

FTP (*File Transfer Protocol*) o Protocolo de Transferencia de Archivos (o archivos informáticos) es uno de los protocolos estándar más utilizados en Internet por ser el más idóneo para la transferencia de grandes bloques de datos a través de redes que soporten TCP/IP. El servicio utiliza los puertos 20 y 21, exclusivamente sobre TCP. El puerto 20 es utilizado para el flujo de datos entre cliente y servidor. El puerto 21 es utilizado para el envío de órdenes del cliente hacia el servidor.

3.1.2 Configuración de FTP

Primero se procede a instalar los paquetes o dependencias necesarias mediante el comando: *yum -y install vsftpd*. Se debe esperar que el proceso de instalación inicie, este tomará un periodo corto de tiempo (ver figura 46).

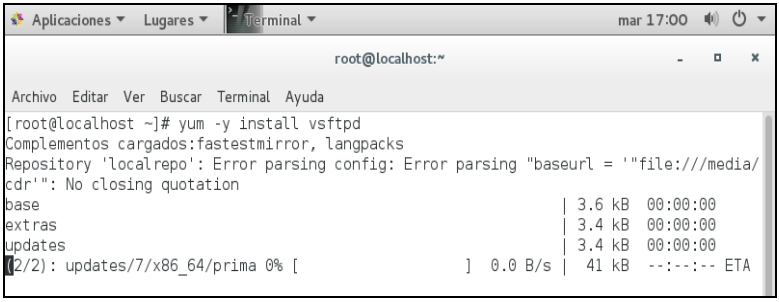


Figura 46. Instalación de los paquetes FTP.

3.1.3 FTP sin certificados

Ingresar al usuario *root* con el comando *su* (ver figura 47).

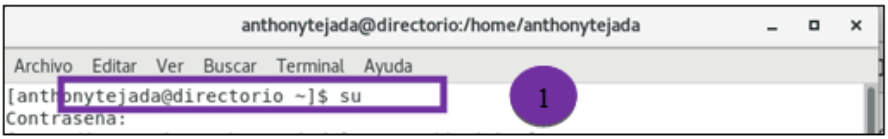


Figura 47. Configuración FTP paso 1

3.1.4 Creación de Usuarios y Grupos

Se crean dos usuarios para poder emplear el servicio de FTP, en el cual se lanza el comando *useradd* seguido del nombre a crear y el *passwd*, en él se vuelve a ingresar el nombre del usuario. El sistema pedirá ingresar un cambio de contraseña (ver figura 48).

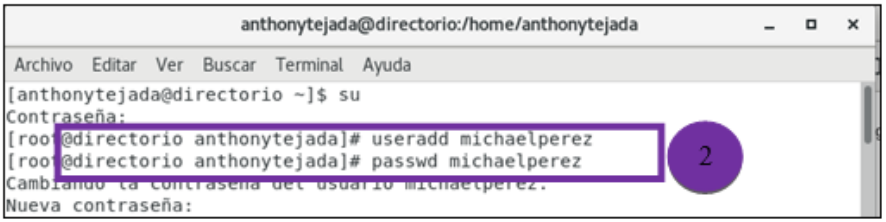


Figura 48. Configuración FTP paso 2

Se realiza el mismo procedimiento para crear otro usuario (ver figura 49).

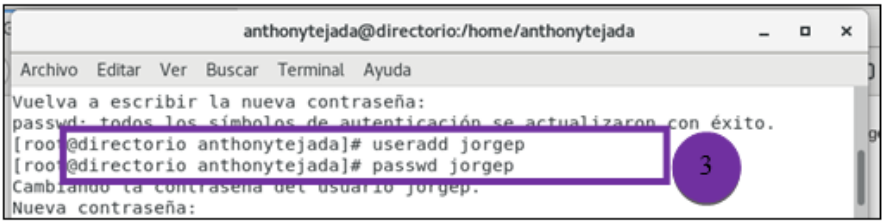


Figura 49. Configuración FTP paso 3

Aparece la opción de crear un grupo y añadir a los nuevos usuarios, mediante el siguiente comando: *groupadd Administracion y gpasswd -a michaelperez Administracion* (ver figura 50).

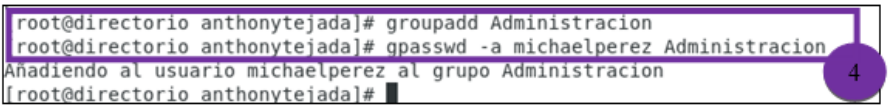


Figura 50. Configuración FTP paso 4

3.1.5 Proceso de Instalación y Configuración

- Instalar el paquete *wsftpd*, necesario para levantar este servicio. Si se tiene conexión a Internet hacerlo mediante *yum*, ejecutar: *yum -y install vsftpd* (ver figura 51 y 52).

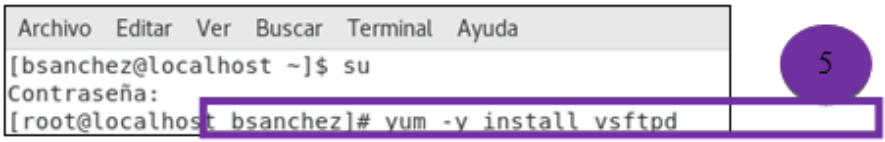


Figura 51. Configuración FTP paso 5.1

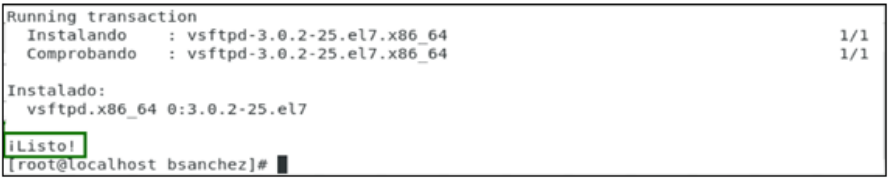


Figura 52. Configuración FTP paso 5.2

En caso de presentar error en la instalación, solucionar matando la aplicación que impide la instalación con: kill [pid del proceso] (ver figura 53).

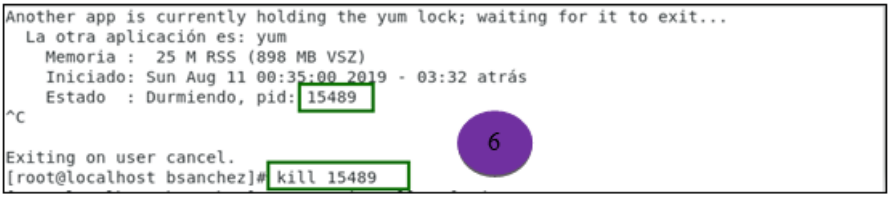


Figura 53. Configuración FTP paso 6

El archivo de configuración de VSFTPD, se encuentra en la ruta: */etc/vsftpd/vsftpd.conf*

Se continúa con la instalación del ftp con el comando: *yum install ftp*

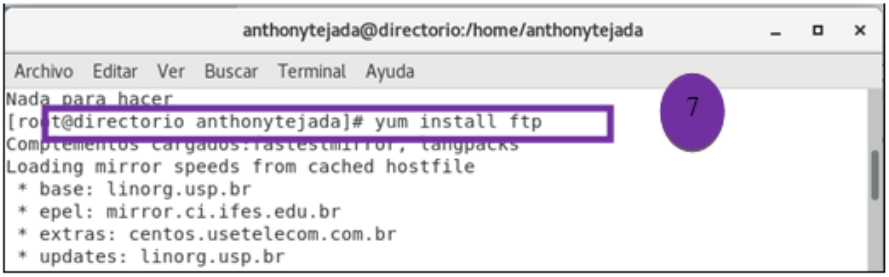


Figura 54. Configuración FTP paso 7

Para configurar de forma permanente el firewall se lanza el siguiente comando: *firewall-cmd --zone=public --add-port=3128/tcp –permanent*

Luego, actualizar el firewall para hacer efectivos los cambios realizados con el comando: *firewall-cmd --reload*

Ingresar a la ruta *cd /etc/vsftpd*

Mostrar los diferentes usuarios que previamente se han creado con el comando *ls*

Editar el archivo de configuración *vsftpd.conf* con el comando: nano *vsftpd.conf* (ver figura 55).

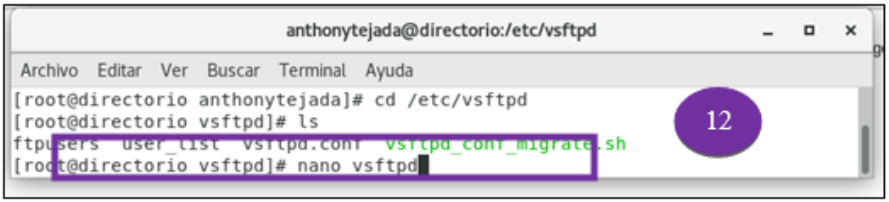


Figura 55. Configuración FTP paso 12

En el documento de configuraciones se edita el acceso anónimo, al denegar, de la siguiente forma: *anonymous_enable=NO* (ver figura 56).

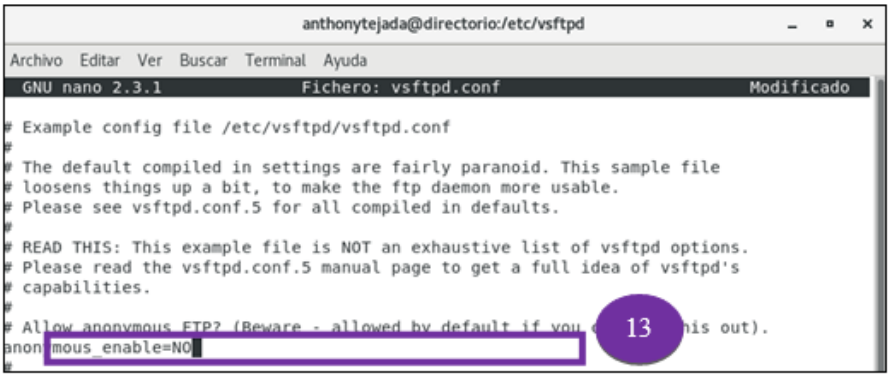


Figura 56. Configuración FTP paso 13

Se continúa con el proceso de edición con la línea: *userlist_enable userlist_enable=NO* (ver figura 57).

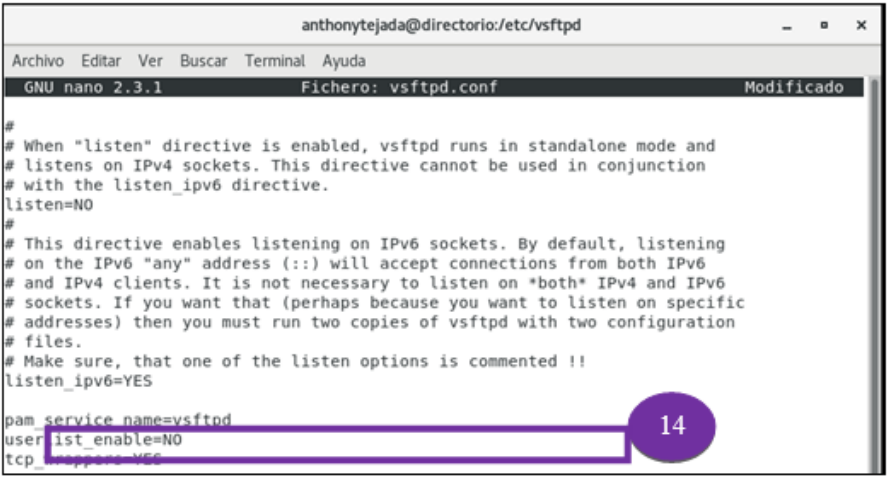


Figura 57. Configuración FTP paso 14

Se edita la lista de usuarios que podrán acceder al servicio ftp: *nano user_list* (ver figura 58).

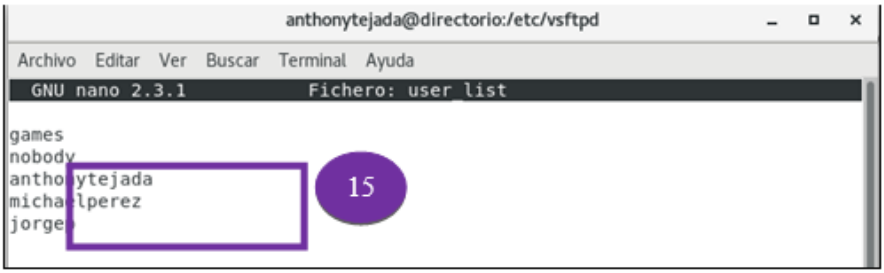


Figura 58. Configuración FTP paso 15

Se finaliza con el proceso de configuración al iniciar el servicio vsftpd con: *service vsfpd start* (ver figura 59).

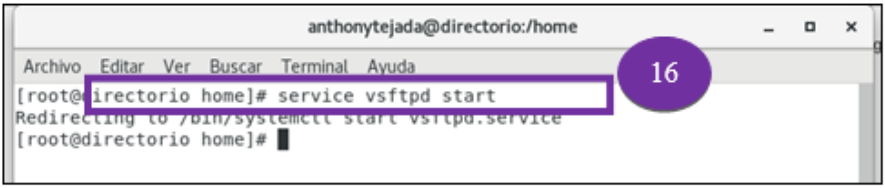


Figura 59. Configuración FTP paso 16

3.1.6 Creación de Archivos para el Servicio FTP

- Se ingresa al directorio cd /home, lanzar ls para mostrar las carpetas de los usuarios (ver figura 60).

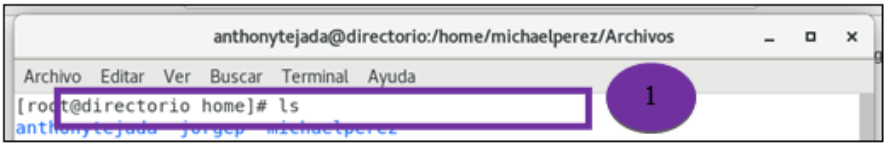


Figura 60. Creación de Archivos para el Servicio FTP paso 1

- Ingresar a la carpeta del usuario.
- Crear una nueva carpeta con el comando: *mkdir Archivos*
- Crear un nuevo archivo de tipo texto: *touch pruebaPerez.txt*
- Editar el nuevo archivo: *nano pruebaPerez.txt*
- Ingresar a la carpeta *cd /home/michaelperez* y hacemos *chmod 777 archivos* (ver figura 61).

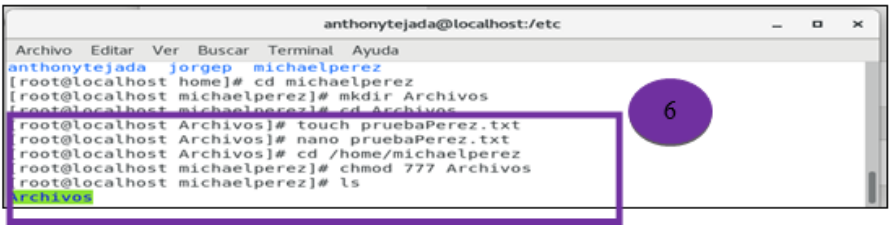


Figura 61. Creación de Archivos para el Servicio FTP paso 6

Realizar el mismo proceso con el siguiente usuario (ver figura 62).

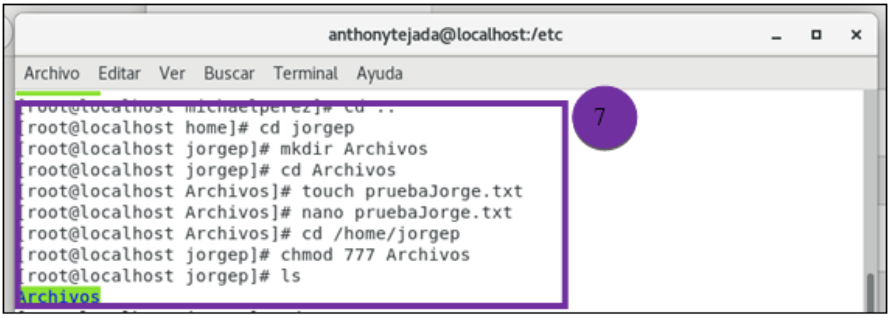


Figura 62. Creación de Archivos para el Servicio FTP paso 7

- Lanzar el comando: *setsebool -P ftp home_dir=1*
- Lanzar el commando: *firewall-cmd --permanent --add-service=ftp* (ver figura 63).

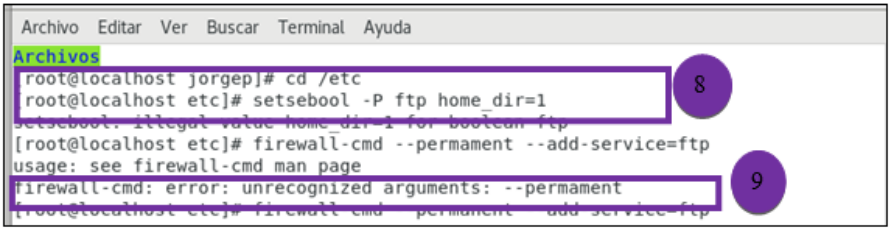


Figura 63. Creación de Archivos para el Servicio FTP paso 9

Notas:

- Para eliminar un usuario se usa el comando *userdel*
- Para borrar el contenido de su carpeta home, a *userdel* se añade el parámetro -r:
- El comando cat sirve para ver el leer archivo o mostrar su contenido (solo lectura): cat /etc/passwd | grep bsanchez
- Para modificar un usuario, se tienen los mismos parámetros que en la creación: Ingresar al navegador y digitar el usuario y contraseña (ver figura 64).

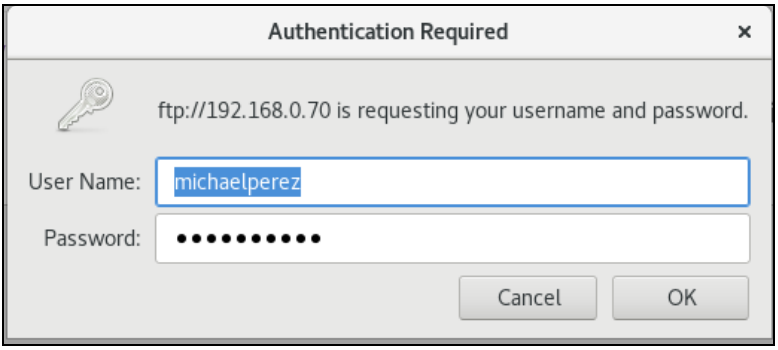


Figura 64. Creación de Archivos para el Servicio FTP paso 10

• Acceder a la carpeta que fue creada con el archivo *pruebaPerez.txt* y así mismo con el otro usuario *pruebaJorge.txt*. (ver figura 65, 66 y 67).

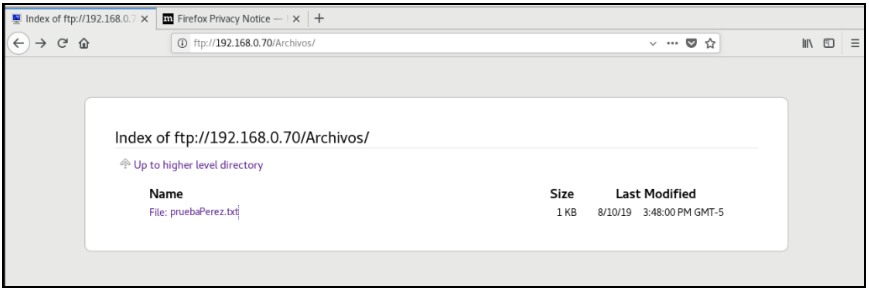


Figura 65. Creación de Archivos para el Servicio FTP paso 11.1

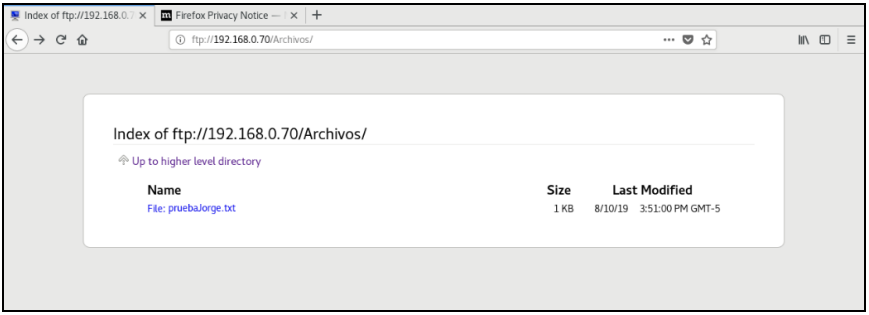


Figura 66. Creación de Archivos para el Servicio FTP paso 11.2

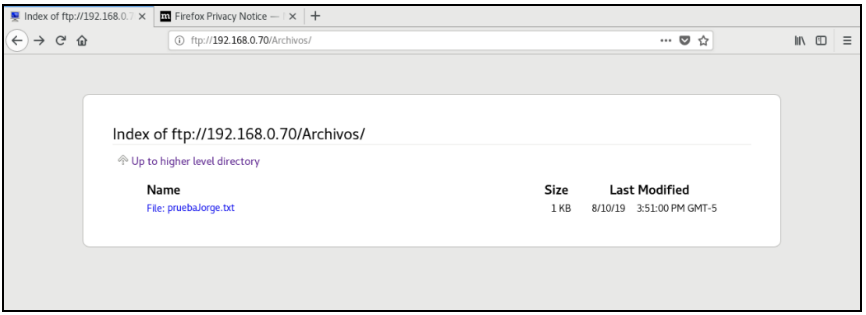


Figura 67. Creación de Archivos para el Servicio FTP paso 11.3

Se podrá identificar el archivo e ingresar para verificar el mensaje que se describió en el mismo. En este caso se refleja el mensaje compartido, mostrará la descripción del archivo .txt con el mensaje confirmando la validación del FTP.

3.1.7 Ediciones Adicionales en el Archivo de Configuración VSFTPD

- Opción *ftpd_banner*. Sirve para establecer el banderín de bienvenida que será mostrado cada vez que un usuario acceda al servidor. Puede establecerse cualquier frase breve que considere conveniente, pero sin signos de puntuación. Ejecutar: *ftpd_banner=Bienvenido al servidor FTP de Sistemas Operativos* (ver figura 68)

```
# You may fully customise the login banner string:
ftpd_banner=Bienvenido al servidor FTP de Sistemas Operativos
```

Figura 68. Ediciones Adicionales en el Archivo de Configuración VSFTPD paso 1

Las siguientes opciones están ausentes en la configuración predeterminada, se añaden al final del archivo */etc/vsftpd/vsftpd.conf.*

Opciones *pasv_min_port* y *pasv_max_port*. Permiten establecer el rango arbitrario de puertos utilizados para las conexiones pasivas. Puede elegirse cualquier rango de puertos entre 1024 y 65535, el mismo que deberá ser habilitado en el muro cortafuegos del servidor: *pasv_min_port=30300* y *pasv_max_port=30309* (ver figura 69).

```
#pasv_min_port y pasv_max_port
pasv_min_port=30300
pasv_max_port=30309
```

Figura 69. Ediciones Adicionales en el Archivo de Configuración VSFTPD paso 2

Opción *anon_max_rate*. Se utiliza para limitar la tasa de transferencia, en bytes por segundo, para los usuarios anónimos. Para limitar la tasa de transferencia a 500 Kb por

segundo para usuarios anónimos ejecutar: *anon_max_rate=524288* (ver figura 70).

```
#anon_max_rate
anon_max_rate=524288
```

Figura 70. Ediciones Adicionales en el Archivo de Configuración VSFTPD paso 3

Opción local_max_rate. Hace lo mismo que anon_max_rate, pero aplica para usuarios locales del servidor. Para limitar la tasa de transferencia a 1 MB por segundo para los usuarios locales*: local_max_rate=1048576* (ver figura 71).

```
#local_max_rate
local_max_rate=1048576
```

Figura 71. Ediciones Adicionales en el Archivo de Configuración VSFTPD paso 4

Opción max_clients. Establece el número máximo de clientes que podrán acceder simultáneamente hacia el servidor FTP. Para limitar el acceso a 20 clientes simultáneos ejecutar: *max_clients=20* (ver figura 72).

```
#max_clients
max_clients=20
```

Figura 72. Ediciones Adicionales en el Archivo de Configuración VSFTPD paso 5

Opción max_per_ip. Establece el número máximo de conexiones que se pueden realizar desde una misma dirección IP. Tome en cuenta que algunas redes acceden a través de un servidor intermediario (Proxy) o puerta de enlace y debido a esto podrían quedar bloqueados innecesariamente algunos accesos. Para limitar el número de conexiones por IP simultáneas a un máximo de 10 ejecutar: *max_per_ip=10* (ver figura 73).

```
#max_per_ip
max_per_ip=10
```

Figura 73. Ediciones Adicionales en el Archivo de Configuración VSFTPD paso 6

Guardar los cambios y reiniciar el servicio de VSFTPD para hacer efectivos los cambios (ver figura 74).

```
[root@localhost bsanchez]# service vsftpd restart
Redirecting to /bin/systemctl restart vsftpd.service
```

Figura 74. Ediciones Adicionales en el Archivo de Configuración VSFTPD paso 7

3.1.8 FTP con certificado: Instalación y Configuración del VSFTPD con Soporte SSL/TLS

VSFTPD puede ser configurado fácilmente para utilizar los protocolos SSL (Nivel de Zócalo Seguro) y TLS (Seguridad para Nivel de Transporte) a través de un certificado RSA. Pasos:

- Acceder al directorio */etc/pki/tls/* con el comando: *cd /etc/pki/tls/* (ver figura 75).

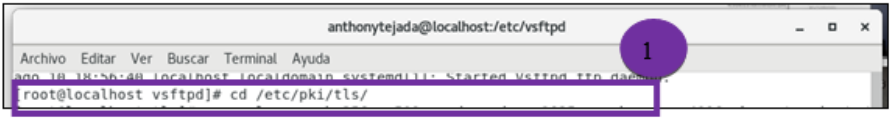


Figura 75. Instalación y Configuración del VSFTPD paso 1

- El certificado y firma digital se pueden generar ejecutando la siguiente línea para utilizar una estructura X.509, algoritmo de cifrado RSA de 4096 bits, sin Triple DES —lo cual permita iniciar normalmente al servicio sin interacción alguna— y una validez por 1825 días —cinco años: *openssl req -sha256 -x509 -nodes -days 1825 -newkey rsa:4096*

-keyout private/vsftpd.key -out certs/vsftpd.crt (ver figura 76).

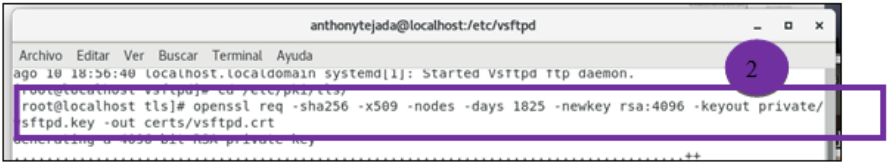


Figura 76. Instalación y Configuración del VSFTPD paso 2

Para la solicitud del certificado se piden los siguientes campos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o bien la razón social.
- Unidad o sección responsable del certificado.
- Nombre del anfitrión (FQDN).
- Dirección de correo electrónico de la persona responsable del certificado (ver figura 77).

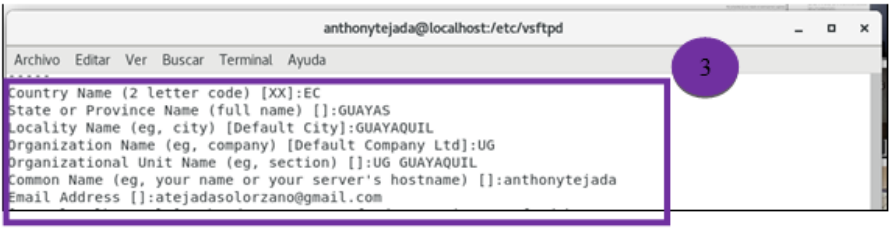


Figura 77. Instalación y Configuración del VSFTPD paso 3

- El archivo del certificado (vsftpd.crt) y el de la firma digital (vsftpd.key), deben tener permisos de lectura y escritura sólo para el usuario root con el comando:

chmod 600 certs/vsftpd.crt private/vsftpd.key (ver figura 78).

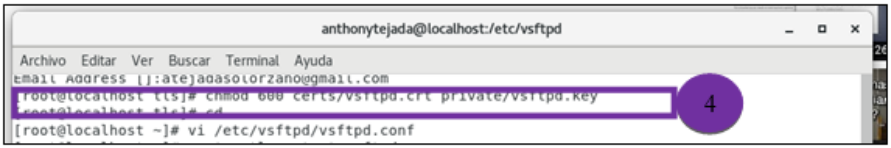


Figura 78. Instalación y Configuración del VSFTPD paso 4

1. Para regresar al directorio de inicio del usuario root con el comando: cd
2. Edite el archivo */etc/vsftpd/vsftpd.conf*: nano */etc/vsftpd/vsftpd.conf*
3. Añada al final de este archivo todo el siguiente contenido:

 # Habilita el soporte de TLS/SSL

ssl_enable=YES

 # Deshabilita o habilita utilizar TLS/SSL con usuarios anónimos

allow_anon_ssl=NO

 # Obliga a utilizar TLS/SSL para todas las operaciones, es decir,

 # transferencia de datos y autenticación de usuarios locales.

 # Establecer el valor NO, hace que sea opcional utilizar TLS/SSL.

force_local_data_ssl=YES

force_local_logins_ssl=YES

 # Se prefiere TLSv1 sobre SSLv2 y SSLv3

ssl_tlsv1=YES

ssl_sslv2=NO

ssl_sslv3=NO

 # Rutas del certificado y firma digital

rsa_cert_file=/etc/pki/tls/certs/vsftpd.crt

rsa_private_key_file=/etc/pki/tls/private/vsftpd.key

ssl_ciphers=HIGH

require_ssl_reuse=NO (ver figura 79)

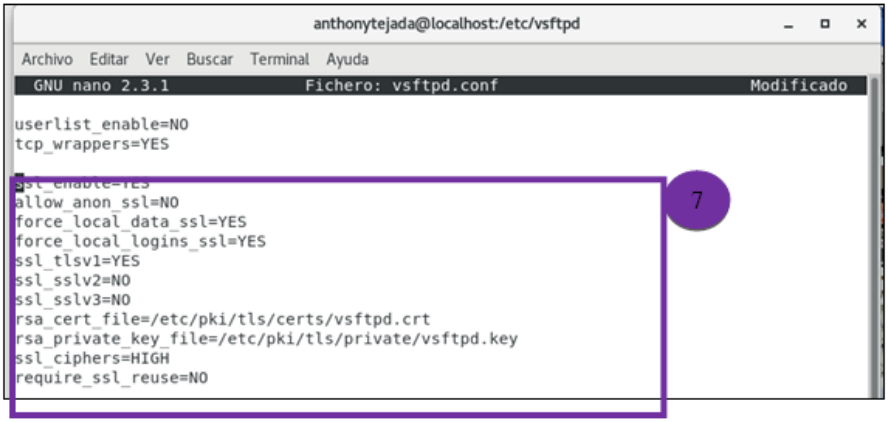


Figura 79. Instalación y Configuración del VSFTPD paso 7

Reinicie el servicio para aplicar los cambios realizados a la configuración, con el comando: *systemctl restart vsftpd* (ver figura 80).

Figura 80. Instalación y Configuración del VSFTPD paso 8

- Se muestra el status del vsftpd con el comando: *systemctl status vsftpd* (ver figura 81).

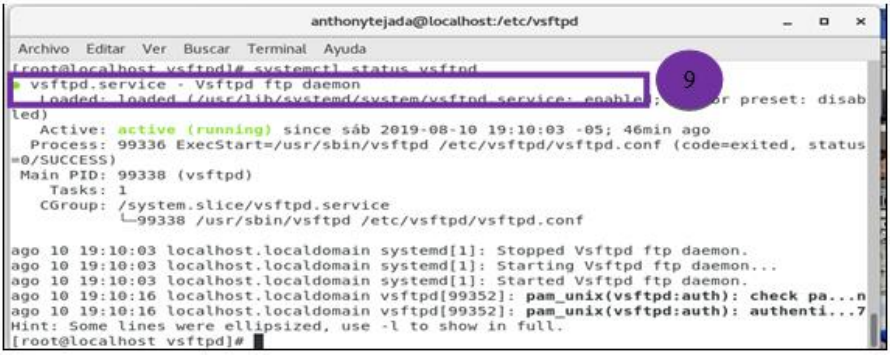


Figura 81. Instalación y Configuración del VSFTPD paso 9

3.2 Acceso por Autenticación con NSCA

3.2.1 Autenticación NSCA

Establecer un sistema de autenticación para acceder a Internet es muy útil, debido a que permite controlar quiénes accederán sin importar desde qué máquina de la red local lo hagan. De este modo se obtiene un control tanto por dirección IP, como por nombre de usuario y contraseña.

NSCA (Nagios Service Check Acceptor) es un módulo que permite efectuar la monitorización pasiva en modo cliente-servidor. El cliente se instala en el recurso y el servidor en el servidor de monitorización. Se ejecuta una tarea de forma regular por el cliente NSCA para efectuar los controles. Durante la detección de una alerta, el cliente NSCA envía la información al servidor de supervisión a través de TCP por el puerto 5667 (por defecto).

3.2.2 Configuración de Acceso por dirección IP

Para controlar el tráfico de los clientes hacia Internet, se pueden aplicar las dos formas. Se trabaja sobre el archivo de configuración localizado en */etc/squid/squid.conf*. Para editar el documento usar: *vi /etc/squid/squid.conf*. Adicionalmente se deben comentar algunas líneas de comandos (presionar la letra “o” hasta que el terminal se ponga en modo INSET), que serán reemplazados por los que se indican a continuación (ver figura 82):

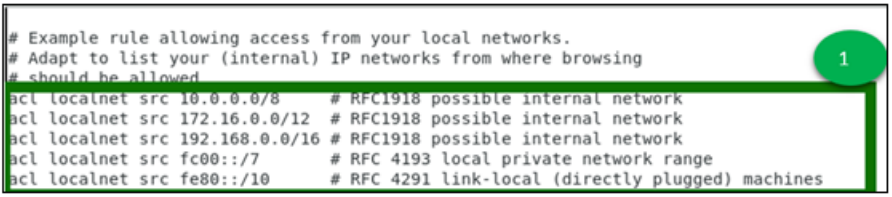


Figura 82. Instalación y Configuración de acceso por dirección IP paso 1

Después de las líneas comentadas, definir la IP correspondiente a la red y la máscara de la sub-red con: *acl localnet src 192.168.1.0/24* (2.1); y darles acceso a todas las redes con: *http_access allow localnet* (2.2) (ver figura 83).

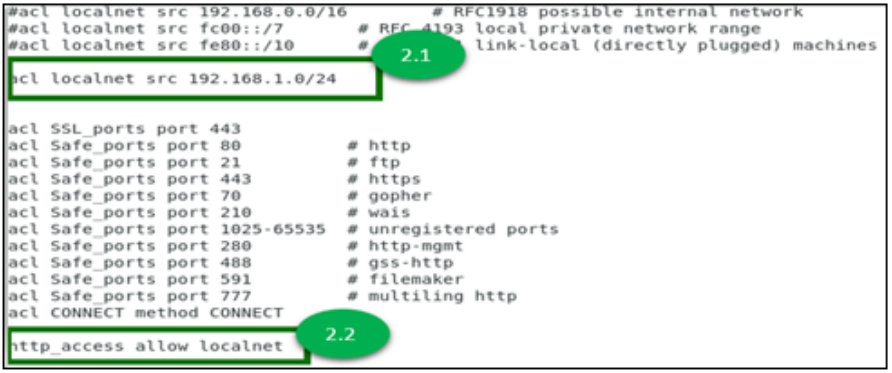


Figura 83. Instalación y Configuración de acceso por dirección IP paso 2

En caso de que el acceso quiera otorgarse a host específicos de la red, se debe definir una Lista de Control de Acceso, el archivo que contendrá las IP de la red permitidas contenido en la ruta */etc/squid/*, con el comando: vi */etc/squid/ip_permitidas* (ver figura 84).

Figura 84. Instalación y Configuración de acceso por dirección IP paso 3

Adicionalmente, se especifica una *acl* dentro del archivo de configuración de Squid, que contiene la lista de direcciones permitidas, se permite el acceso con la regla: *acl ip_permitidas src "/etc/squid/ip_permitidas"*(ver figura 85).

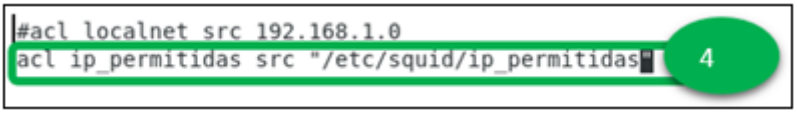


Figura 85. Instalación y Configuración de acceso por direccion IP paso 4

Si lo que se desea es permitir el acceso de un solo cliente: se debe especificar una acl con la dirección IP como muestra la siguiente línea:

5.1*. acl contador src 192.168.1.8/32* (/32 indica que el acceso es para un único cliente).

5.2. *http_access allow* contador (antes de los demás http_access) (ver figura 86).

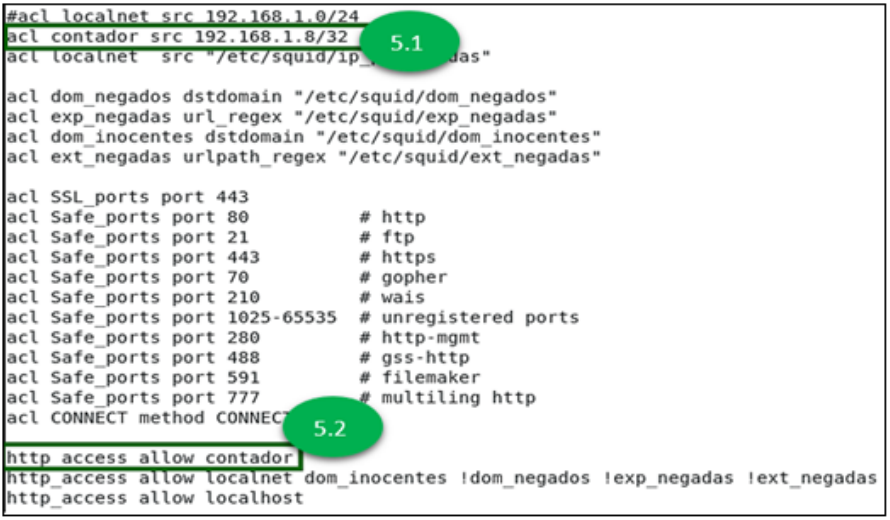


Figura 86. Instalación y Configuración de acceso por dirección IP paso 5

3.2.3 Configuración de Acceso por Autenticación NSCA

Squid puede utilizar el módulo *ncsa_auth*, de la NCSA y que ya viene incluido como parte del paquete principal de Squid en la mayoría de las distribuciones actuales. Este módulo provee una autenticación muy sencilla a través de un archivo de texto simple cuyas contraseñas fueron creadas con *htpasswd*.

Se requerirá la creación previa de un archivo que contendrá los nombres de usuarios y sus correspondientes contraseñas (cifradas). El archivo puede localizarse en cualquier lugar del sistema, para ello se usa el comando: *touch /etc/squid/claves* (ver figura 87).

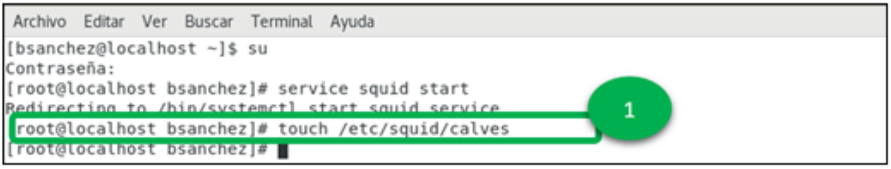


Figura 87. Configuración de Acceso por Autenticación NSCA paso 1

Este archivo debe tener atributos de lectura y escritura solo para el usuario squid, ver en la figura la ejecución de comandos: *chmod 600 /etc/squid/claves y chown squid:squid /etc/squid/claves* (ver figura 88).

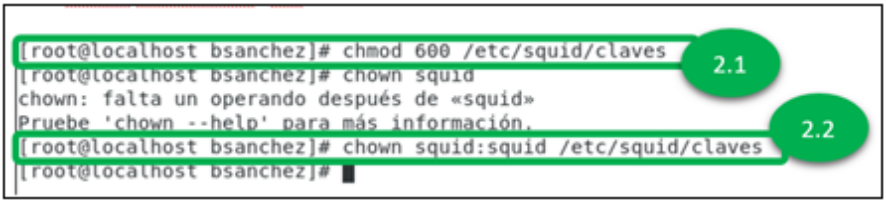


Figura 88. Configuración de Acceso por Autenticación NSCA paso 2

Es necesario dar de alta las cuentas que sean necesarias, utilizando el *htpasswd*, viene incluido en el paquete httpd-2.0.x-. Ejecutar: *htpasswd /etc/squid/claves scastillo* (3.1). Asimismo, se debe definir una contraseña al usuario (3.2) (ver figura 89).

Figura 89. Configuración de Acceso por Autenticación NSCA paso 3

Todas las cuentas que se den de alta de este modo son independientes a las ya existentes en el sistema. Al dar de

alta una cuenta o cambiar una contraseña lo estará haciendo exclusivamente para el acceso al servidor Proxy.

A continuación, se debe editar el archivo */etc/squid/squid.conf*, para agregar la etiqueta *auth_param basic program* (debe ir al inicio del archivo de configuración). De modo predeterminado esta opción viene desactivada y carece de valores, escribir: *auth_param basic program /usr/lib64/squid/ncsa_auth /etc/squid/claves* (ver figura 90).

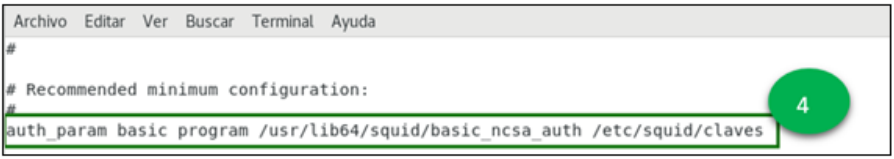


Figura 90. Configuración de Acceso por Autenticación NSCA paso 4

Así también se debe especificar, dentro de este mismo archivo, una lista de control de acceso denominada passwd la cual se configurará para utilizar de modo obligatorio la autenticación para poder acceder a Squid, específicamente en la sección de Listas de Control de Acceso la regla: *acl password proxy_auth REQUIRED* (ver figura 91).

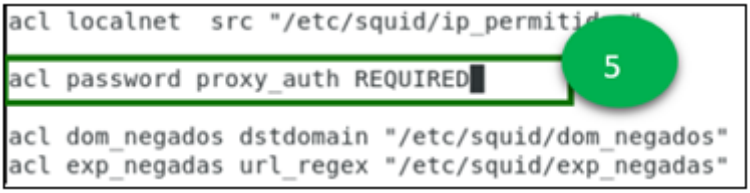


Figura 91. Configuración de Acceso por Autenticación NSCA paso 5

Adicionalmente, debe modificar la regla de control de accesos, para permitir el acceso a Internet mediante el proxy, la regla modifica deberá ser similar a la siguiente línea: *http_access allow localnet password* (ver figura 92).

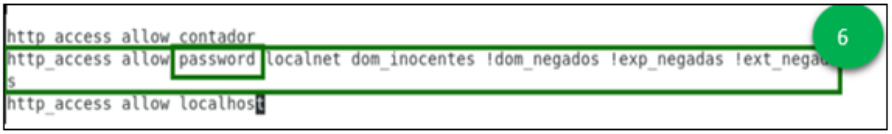


Figura 92. Configuración de Acceso por Autenticación NSCA paso 6

3.2.4 Verificación del acceso por autenticación NSCA

La comprobación de que el servicio se ha establecido correctamente se hace accediendo desde el cliente a Internet. Al intentar acceder se solicitará un usuario y contraseña, usar los datos de cualquiera de los usuarios creados (ver figura 93).

Figura 93. Verificación del acceso por autenticación NSCA

Capítulo 4

CAPÍTULO 4: ADMINISTRACIÓN DE RESTRICCIONES

4.1 Restricción de Acceso a Sitios de Internet

4.1.1 Denegar Acceso

Denegar el acceso a ciertos Sitios de Red permite hacer un uso más racional del ancho de banda con el que dispone la empresa. Su funcionamiento es verdaderamente simple y consiste en denegar el acceso a nombres de dominio o direcciones de Internet que contengan patrones en común.

Se especifican negaciones a dominios, expresiones y extensiones; asimismo, se declaran dominios inocentes. A los mencionados anteriormente se les niega o permite el acceso sobre la base de archivos que contienen listas de aquellos que se desea controlar.

4.1.2 Configuración de Dominios Negados

Crear la lista de dominios a los que se desea restringir acceso, con la siguiente línea: *vi /etc/squid/dom_negados* (ver figura 94).

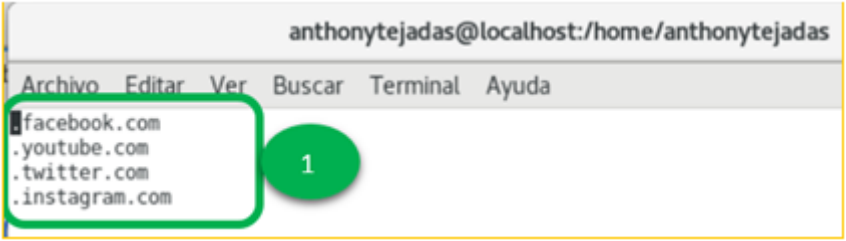


Figura 94. Configuración de Dominios Negados paso 1

Adicionar la acl a acceso: *http_access allow localred !dom_negados* (2.1). Se usa la expresión "!", la cual significa no para bloquear el acceso en la acl: *acl ip_permitidas dstdomain "/etc/squid/dom_negados"* (2.2) (ver figura 95).

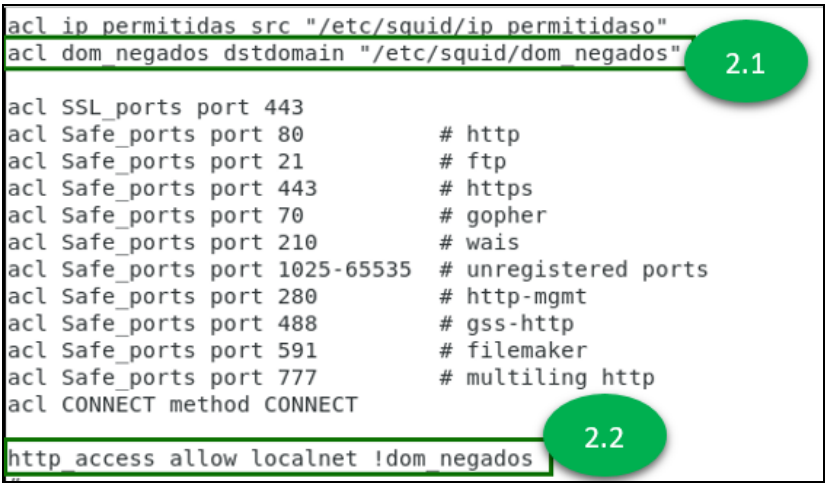


Figura 95. Configuración de Dominios Negados paso 2

4.1.3 Configuración de Expresiones Negadas

Crear la lista de expresiones a los que se desea restringir acceso, con el comando: *vi /etc/squid/exp_negadas* (ver figura 96).

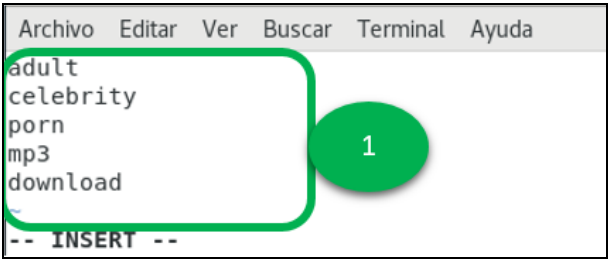


Figura 96. Configuración de Expresiones Negadas paso 1

Se usa la expresión "!", la cual significa no para bloquear el acceso en la acl: *acl exp_negadas url_regex "/etc/squid/exp_negadas"* (2.1) y adicionar la acl de acceso: *http_access allow localred !exp_negadas* (2.2) (ver figura 97).

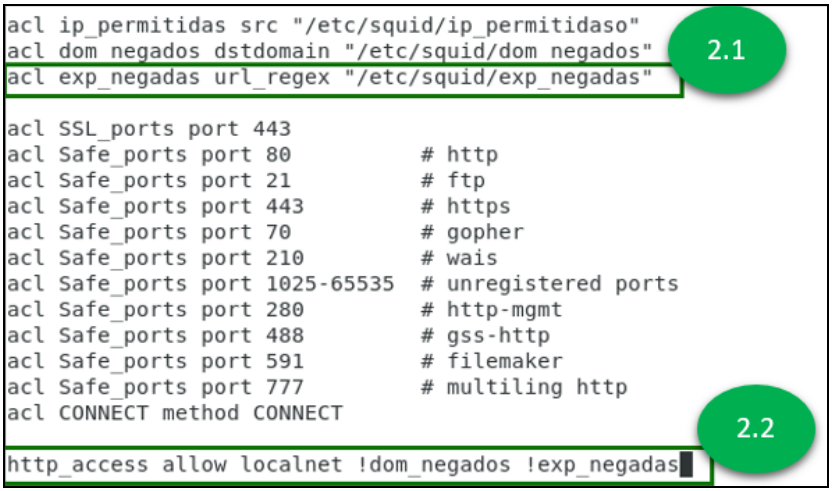


Figura 97. Configuración de Expresiones Negadas paso 2

4.1.4 Configuración de Extensiones Negadas

Crear la lista de dominios a los que se desea permitir acceso, con el comando: *vi /etc/squid/ext_negadas* (ver figura 98).

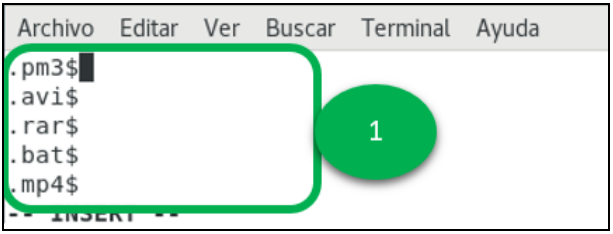


Figura 98. Configuración de Extensiones Negadas paso 1

Para bloquear el acceso a acl: *acl ext_negadas urlpath_regex "/etc/squid/exp_negadas"* (2.1), se usa "!" y adicionar la acl a acceso: *http_access allow localred !ext_negadas* (2.2) (ver figura 99).

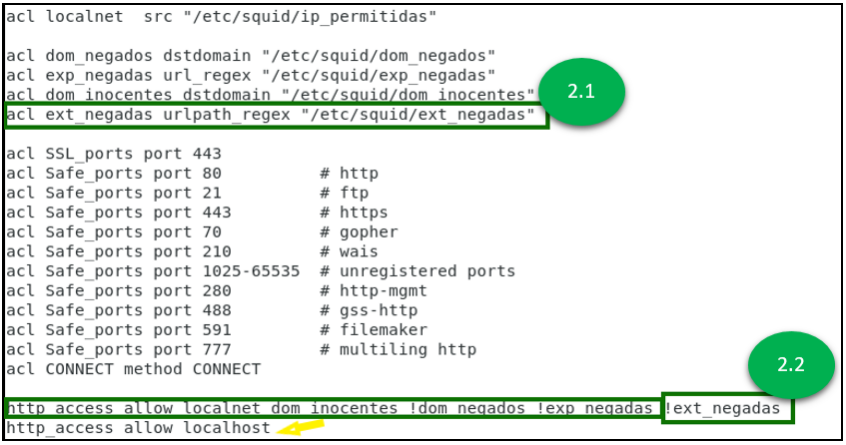


Figura 99. Configuración de Extensiones Negadas paso 2

4.1.5 Configuración de Dominios Inocentes

Crear la lista de dominios a los que se desea permitir acceso, con el siguiente comando: *vi /etc/squid/dom_inocentes* (ver figura 100).

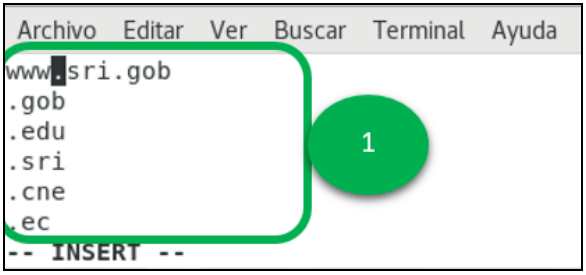


Figura 100. Configuración de Dominios Inocentes paso 1

Para dar acceso a acl: *acl dom_inocentes ddtdomain "/etc/squid/dom_inocentes"* (2.1), se omite "!", y se adiciona la acl a acceso: *http_access allow localred !dom_inocentes* (2.2) (ver figura 101).

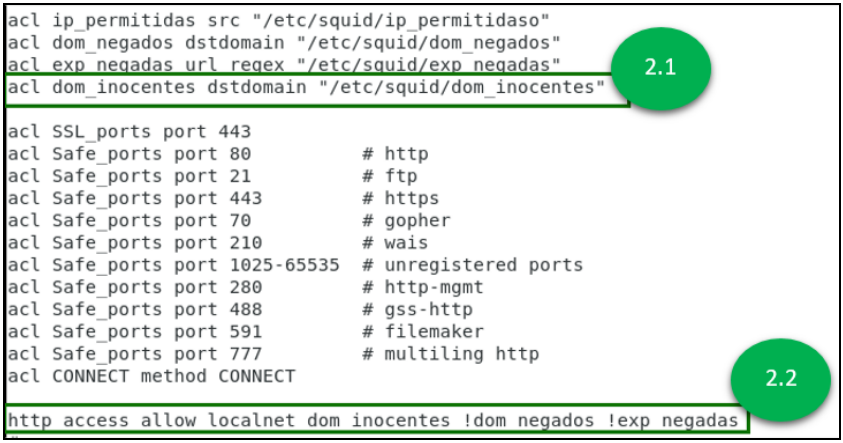


Figura 101. Configuración de Dominios Inocentes paso 2

4.2 Restricción de Acceso por Horarios

Denegar el acceso en ciertos horarios permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple y consiste en denegar el acceso en horarios y días de la semana. Los días de la semana se definen con letras, las cuales corresponden a

la primera letra del nombre en inglés, de modo que se utilizarán:

- S - Domingo
- M - Lunes
- T - Martes
- W - Miércoles
- H - Jueves
- F - Viernes
- A - Sábado

Este tipo de listas se aplican en las Reglas de Control de Acceso con una mecánica similar a la práctica anterior, de negación de expresiones regulares. Esta define una regla que incluye los días de la semana, así como también el horario en que se permite el acceso. Para este caso se define una regla que comprende un horario de 08:00 a 17:00 horas desde el lunes hasta el viernes. Editar el archivo squid.conf ejecutando: *vi /etc/squid/squid.conf* y definir la regla acl que define las condiciones de acceso mencionadas anteriormente: acl semana time MTWHF 08:00-17:00 (ver figura 102).

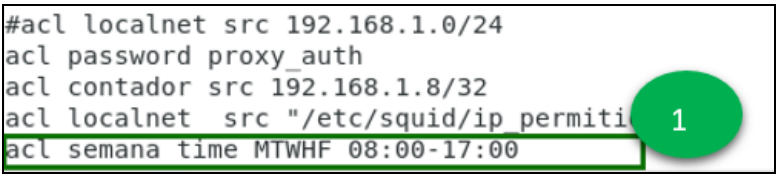


Figura 102. Configuración de Acceso por Horarios paso 1

Establecer que los miembros de la Lista de Control de Acceso denominada localnet tengan permitido acceder hacia Internet en un horario. Como se aprecia a continuación, la regla de

Control de Acceso, ejecutar: *http_access allow* semana *localnet [otras restricciones]* (ver figura 103).

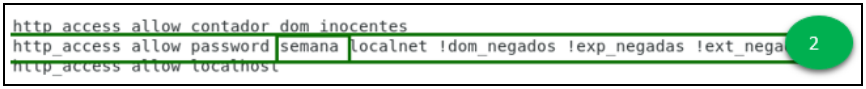


Figura 103. Configuración de Acceso por Horarios paso 2

4.3 Restricción de Acceso por Dirección MAC

En Squid, de modo predeterminado no está incluido el soporte para listas de control de acceso basadas sobre direcciones MAC (Media Access Control). En este se debe configurar la lista de control de acceso con un nombre que la identifique y diferencie claramente de las demás listas, asignado el tipo de lista como arp.

La dirección MAC (media access control) es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red. También se le conoce como dirección física, y es única para cada dispositivo, puesto que son escritas directamente en el hardware en su momento de fabricación. Un ejemplo sería: *38:70:77:1D:51:00*.

4.3.1 Configuración de Control de Acceso por dirección MAC

Para conocer la dirección MAC de un equipo generalmente se emplean las siguientes formas:

- La dirección MAC desde una estación trabajo con Windows se puede obtener mediante el mandato: *ipconfig /all*.
- La dirección MAC desde una estación trabajo con Linux se puede obtener mediante el mandato e *ifconfig*.

Además, se debe tomar en cuenta que para levantar este servicio es necesario que previamente se haya realizado la configuración de Squid. ara activar este servicio, a partir de CentOS 5.6 y Red Hat Enterprise Linux 5.6, el paquete de Squid ya incluye soporte para direcciones MAC. Solo es necesario ejecutar lo siguiente: *yum -y install squid*

Tomando en cuenta lo anterior, se debe crear un archivo que contendrá las direcciones MAC permitidas, se ejecuta la siguiente línea: *vi /etc/squid/mac_redlocal* (ver figura 104).

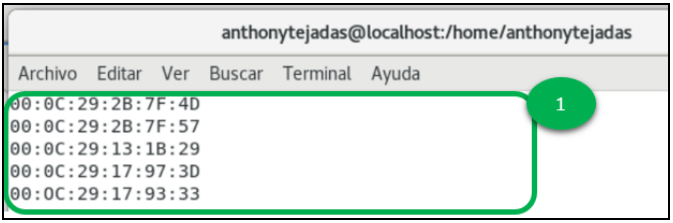


Figura 104. Configuración de Control de Acceso por dirección MAC paso 1

Luego debe modificarse el archivo *squid.conf* con el comando: *vi /etc/squid/squid.conf*, que configura la lista de control de acceso de tipo *arp* y cuyos elementos que la conforman están en ese archivo. Si el archivo que contiene las direcciones MAC se llama mac_redlocal se debe ejecutar: *acl mac_redlocal arp "/etc/squid/mac_redlocal"* (ver figura 105).

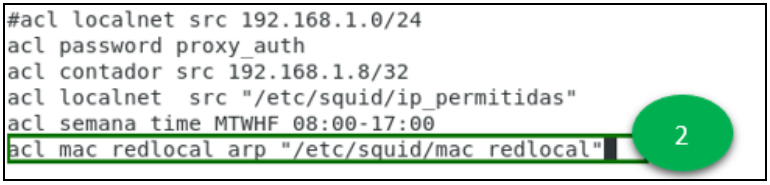


Figura 105. Configuración de Control de Acceso por dirección MAC paso 2

Se crea una regla de control de acceso que permita a los miembros el acceso, la regla de la MAC debe ir antes de las demás, ejecutar: *http_access allow mac_redlocal [otras restricciones]* (ver figura 106).

Figura 106. Configuración de Control de Acceso por dirección MAC paso 3

Para concluir con el levantamiento de este servicio, se deben guardar los cambios y reiniciar el servicio de squid con: *service squid restart*

4.4 Verificación de Restricciones Implementadas

En esta sección se presentan evidencias del correcto funcionamiento de las prácticas implementadas:

En la figura, se muestra el acceso de un cliente (IP) que si consta en la lista permitida (ver figura 107).

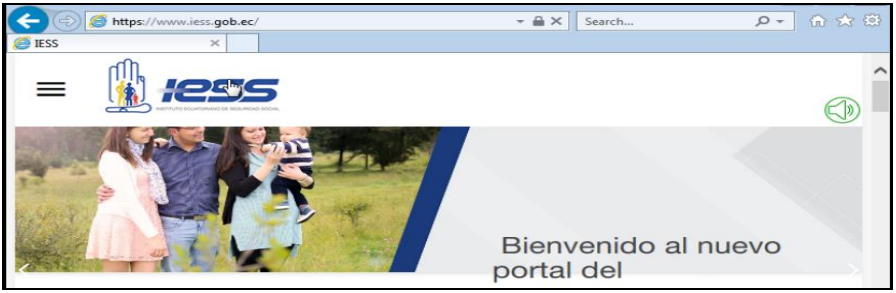


Figura 107. Verificación de Restricciones Implementadas paso 1

Aun cuando la IP conste en la lista, si el dominio, extensiones o expresiones constan con las de los archivos que las

restringen tampoco será posible acceder a dichos sitios (ver figura 108).

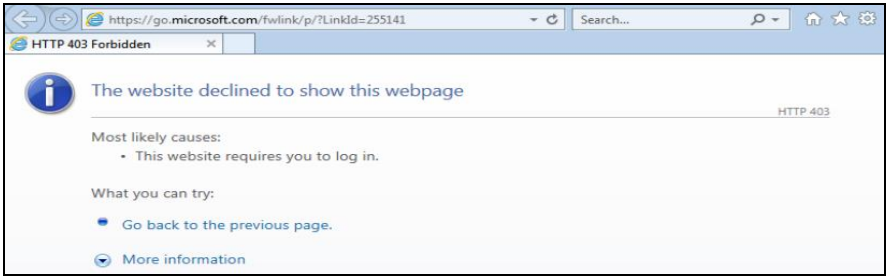


Figura 108. Verificación de Restricciones Implementadas paso 2

Se demuestra que si se accede desde un cliente (IP) que no consta en la lista no puede conectarse a Internet (ver figura 109).

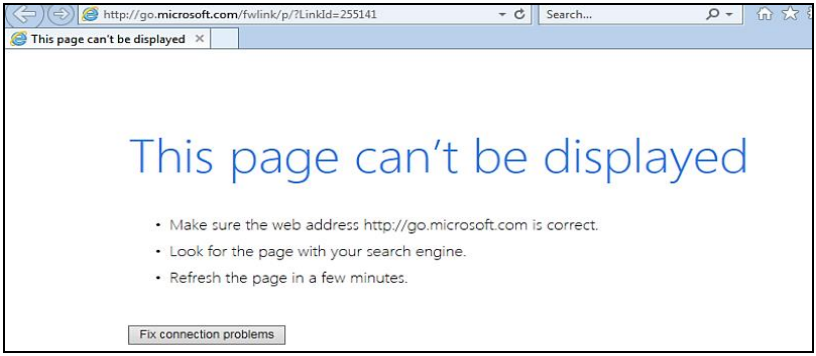


Figura 109. Verificación de Restricciones Implementadas paso 3

Para los dominios negados se hace la comprobación con la página de Facebook (ver figura 110).

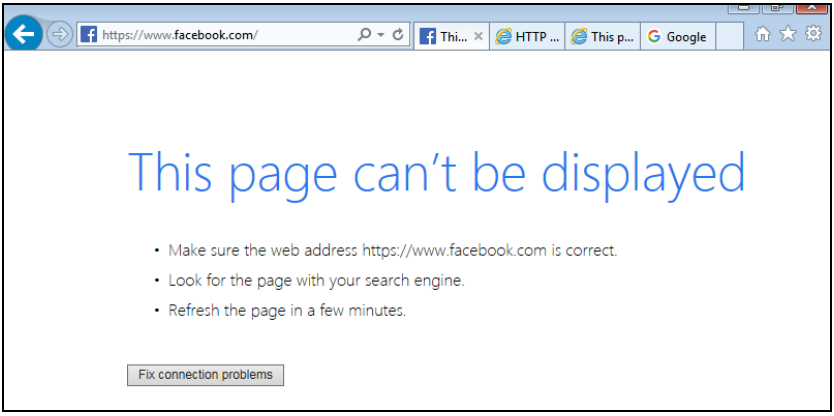


Figura 110. Verificación de Restricciones Implementadas paso 4

4.5 Práctica Cliente. Cliente Telnet

4.5.1 Telnet

Este utiliza el protocolo TCP (Protocolo de Control de Transmisión) con la finalidad de no perder información cuando se tiene una sesión abierta a través de Telnet, también se le han atribuido algunos usos como enviar peticiones a servidores Web entre otras cosas.

Telnet es un protocolo cuya función es interconectar dos dispositivos de redes cualesquiera para obtener una administración o gestión remota. Su publicación fue en el 1983 bajo el RFC854 (*Request for Comments*). Telnet debe tener el puerto 23 abierto para poder funcionar.

4.5.2 Configuración de TELNET. Configuración de la red desde el servidor CentOS

Las máquinas virtuales tanto el servidor CentOS como la máquina cliente deben tener dos adaptadores de red una en NAT que posibilita la conexión a Internet, y otra en puente o Bridge que permite la comunicación con los clientes (ver figura 111).

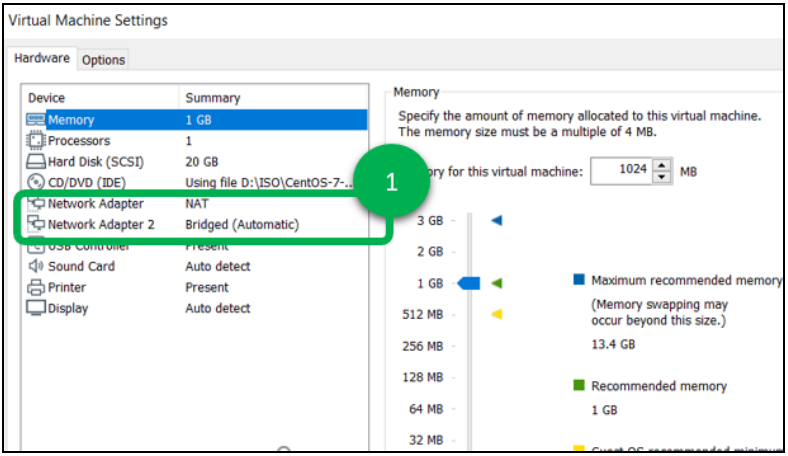


Figura 111. Configuración de la red desde el servidor CentOS paso 1

4.5.3 Acceder a las configuraciones de red

Para este caso es la primera de la lista y acceder a su configuración cableada. Dentro la configuración, seleccionar la pestaña IPv6: Cambiar a Manual el método IPv4 y agregar los campos de dirección IP y la máscara de subred. Aplicar los cambios y salir (ver figura 112).

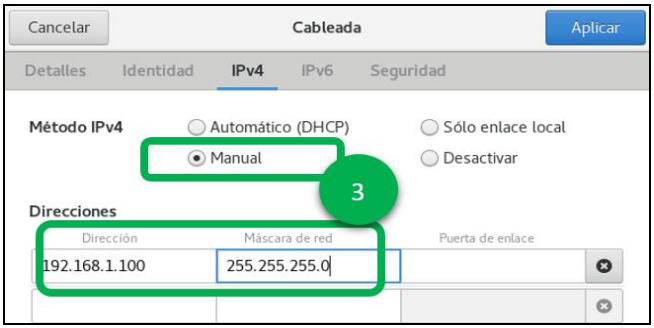


Figura 112. Configuración de la red desde el servidor CentOS paso 2 y 3

Para comprobar que hay acceso a internet hacer ping con la dirección IP: 8.8.8.8. (ver figura 113).

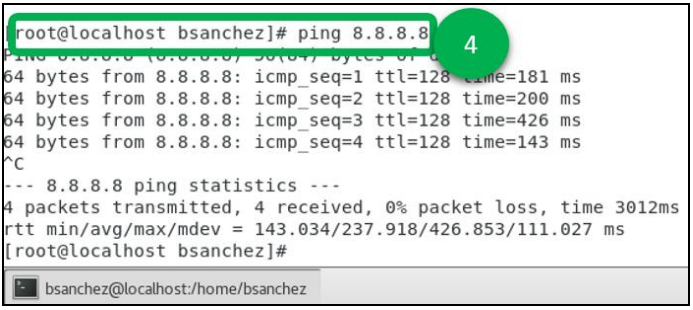


Figura 113. Configuración de la red desde el servidor CentOS paso 4

4.5.4 Activar el Servicio de Telnet desde el cliente

El cliente para efectos de esta práctica será un Windows 7. Para realizar la configuración acceder al panel de control, localizar la opción de “Activar o desactivar las características de Windows”. El sistema solicitará el permiso del administrador en caso de que este tachado a un dominio. Dentro de este menú, seleccionar la opción Cliente Telnet y aceptar, la configuración puede tardar unos minutos (ver figura 114).

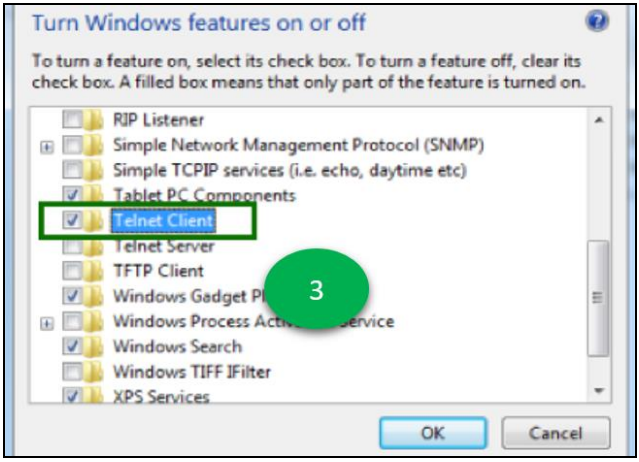


Figura 114. Activar el Servicio de Telnet desde El Cliente.

Se comprueba que se ha establecido la conexión entre el cliente Windows 7 y el CentOS, ejecutando la regla de ping a la dirección IP estática (ens37) desde la ventana del símbolo del sistema (ver figura 115).

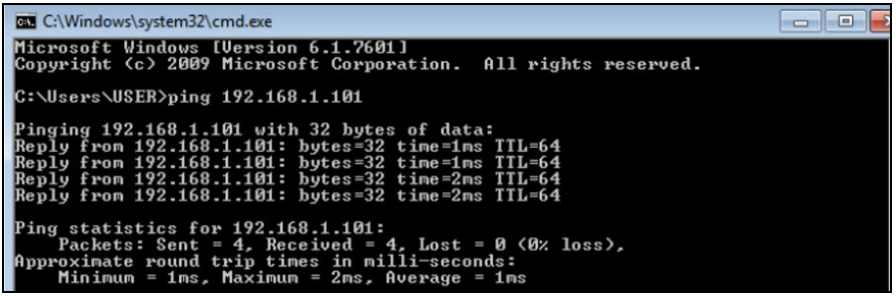


Figura 115. Activar el Servicio de Telnet desde El Cliente comprobación 1

Usar el comando telnet con la dirección IP: 192.168.1.101 y el puerto del squid: 3128 para establecer la comunicación, el comando es el siguiente: *telnet 192.168.73.129 3128*. Si todo está correcto la pantalla de comando se pondrá en negro y solo se verá una línea parpadeando, eso significa que pudimos entrar al server por servicio TELNET (ver figura 116).

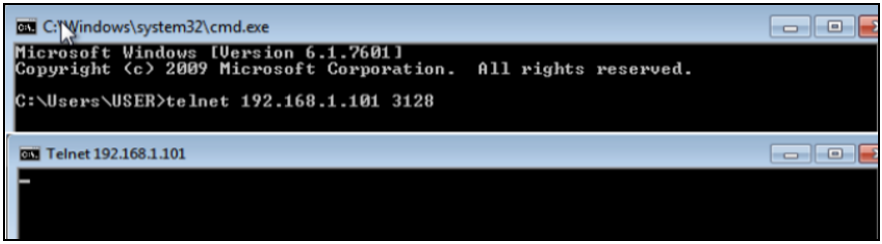


Figura 116. Activar el Servicio de Telnet desde El Cliente. comprobación 2

Capítulo 5

CAPÍTULO 5: VLANS EN GNU/LINUX

5.1 Configurar VLANs en GNU/Linux

VLAN (significado de Virtual LAN o Red en español Área Local Virtual) lo utiliza de un modo en el que nosotros los usuarios podemos crear redes de una manera independiente dentro de una misma red en forma física. Esto es extremadamente útil en entornos de trabajo o en áreas que necesitamos que todos nuestros equipos esten conectados uno al otro, además todo esto se incluye en un único conmutador físico o en una única red física.

Son extremadamente útiles para disminuir el tamaño del dominio de difusión y suportean en la administración de la red, al separar sus segmentos lógicos de una red de área local, lo que impide que puedan intercambiar datos (ver figura 117).

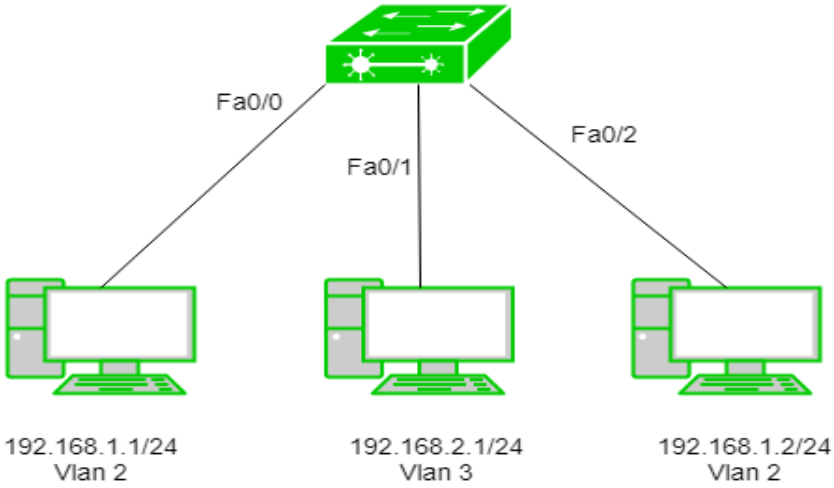


Figura 117. VLANs en GNU/Linux. represetación gráfica

5.1.1 Pasos para relizarlo en CentOS, Fedora y Red Hat Enterprise Linux

Su uso requiere de conmutadores (switches) para los cuales deberán estar previamente configurados para gestionar algunas y entender perfectamente IP versión 4.

El soporte necesario para configurar VLANs se incluye junto con un paquete de nombre *iproute*, el cual se incluye en la instalación, pues se trata de un paquete obligatorio y muy importante para el sistema. De manera alternativa se puede gestionar también las VLANS a través del paquete *vconfig*, ejecutando lo siguiente (Guerrero, 2018): *yum -y install vconfig*

5.1.2 Procedimientos

- Utilizar el siguiente comando en el archivo etc/sysconfig/network: Vim/etc/sysconfig/network
- Añadir el siguiente parámetro para activar el soporte para nuestra red VLAN, el cual permitirá debido a nuestras opciones que luego cargue

automáticamente el módulo de nombre 8021q del núcleo del sistema operativo Linux (Clara, 2018): VLAN=yes.

- Si se asume que se utiliza la interfaz de nombre eth1 para acceder a nuestra red de área local, con el siguiente comando se podrá editar el archivo de configuración nosotros mismos: Vin/etc/sysconfig/network-scripts/ifcfg-eth1
- Para quitar todos los parámetros de red establecidos y dejar el contenido como el de este ejemplo en el cual se asume que la dirección MAC del dispositivo de red corresponde a la siguiente dirección de nombre 44:87:FC:AA:DD:2D (García Castillo, 2010).

DEVICE=eth1

TYPE=Ethernet

BOOTPROTO=none

ONBOOT=yes

HWADDR=44:87:FC:AA:DD:2D

NM_CONTROLED=no

- Para reiniciar el servicio de red para que aplique el cambio y se cargue de una manera automática el módulo 8021q del núcleo de Linux (Barrios, 2016): *service network restart*
- Se pueden crear dispositivos VLAN de manera temporal de esta forma (ver figura 118).

```
ip link add link DISPOSITIVO name DISPOSITIVO.ID-VLAN type vlan id ID-VLAN
ip addr add IP/CIDR brd BROADCAST dev DISPOSITIVO.ID-VLAN
ip link set dev DISPOSITIVO.ID-VLAN up
```

Figura 118

Entonces, podremos observar que ocurre esto (ver figura 119).

```
ip link add link eth1 name eth1.2 type vlan id 2
ip addr add 172.16.0.65/26 brd 172.16.0.127 dev eth1.2
ip link set dev eth1.2 up

ip link add link eth1 name eth1.3 type vlan id 3
ip addr add 172.16.0.129/26 brd 172.16.0.191 dev eth1.3
ip link set dev eth1.3 up

ip link add link eth1 name eth1.4 type vlan id 4
ip addr add 172.16.0.193/26 brd 172.16.0.255 dev eth1.4
ip link set dev eth1.4 up
```

Figura 119

También existe otra forma, utilizando los comandos/mandatos *vonfig* e *ifconfig* así (Guerrero, 2018) (ver figura 120).

```
vconfig add eth1 2
vconfig add eth1 3
vconfig add eth1 4
ifconfig eth1.2 172.16.0.65 netmask 255.255.255.192
ifconfig eth1.3 172.16.0.129 netmask 255.255.255.192
ifconfig eth1.4 172.16.0.193 netmask 255.255.255.192
```

Figura 120

Si fuera necesario eliminar los dispositivos de VLAN, ejecutar el mandato IP de la siguiente manera (ver figura 121).

```
ip link set dev DISPOSITIVO.ID-VLAN down
ip link delete DISPOSITIVO.ID-VLAN
```

Figura 121

Luego saldrá esto (ver figura 122).

```
ip link set dev eth1.2 down
ip link delete eth1.2

ip link set dev eth1.3 down
ip link delete eth1.3

ip link set dev eth1.4 down
ip link delete eth1.4
```

Figura 122

También de manera alternativa a esta se pueden utilizar los comandos *vconfig* con la opción rem, seguido del nombre de nuestro dispositivo VLAN. Ejecutar lo siguiente (Fuentes, 2003) (ver figura 123).

```
vconfig rem eth1.2
vconfig rem eth1.3
vconfig rem eth1.4
```

Figura 123

Si se desea que los dispositivos VLAN estén de manera permanente, crear dentro del directorio en la ruta */etc/sysconfig/network-scripts* (ver figura 124)

```
icfg-DISPOSITIVO.ID-VLAN
```

Figura 124

El número de VLAN preferiblemente debe corresponder a los mismos que los del conmutador principal. Se debe evitar usar la VLAN 1 (eth.1.1 o eth 1.1), 172.16.0.1 como IP en el servidor así como también, la red 172.16.0.0/26, porque suelen corresponder al número de VLAN, dirección IP y segmento de red que regularmente utilizan los conmutadores (León, 2018). Ejemplo de contenido de */etc/sysconfig/network-scripts/ifcfg-eth1.2.* (ver figura 125)

```
DEVICE=eth1.2
TYPE=Ethernet
BOOTPROTO=static
ONBOOT=yes
NM_CONTROLED=no
IPADDR=172.16.0.65
PREFIX=26
BROADCAST=172.16.0.127
NETWORK=172.16.0.64
```

Figura 125

Reiniciar el servicio de red para que puedan iniciarse las interfaces de VLAN con service network restart

Se puede verificar que todos las VLAN estén presentes con el comando ip addr show.

Debe salir lo siguiente (ver figura 126)

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet 127.0.0.2/8 brd 127.255.255.255 scope host secondary lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 44:87:FC:AA:DD:2D brd ff:ff:ff:ff:ff:ff
3: eth1.2@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 44:87:FC:AA:DD:2D brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.65/26 brd 172.16.0.127 scope global eth1.2
    inet6 fe80::a00:27ff:fece:5172/64 scope link
       valid_lft forever preferred_lft forever
4: eth1.3@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 44:87:FC:AA:DD:2D brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.129/26 brd 172.16.0.191 scope global eth1.3
    inet6 fe80::a00:27ff:fece:5172/64 scope link
       valid_lft forever preferred_lft forever
5: eth1.4@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 44:87:FC:AA:DD:2D brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.193/26 brd 172.16.0.255 scope global eth1.4
    inet6 fe80::a00:27ff:fece:5172/64 scope link
       valid_lft forever preferred_lft forever
```

Figura 126

De manera alternativa, con el método ifconfig se podrá ver que todas las VLAN estén presentes (Cruz, Mora, Sauza, Pérez y Cruz, 2016) (ver figuras 127 y 128).

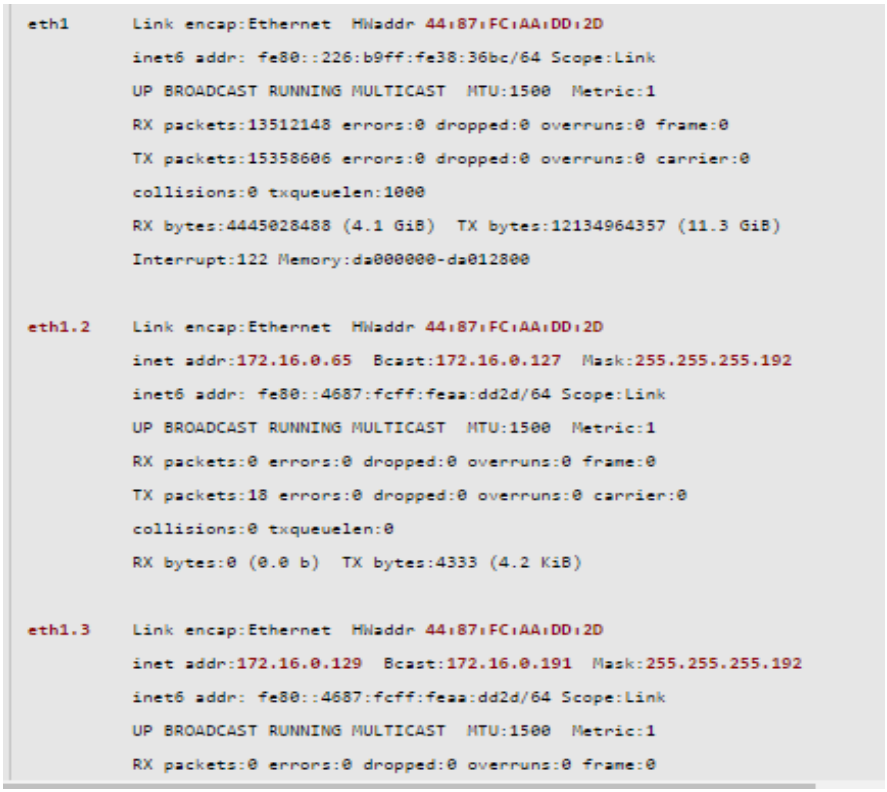

eth1 Link encap:Ethernet HWaddr 44:87:FC:AA:DD:2D
inet6 addr: fe80::226:b9ff:fe38:36bc/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:13512148 errors:0 dropped:0 overruns:0 frame:0
TX packets:15358606 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4445028488 (4.1 GiB) TX bytes:12134964357 (11.3 GiB)
Interrupt:122 Memory:da000000-da012800
eth1.2 Link encap:Ethernet HWaddr 44:87:FC:AA:DD:2D
inet addr:172.16.0.65 Bcast:172.16.0.127 Mask:255.255.255.192
inet6 addr: fe80::4687:fcff:feaa:dd2d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:4333 (4.2 KiB)
eth1.3 Link encap:Ethernet HWaddr 44:87:FC:AA:DD:2D
inet addr:172.16.0.129 Bcast:172.16.0.191 Mask:255.255.255.192
inet6 addr: fe80::4687:fcff:feaa:dd2d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0

Figura 127

```
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:4235 (4.1 KiB)

eth1.4    Link encap:Ethernet  HWaddr 44:87:FC:AA:DD:2D
          inet addr:172.16.0.193  Bcast:172.16.0.255  Mask:255.255.255.192
          inet6 addr: fe80::4687:fcff:feaa:dd2d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:3405 (3.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:183 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21398 (20.8 KiB)  TX bytes:21398 (20.8 KiB)
```

Figura 128

También es posible utilizar el servicio de DHCP para que se pueda gestionar la administración de direcciones a través de algún servidor DHCP. Se edita el archivo */etc/sysconfig/dhcpd* y definen las interfaces de VLAN junto con el servidor DHCP (ver figura 129).

```
DHCPDARGS="eth1.2 eth1.3 eth1.4";
```

Figura 129

Editar el archivo */etc/dhcpd.conf* (CentOS 5 y Red Hat Enterprise Linux 5) o bien */etc/dhcp/dhcpd.conf* (CentOS 6 y

Red Hat Enterprise Linux 6), y definir una sección por cada red (Capella, 2012) (ver figura 130).

```
ddns-update-style interim;
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option ip-forwarding off;
option domain-name "red-local.net";
option ntp-servers 200.23.51.205, 132.248.81.29, 148.234.7.30;

shared-network vlan2 {
        subnet 172.16.0.64 netmask 255.255.255.192 {
                option routers 172.16.0.65;
                option subnet-mask 255.255.255.192;
                option broadcast-address 172.16.0.127;
                option domain-name-servers 172.16.0.65;
                option netbios-name-servers 172.16.0.65;
                range 172.16.0.66 172.16.0.126;
        }
}
shared-network vlan3 {
        subnet 172.16.0.128 netmask 255.255.255.192 {
                option routers 172.16.0.129;
```

Figura 130

```
        }
}
shared-network vlan3 {
        subnet 172.16.0.128 netmask 255.255.255.192 {
                option routers 172.16.0.129;
                option subnet-mask 255.255.255.192;
                option broadcast-address 172.16.0.191;
                option domain-name-servers 172.16.0.192;
                option netbios-name-servers 172.16.0.192;
                range 172.16.0.130 172.16.0.190;
        }
}
shared-network vlan4 {
        subnet 172.16.0.192 netmask 255.255.255.192 {
                option routers 172.16.0.193;
                option subnet-mask 255.255.255.192;
                option broadcast-address 172.16.0.255;
                option domain-name-servers 172.16.0.193;
                option netbios-name-servers 172.16.0.193;
                range 172.16.0.194 172.16.0.254;
        }
}
```

Figura 131

Reiniciar el método dhcpd y comprobar que funcione correctamente el servicio, conectando algunos equipos a los conmutadores involucrados: *service dhcpd restart* (ver figura 131)

5.2 La ingeniería social y los malos hábitos de los usuarios

La mejor tecnología moderna y todos los fondos destinados para la seguridad de nuestras cuentas y equipos de trabajos es absolutamente inservible cuando un usuario no es capaz de mantener una clave de acceso o información de manera confidencial. Por tal motivo, es que tiene muchísima relevancia el impulsar la concienciación de los usuarios acerca de los peligros que otros usuarios puedan realizar con la

ingeniería social y vulnerar la Seguridad Informática de nuestro hogar o área de trabajo.

Clásicos ejemplos de ataques mediante la ingeniería social es el envío de los archivos, fotos o documentos adjuntos en el correo electrónico (mundialmente conocidos estas malicias como virus, troyanos y gusanos) que pueden ejecutarse de forma maliciosa en el trabajo o computadora personal (López, 2013).

Otro tipo de ataque muy usual es dentro del marco de la ingeniería social, e increíblemente el más fácil de realizar, consiste en estafar a un usuario al hacerle pensar que se trata de un administrador de la red donde sel trabaja o reside que solicita claves de acceso u otro tipo de información confidencial.

Buena parte del correo electrónico que llega al buzón del usuario consiste en engaños, solicitan claves de acceso, números de tarjeta de crédito o débito y otra información. Este tipo de ataque se conoce actualmente como phising (pesca). Lamentablemente muchos estudios muestran que los usuarios tienen una muy mala percepción acerca de la importancia de la seguridad en nuestra época.

Un tipo de ingeniería social muy efectiva es incluir inmensas cantidades de texto a un acuerdo de licencia que se encuentra en muchos lados, por ejemplo: cuando queremos instalar un programa, o registrarnos en una página web, descargar algún archivo etc. La gran mayoría de los usuarios, incluidos administradores, rara vez leen una palabra contenida en dicho texto y simplemente dan clic en aceptar en los contratos de licenciamientos y acuerdos (Sierra, 2017).

La principal defensa contra la ingeniería social es la educación del usuario, empezando por los propios administradores de

redes. La mejor forma de combatir la ingeniería social es la prevención de nuestra información.

5.2.1 Recomendaciones para evitar ser víctimas de la ingeniería social a través del correo electrónico:

1. Desconfiar de ofertas y promociones que encontremos en redes sociales. Para poder tener un punto de vista positivo de alguna promoción o compra debe visitarse la página web oficial de la empresa en cuestión y comprobar si tienen algún descuento o promoción en marcha. Si no se ve la oferta en el perfil oficial es que no existe. De esta manera con unos simples pasos se puede evadir una estafa.
2. No utilizar o ingresar cuentas de correo electrónico personal para asuntos laborales.
3. No utilizar o ingresar cuentas de correo electrónico para uso laboral en asuntos personales.
4. Decir a los usuarios para qué jamás debemos publicar cuentas de correo en áreas públicas que permitan sean encontradas por software para este fin.
5. Concienciar al usuario para no publicar cuentas de correo electrónico en lugares públicos.
6. Concienciar al usuario a utilizar claves más complejas.
7. Concienciar al usuario a no abrir y clickear a todo lo que llegue por correo.
8. Concienciar al usuario para jamás responder a un mensaje de spam.

5.2.2 Cómo instalar y configurar el programa Vacation para responder avisos automáticos en vacaciones

Vacation cuyo nombre real es (Vacation Mail Responder) es un ligero y extremadamente útil programa que permite configurar cuentas de correo electrónico para que respondan automáticamente con un mensaje e indican que el usuario se encuentra de vacaciones. Es el programa automático de respuesta de correo que se encuentra en muchos sistemas Unix, muy ideal si somos un usuario con un puesto alto en una empresa o somos administradores de un área en cuestión y debemos siempre estar al tanto de nuestros correos electrónicos.

5.2.3 Instalación a través de yum

Si se utiliza CentOS o Red Hat™ Enterprise Linux, primero configurar el almacén YUM. En este ejemplo se usará el de Alcance Libre (ver figura 132).

```
cd /etc/yum.repos.d/
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo
cd -
```

Figura 132

Para instalar el paquete, ejecutar: *yum -y install vacation*

5.2.4 Vacation y SELinux

SELinux impedirá que Sendmail pueda ejecutar el programa vacation. El siguiente procedimiento, crear una norma que permitirá a vacation operar normalmente.

Crear el directorio */usr/share/selinux/packages/vacation* (Soler, 2017): *mkdir/usr/share/selinux/packges/vacation*

Cambiar el directorio */usr/share/selinux/packages/vacation: cd/usr/share/selinux/packages/vacation*

Editar el archivo vacation.te: *vi vacation.te*

Verificamos que el archivo vacation tenga el siguiente contenido (ver figura 133):

```
module vacation 1.0;

require {
        type sendmail_t;
        type etc_runtime_t;
        class file { execute };
}

#============= sendmail_t ==============
allow sendmail_t etc_runtime_t:file execute;
```

Figura 133

Crear el archivo de módulo vacation.mod a partir del archivo vacation.te: *checkmodule -M -m -o vacation.mod vacation.te*

Crear el archivo de política vacation.pp a partir del archivo vacation.mod: *semodule_package -0 vacation.pp -m vacation.mod*

Incluir la política al sistema: *semodule -i /usr/share/selinux/packages/vacation/vacation.pp*

Regresar al directorio de inicio de root con el método cd

5.2.5 Proceso Sendmail en programa Vacation

Si se desea que Sendmail permita utilizar el programa Vacation, es necesario crear primero un enlace dentro del directorio */etc/smrsh* y este que apunte hacia */usr/bin/vacation.* Ejecutar lo siguiente: *ln -s /usr/bin/vacation /etc/smrsh/vacation*

Es indispensable que el usuario a utilizar tenga acceso al intérprete de mandatos, dicho de otra manera, ser

administrador, de otro modo será imposible utilizar el programa vacation. Asignar al usuario */bin/bash* como intérprete de mandatos o bien */bin/sh* ejecutar lo siguiente (Soler, 2017): *usermod -s /bin/bash usuario*

Cambiar a la sesión del usuario: *su -l usuario*

Utilizar vi para crear el archivo *~/.vacation.msg: vi ~/.vacation.msg*

Colocar dentro del archivo un contenido similar al siguiente, evitar tildes, la letra ñ y cualquier otro carácter distinto a los de la tabla ASCII debido a la nomenclatura americana (ver figura 134):

```
Subject: Estoy de vacaciones.
From: como se llame <usuario@mi-dominio.com.mx>
Reply-To: como se llame <usuario@mi-dominio.com.mx>
Buen dia, por el momento no me encuentro en la oficina, estoy de regreso el
proximo DD de MMMM de AAAA.

Reciba un cordial saludo.

Atentamente
Lic. como se llame

NOTA: Mensaje *intencionalmente* enviado sin acentos.
```

Figura 134

Pulsar la tecla Esc, guardar cambios y salir de vi pulsando la combinación de teclas :wq y luego la tecla ⏎ (ENTER).

Utilizar vi para crear el archivo *~/.forward: vi ~/.forward*

Pulsar la tecla Insert.

Añadir el siguiente contenido, tomando en cuenta que la omisión de la barra invertida (\) al inicio hará que el programa vacation falle irremediablemente: \usuario, *"|/usr/bin/vacation usuario"*

Pulsar la tecla Esc, guardar cambios y salir de vi pulsando la combinación de teclas: wq y luego la tecla ⏎ (ENTER).

Cambiar los permisos del archivo para que solo permitan la lectura y escritura al usuario propietario: *chmod 600 ~/.forward*

Como usuario ejecutar el siguiente mandato, a fin de iniciar el programa: *vacation -I*

Salir de la sesión de usuario con el método *exit*

A partir de este momento, todo el correo electrónico que se envíe a la cuenta del usuario será respondido automáticamente con un mensaje que incluirá el texto definido en el archivo, absolutamente todo lo escrito estará ahí. */home/usuario/.vacation.msg. Mv /home/usuario/.forward /home/usuario/.forward.old*

Definir nuevamente */dev/null, /bin/false o /sbin/nologin* como intérprete de comandos para el usuario: *usedrmod -s /dev/null usuario* (ver figura 135).

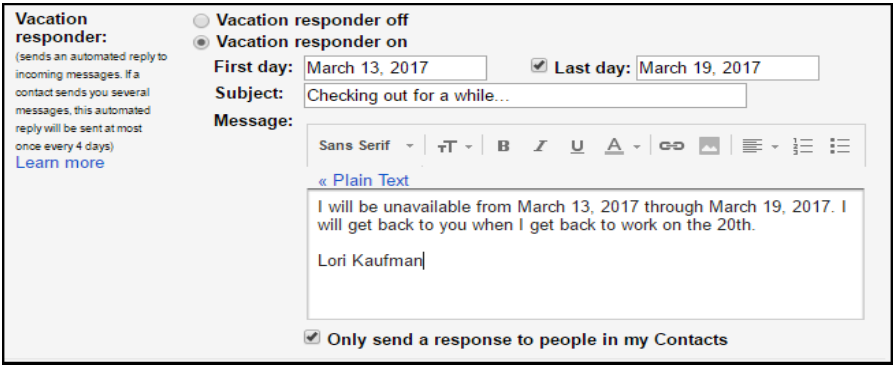


Figura 135. Proceso Sendmail en programa Vacation

Capítulo 6

CAPÍTULO 6: QUAGGA EN CENTOS 7

6.1 Configuración de Quagga en Centos 7: Ruteo estático, RIP y OSPF

Esta es una buena forma de convertir un servidor Linux en un router con todas las bondades que ofrecen las herramientas Open Source.

6.1.1 Instalación de Quagga sobre -CENTOS7

Instalar el paquete de quagga ejecutando: *# yum –y install quagga* (ver figura 136)

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[andres@localhost ~]$ su
Contraseña:
'abrt-cli status' timed out
[root@localhost andres]# clear
[root@localhost andres]# yum install quagga
Complementos cargados:fastestmirror, langpacks
Determining fastest mirrors
 * base: mirror.cedia.org.ec
 * extras: mirror.ufscar.br
 * updates: centosd6.centos.org
(1/2): base/7/x86_64/primary_db                          | 5.9 MB   00:01
(2/2): updates/7/x86_64/primary_db                       | 4.3 MB   00:03
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete quagga.x86_64 0:0.99.22.4-5.el7_4 debe ser instalado
--> Procesando dependencias: net-snmp para el paquete: quagga-0.99.22.4-5.el7_4.
x86_64
--> Procesando dependencias: libnetsnmpmibs.so.31()(64bit) para el paquete: quag
ga-0.99.22.4-5.el7_4.x86_64
--> Procesando dependencias: libnetsnmpagent.so.31()(64bit) para el paquete: qua
gga-0.99.22.4-5.el7_4.x86_64
--> Ejecutando prueba de transacción
---> Paquete net-snmp.x86_64 1:5.7.2-33.el7_5.2 debe ser instalado
--> Procesando dependencias: net-snmp-libs = 1:5.7.2-33.el7_5.2 para el paquete:
```

Figura 136. Instalación de Quagga sobre -CENTOS7 paso 1

En CentOS 7, SELinux evita que */usr/sbin/zebra* escriba de manera predeterminada en su directorio de configuración. Esta política SELinux interfiere con el procedimiento de configuración que se va a describir, por lo que queremos deshabilitar esta política. Para eso, apague SELinux (que no se recomienda) o habilite el booleano *'zebra_write_config'* de la siguiente manera. Omita este paso si está usando CentOS 6 (ver figura 137).

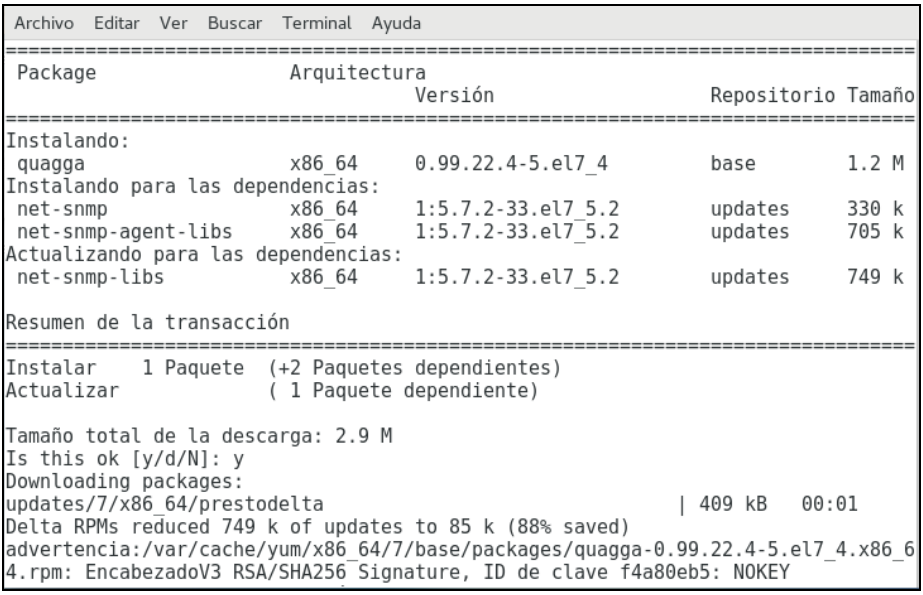


Figura 137. Instalación de Quagga sobre -CENTOS7 paso 2

Debido a la seguridad de SELinux debe activarse la siguiente política: *# setsebool -P zebra_write_config 1*

Sin este cambio, viene el siguiente error al intentar guardar la configuración de Zebra desde dentro del shell de comandos de Quagga: Can't open configuration file */etc/quagga/zebra.conf.OS1Uu5*.

Después de instalar Quagga, configurar las direcciones IP de peering necesarias y actualizar la configuración de OSPF. Quagga viene con un shell de línea de comandos llamado vtysh. Los comandos de Quagga utilizados dentro de vtysh son similares a los de los principales proveedores de enrutadores como Cisco o Juniper.

6.2 Configuración de Zebra

Una vez instalados dos servidores Linux Centos o más, lo siguiente es haber instalado zebra, para lo cual es necesario configurar, y mantener el esquema mostrado para su correcta configuración en red (ver figura 138).

6.2.1 Esquema 0

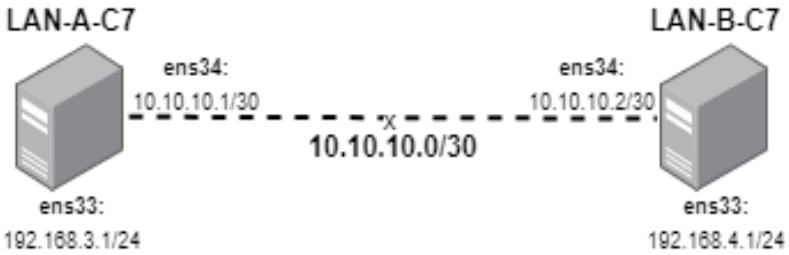


Figura 138. Esquema 0

6.2.2 Proceso de Configurar Zebra:

Crea un archivo de configuración de Zebra (verificar versión), comúnmente se copia el archivo *zebra.conf.sample* con el nombre de *zebra.conf* en las rutas especificadas (ver figura 139).

#cp /usr/share/doc/quagga-XXXXX/zebra.conf.sample /etc/quagga/zebra.conf

#service zebra start

#chkconfig zebra on

```
[root@localhost andres]# service zebra start
Redirecting to /bin/systemctl start zebra.service
[root@localhost andres]# chkconfig zebra on
Nota: Reenviando petición a 'systemctl enable zebra.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/zebra.service to /usr/lib/systemd/system/zebra.
service.
[root@localhost andres]# vtysh

Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

localhost.localdomain# configure terminal
localhost.localdomain(config)# log file /var/log/quagga/quagga.log
localhost.localdomain(config)# exit
localhost.localdomain# write
Building Configuration...
Configuration saved to /etc/quagga/zebra.conf
[OK]
localhost.localdomain# show interface
Interface enp0s3 is up, line protocol detection is disabled
  index 2 metric 1 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 08:00:27:9e:d5:db
  inet 10.0.2.15/24 broadcast 10.0.2.255
  inet6 fe80::ce58:7ca1:d3a2:a38/64
Interface enp0s8 is up, line protocol detection is disabled
  index 3 metric 1 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 08:00:27:b9:06:ee
  inet 10.0.3.15/24 broadcast 10.0.3.255
  inet6 fe80::b1fd:1dca:bc9d:ba2/64
Interface lo is up, line protocol detection is disabled
  index 1 metric 1 mtu 65536
  flags: <UP,LOOPBACK,RUNNING>
  inet 127.0.0.1/8
```

Figura 139. Proceso de Configurar Zebra paso 1

Luego ejecutar el comando: *# vtysh*.

Para entrar en la Shell de la terminal como se muestra en la figura 140:

```
[root@localhost lana]# vtysh

Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

localhost.localdomain# configure terminal
```

Figura 140. Proceso de Configurar Zebra paso 2

Note que el prompt cambió, de *root@localhost lana]# a localhost.localdomaind#* A partir de aquí se puede cambiar el nombre del host, con el comando *hostname site-A-RTR*, lo que hará es cambiar el nombre del servidor inmediatamente, ejemplo: *site-A-RTR* (ver figura 141):

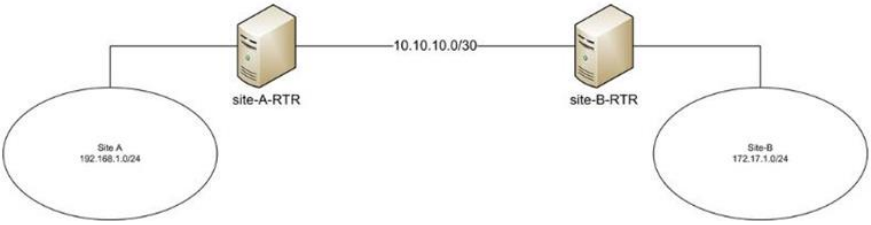


Figura 141. Cambiar el nombre del host

A partir de este momento se puede configurar el router desde comandos. Para ello se necesita entrar en modo de configuración global ejecutando: *site-A-RTR#configure terminal*

Y especificar la ubicación del archivo de registro, luego salga del modo: *site-A-RTR(config)# log file /var/log/quagga/quagga.log y site-A-RTR(config)# exit*

Guardar la configuración permanentemente: *site-A-RTR# write*

A continuación, identificar las interfaces disponibles y configurar sus direcciones IP según sea necesario: *site-A-RTR# show interface*

Configurar los parámetros de enp0s3:

site-A-RTR# configure terminal

site-A-RTR(config)# interface enps03

site-A-RTR(config-if)# ip address 10.10.10.1/30

site-A-RTR(config-if)# description to-site-B

site-A-RTR(config-if)# no shutdown

Configurar los parámetros de enps08:

site-A-RTR(config)# interface enps08

site-A-RTR(config-if)# ip address 192.168.1.1/24

site-A-RTR(config-if)# description to-site-A-LAN

site-A-RTR(config-if)# no shutdown

Verificar la configuración: *site-A-RTR(config-if)# do show interface*

Interface enps03 is up, line protocol detection is disabled: *inet 10.10.10.1/30 broadcast 10.10.10.3*

Interface enps08 is up, line protocol detection is disabled: *inet 192.168.1.1/24 broadcast 192.168.1.255 y site-A-RTR(config-if)# do show interface description*

Guardar la configuración permanentemente y salir del modo de configuración de interfaz:

site-A-RTR(config-if)# do write

site-A-RTR(config-if)# exit

site-A-RTR(config)# exit site-A-RTR#

Salir del Shell vtysh para regresar al de centos: site-A-RTR# exit

A continuación, habilitar el reenvío de IP para que el tráfico se pueda reenviar entre las interfaces enps03 y enps08: *# echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf y # sysctl -p /etc/sysctl.conf*

Repetir la configuración de la dirección IP y el reenvío de IP, lo que también permite pasos en el servidor del sitio B.

Si todo va bien, debería poder hacer ping a la IP 10.10.10.2 de peering del sitio B desde el servidor del sitio A.

Tenga en cuenta que una vez que Zebra Daemon ha comenzado, cualquier cambio realizado con la interfaz de línea de comandos de *vtysh* surte efecto inmediatamente. No

es necesario reiniciar Zebra daemon después del cambio de configuración.

6.2.3 Otro ejemplo con direcciones de clase C

A continuación, verificar las interfaces de red disponibles para luego configurarlas según sea necesario, ejecutar: show interface

Para asignar las direcciones ip correspondientes a la primera interfaz -ens33- se realiza lo siguiente:

configure terminal

interface ens33

ip address 192.168.3.1/24

description in-lan-A

no shutdown

En la segunda interfaz-ens34- de igual manera se asigna la ip necesaria:

configure terminal

interface ens34

ip address 10.10.10.1/30

description out-lan-A

no shutdown

Verificar la configuración ejecutando: do show interface (ver figura 142)

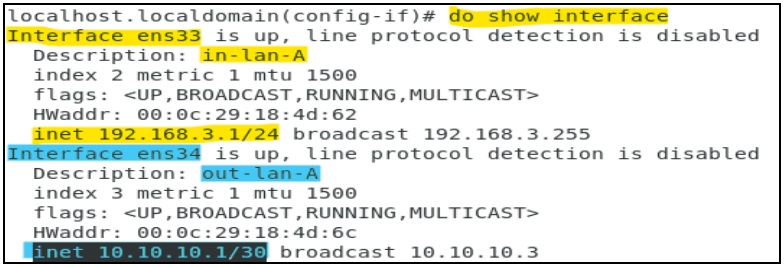


Figura 142. Ejecución do show interface

Guardar la configuración de forma permanente y salimos hasta la shell de Linux:

do write

exit

exit

exit

El prompt volverá a cambiar (ver figura 143):

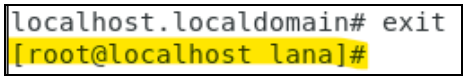


Figura 143. Cambio prompt

Por último, se habilita el reenvío de IP para que el tráfico se pueda reenviar entre las interfaces configuradas, ejecutar:

echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf

sysctl -p /etc/sysctl.conf

6.2.4 Pruebas de ping entre servidores

Se realizan las mismas configuraciones entre los dos servidores de Centos 7, teniendo en consideración que las direcciones IP cambian de acuerdo con el esquema planteado. Una vez que se haya terminado la instalación y configuración en los dos servidores se pueden realizar las

pruebas de ping para verificar la conexión entre los mismos, como se muestra a continuación (ver figuras 144 y 145):

```
[root@localhost lana]# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=0.447 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.425 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.915 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=64 time=0.983 ms
^C
--- 10.10.10.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.425/0.692/0.983/0.259 ms
```

Figura 144. C7-LAN-A (10.10.10.1)

```
[root@localhost lanb]# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.593 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.454 ms
^C
--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.454/0.706/1.072/0.265 ms
```

Figura 145. C7-LAN-B (10.10.10.2)

6.3 Enrutamiento estático

El enrutamiento estático es la solución para redes pequeñas por su seguridad y por la economía de sus recursos; no consume ancho de banda, no hace trabajar a la CPU del router y es fácil de configurar. En este se exige la intervención del administrador cada vez que se producen cambios en la red. Para su configuración se ejecuta el siguiente comando: *#ip route ip_red_destino máscara_red_destino ip_puerta_entrada*

Donde:

- ip_red_destino → corresponde a la red vecina donde se quiere acceder.

- máscara_red_destino → corresponde a la máscara de la red vecina.

- ip_puerta_entrada → corresponde a la ip de la interface que se encuentra relacionada con la red a la que se quiere acceder (ver figura 146).

6.3.1 Esquema 1

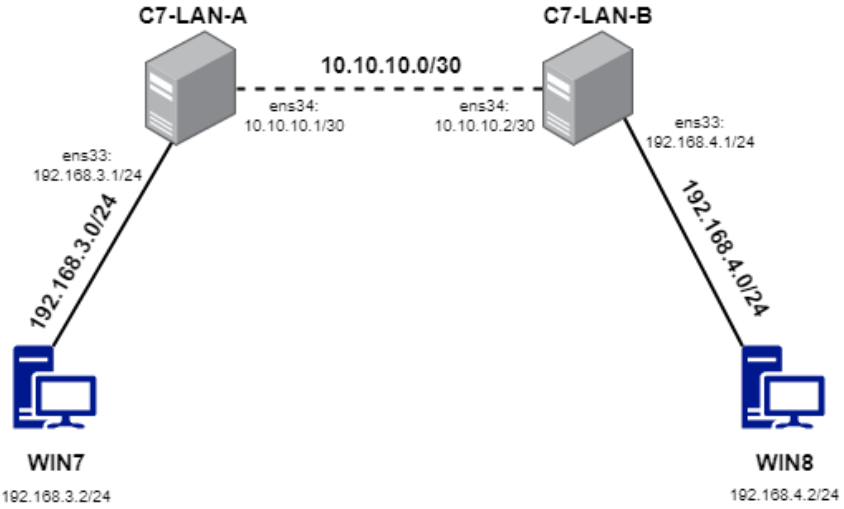


Figura 146. Esquema 1

Proceso

Para la configuración del esquema 1 presentado, se asume haber realizado la correcta implementación del **esquema 0** estudiando anteriormente. Se empieza agregando direccionamiento lógico a las máquinas clientes de cada red según corresponda, de tal manera que (ver cuadro 2):

Cliente:	**WIN7**	**WIN8**
Dirección ip:	192.168.3.2	192.168.4.2

Máscara de subred:	255.255.255.0	255.255.255.0
Gateway (puerta de enlace):	192.168.3.1	192.168.4.1

Cuadro 2 Direccionamiento lógico a las máquinas clientes

Las máquinas clientes ya tendrían comunicación con sus servidores, pero entre ellas aún no, debido a que el servidor *C7-LAN-A* no conoce de la red *192.168.4.0/24* que es manejado por el servidor *C7-LAN-B* y viceversa. Para ello se añaden las redes vecinas en cada uno de los servidores, ejecutar:

En la terminal de C7-LAN-A:

#vtysh

#conf t

#ip route 192.168.4.0 255.255.255.0 10.10.10.2

En la terminal de C7-LAN-B:

#vtysh

#conf t

#ip route 192.168.3.0 255.255.255.0 10.10.10.1

De esta forma, ya se encuentran en convergencia las dos redes y sus máquinas clientes pueden comunicarse. A continuación, se realizan las pruebas con el comando *ping* y *tracert*:

Desde la máquina WIN7 (ver figuras 147 y 148):

Figura 147. Pruebas con el comando ping WIN 7

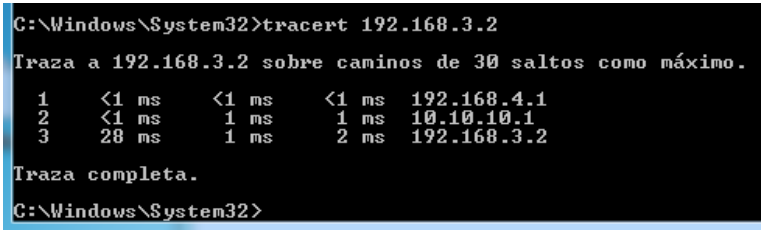


Figura 148. Pruebas con el comando tracert WIN 7

Desde la máquina WIN8 (ver figuras 149, 150 y 151):

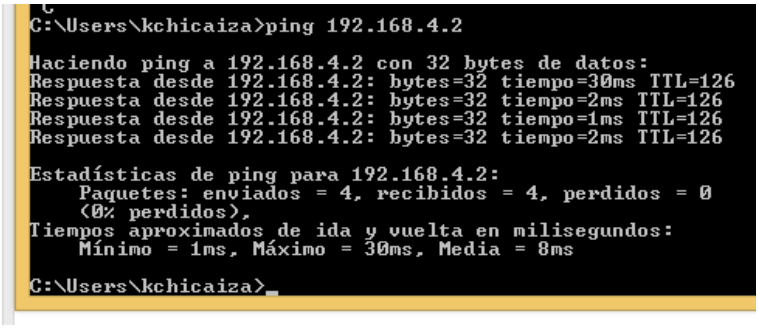


Figura 149. Pruebas con el comando ping WIN 8

```
C:\Users\kchicaiza>tracert 192.168.4.2

Traza a 192.168.4.2 sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  192.168.3.1
  2     1 ms    <1 ms    <1 ms  10.10.10.2
  3     1 ms    27 ms     1 ms  192.168.4.2

Traza completa.

C:\Users\kchicaiza>
```

Figura 150. Pruebas con el comando tracert WIN 8

6.3.2 Esquema 2

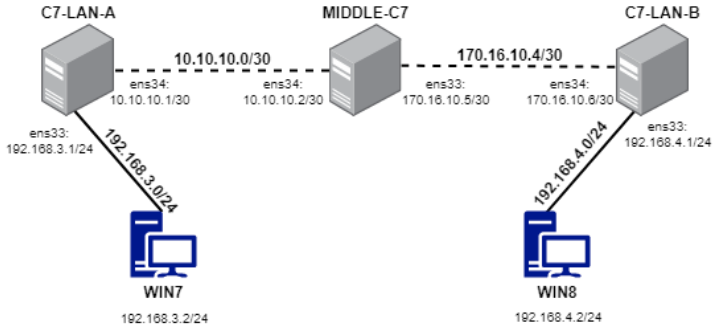


Figura 151. Esquema 2

Proceso

En comparación con el esquema 1 se agrega un servidor intermedio y una nueva red *WAN*, la configuración de los servidores es muy similar a la del esquema anterior, por lo que se presenta a continuación sin mayores detalles (ver cuadro 3):

*Tomando en consideración que se entra por primera vez a la Shell vtysh

Configuración de interfaces	
C7-LAN-A	**MIDDLE-C7**
vtysh conf t log file	*Cambios en la interfaz ens34:* ip add 10.10.10.2 255.255.255.252

/var/log/quagga/quagga.log int ens33 ip add 192.168.3.1 255.255.255.0 desc LAN-A no shut exit int ens34 ip add 10.10.10.1 255.255.255.252 desc link to MIDDLE-C7 no shut exit exit write	desc link to LAN-A *Cambios en la interfaz ens33:* ip add 170.16.10.5 255.255.255.252 desc link to LAN-B **C7-LAN-B** *Cambios en la interfaz ens34:* ip add 170.16.10.6 255.255.255.252 desc link to MIDDLE-C7 *Cambios en la interfaz ens33:* ip add 192.168.4.2 255.255.255.0 desc LAN-B

Cuadro 3 Configuración de interfaces

De esta forma, los servidores se encuentran correctamente configurados y podrían hacer ping entre ello, exceptuando que C7-LAN-A y C7-LAN-B no se podrán comunicar y que, de la misma forma, las máquinas clientes de cada red no pueden comunicarse entre ellas. Para ello, se añaden las redes vecinas de la siguiente manera:

En el servidor C7-LAN-A:

#ip conf t

#ip route 170.16.10.4 255.255.255.252 10.10.10.2

#ip route 192.168.4.0 255.255.255.0 170.16.10.6

En el servidor MIDLLE-C7:

#ip conf t

#ip route 192.168.3.0 255.255.255.0 10.10.10.1

#ip route 192.168.4.0 255.255.255.0 170.16.10.6

En el servidor C7-LAN-B:

#ip conf t

#ip route 10.10.10.0 255.255.255.252 170.16.10.5

#ip route 192.168.3.0 255.255.255.0 10.10.10.1

Por último, se les asigna direccionamiento lógico a las máquinas clientes y se ejecuta el comando ping y tracert para verificar que haya comunicación entre ellas.

6.4 Protocolo de enrutamiento RIP

Protocolo de enrutamiento por vector distancia con clase más antiguo, utiliza el conteo de saltos como métrica, es decir, se considera un salto cada vez que un paquete viaja de un router a otro con un límite de 15 saltos (si llega al salto 16 se considera como red inalcanzable) por paquete (TTL – tiempo de vida del paquete) y su distancia administrativa es de 120.

Para realizar la configuración con RIP es necesario copiar y activar el servicio dentro del servidor Centos 7, para ello ejecutamos con permisos de root (ver figura 152):

cp /usr/share/doc/quagga- XXXXX /ripd.conf.sample /etc/quagga/ripd.conf

service start ripd

chkconfig ripd on

6.4.1 Esquema 1

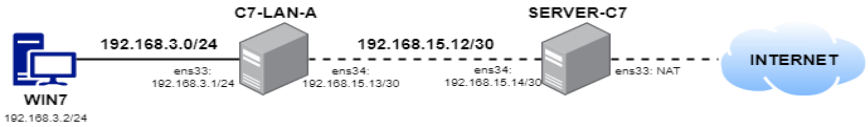


Figura 152. Esquema 1

Proceso

A continuación, se presenta la configuración de los servidores (ver cuadro 4) *Tomando en consideración que se entra por primera vez a la Shell vtysh

Configuración de interfaces	
C7-LAN-A	**SERVER-C7**
vtysh conf t log file /var/log/quagga/quagga.log int ens33 ip add 192.168.3.1 255.255.255.0 desc LAN-A no shut exit int ens34 ip add 192.168.15.13 255.255.255.252 desc link to SERVER-C7 no shut exit exit write	*La interfaz **ens33** se encuentra en modo NAT de forma predeterminada.* *Mientras que para la interfaz **ens34** se realiza lo siguiente:* vtysh conf t log file /var/log/quagga/quagga.log int ens34 ip add 192.168.15.14 255.255.255.252 desc link to LAN-A no shut exit exit write

Cuadro 4 Configuración de interfaces

Ahora para el ruteo entre los servidores se utiliza RIPv1 para añadir y publicar las redes conectadas directamente en cada uno de los servidores, por lo que se realiza lo siguiente:

En el servidor C7-LAN-A:

#vtysh

#conf t

#router rip

#version 1

#network 192.168.3.0/24

#network 192.168.15.12/30

En el servidor SERVER-C7:

#vtysh

#conf t

#router rip

#version 1

#network 192.168.15.12/30

Es necesario incorporar una ruta estática dentro del servidor de la LAN-A para el acceso a internet: #ip route 0.0.0.0 0.0.0.0 192.165.15.14

Por último, se agregan las reglas de firewall dentro de los servidores para permitir el paso hacia la conexión internet:

En el servidor C7-LAN-A:

#iptables –A FORWARD –s 192.168.3.0/24 –d 192.168.15.12/30 –j ACCEPT

#iptables –A FORWARD –s 192.168.3.0/24 –d 0/0 –j ACCEPT

#echo 1 > /proc/sys/net/ipv4/ip_forward

En el servidor SERVER-C7:

#iptables –A FORWARD –s 192.168.15.12/30 –d 0/0 –j ACCEPT

#iptables –A FORWARD –s 192.168.3.0/24 –d 0/0 –j ACCEPT

#iptables –t nat –A POSTROUTING –o ens33 –j MASQUERADE

#echo 1 > /proc/sys/net/ipv4/ip_forward

Se asigna direccionamiento lógico a las máquinas clientes y se podrán realizar las pruebas con el comando *ping* y *tracert* para verificar los saltos hasta llegar a la dirección destino, en este caso usamos 8.8.8.8 de Google (ver figuras 153 y 154):

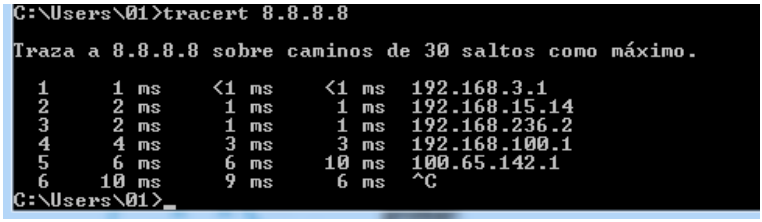


Figura 153. Verificación de los saltos

6.4.2 Esquema 2

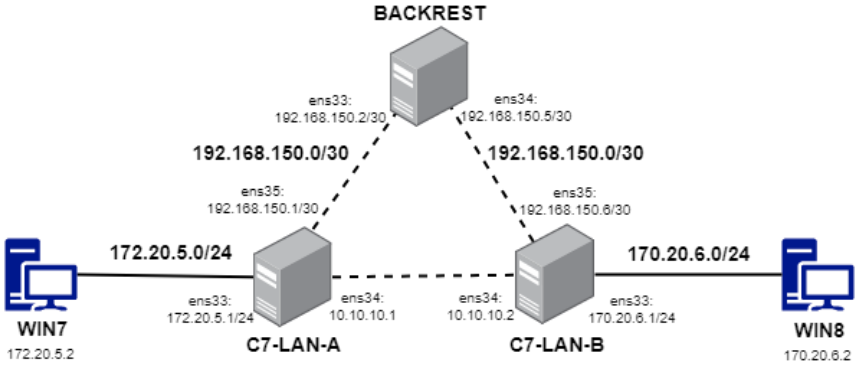


Figura 154. Esquema 2

Proceso

El esquema presentado permite tener una ruta de soporte en caso de que la principal falle. La configuración básica de todas ellas es la siguiente (ver cuadro 5):

<table>
<tr><th colspan="2">Configuración de interfaces</th></tr>
<tr><th>C7-LAN-A</th><th>BACKREST</th></tr>
<tr><td rowspan="2">vtysh
conf t
log file /var/log/quagga/quagga.log
int ens33
ip add 170.20.5.1 255.255.255.0
desc LAN-A
no shut
exit
int ens34
ip add 10.10.10.1 255.255.255.252
desc link to LAN-B
no shut
exit
int ens35
ip add 192.168.150.1 255.255.255.252
desc link to BACKREST</td><td>Cambios en la interfaz ens33:
ip add 192.168.150.2 255.255.255.252
desc link to LAN-A

Cambios en la interfaz ens34:
ip add 192.168.150.5 255.255.255.252
desc link to LAN-B</td></tr>
<tr><td>C7-LAN-B</td></tr>
<tr><td></td><td>Cambios en la interfaz ens33:
ip add 170.20.6.1 255.255.255.0
desc LAN-B

Cambios en la interfaz ens34:
ip add 10.10.10.2 255.255.255.252</td></tr>
</table>

no shut exit exit write	desc LAN-B *Cambios en la interfaz ens35:* ip add 192.168.150.6 255.255.255.252 desc link to BACKREST

Cuadro 5 Configuración de interfaces

Luego, mediante RIPv1 se realiza la publicación de las redes en cada uno de los servidores, de la siguiente manera:

En el servidor C7-LAN-A:

En el servidor C7-LAN-A:

#vtysh
#conf t
#router rip
#version 1
#network 170.20.5.0/24
#network 10.10.10.0/30
#network 192.168.150.0/30

En el servidor C7-LAN-B:

#vtysh
#conf t
#router rip
#version 1
#network 170.20.6.0/24
#network 10.10.10.0/30
#network 192.168.150.0/30

En el servidor BACKREST:

#vtysh
#conf t
#router rip

#version 1

#network 192.168.150.0/30

Por último, se realizan las pruebas con el comando *ping* y *tracert* para verificar si se logra la comunicación y por dónde se escapan los paquetes.

Como se especificó al principio del esquema, la configuración responde ante un fallo en alguna de sus dos rutas de comunicación, lo que permite que siga transmitiendo por una de las dos. Por ejemplo (ver figura 155):

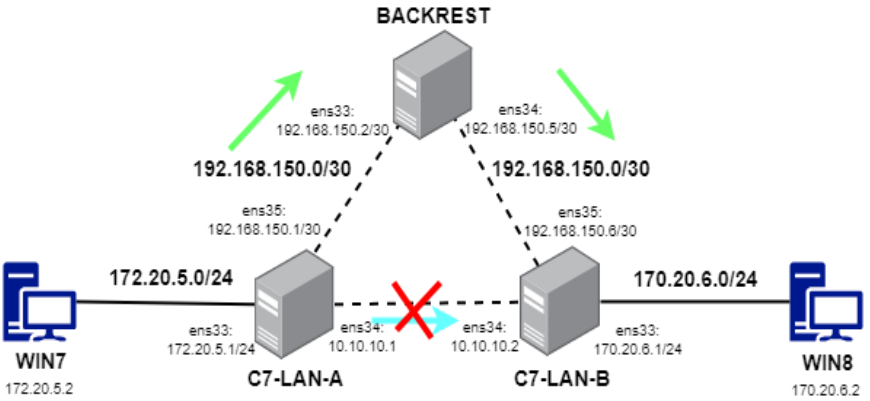


Figura 155. Esquema de configuración respondiendo ante un fallo

6.5 Configuración de OSPF

OSPF es un protocolo de enrutamiento de estado de enlace que se asemeja un sistema de navegación que tiene un mapa completo de la red. Si tiene un mapa completo de la red, puede calcular la ruta más corta a todos los diferentes destinos que existen. Se define como:

- Enlace: a la interfaz de nuestro enrutador.

- Estado: descripción de la interfaz y cómo está conectada a los enrutadores vecinos.

Los protocolos de enrutamiento de estado de enlace funcionan mediante el envío de anuncios de estado de enlace (LSA) a todos los demás enrutadores de estado de enlace.

El Protocolo OSPF traba con áreas por las que se enviarán los mensajes de actualización de rutas. Para ello cada, cada red se añade de la siguiente manera: # *network <dirección_red> <máscara_wildcard> area<id_área>*

Donde:

- *<dirección_red>:* puede ser una red completa, una subred o la dirección de la interfa
- *<máscara_wildcard>:* representa un conjunto de direcciones. La máscara tiene bits wildcard donde 0 representa que debe existir coincidencia y 1 donde no se comprueba la coincidencia. Por ejemplo 0.0.0.255 hace referencia a la máscara 255.255.255.0, por tanto, los primeros tres octetos deben coincidir mientras que él último no es necesario.
- *area<id_área>:* utilizado para agrupar varios routers en la misma área y su id.

Para empezar a utilizarlo en CentOS 7 es necesario copiar el archivo de configuración y activarlo, ejecutar lo siguiente (ver figura 156):

cp/usr/share/doc/quagga-XXXXX/ospfd.conf.sample /etc/quagga/ospfd.conf

service ospfd start

chkconfig ospfd on

6.5.1 Esquema 1

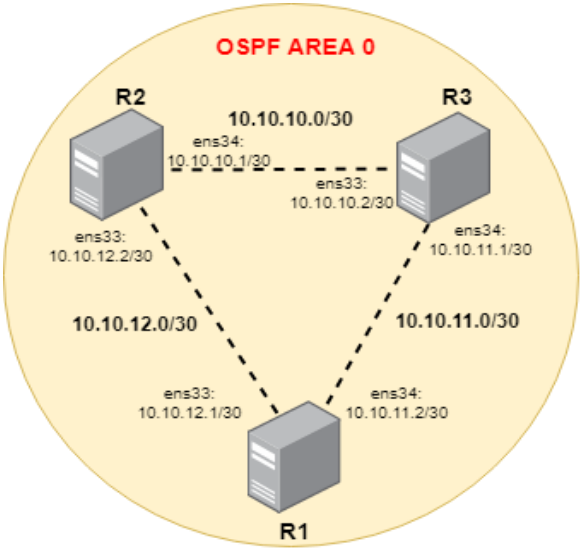


Figura 156. Esquema 1

Proceso

Configuración de las interfaces de los servidores (ver cuadro 6):

Configuración de interfaces	
R1	**R2**
vtysh conf t log file /var/log/quagga/quagga.log int ens33	*Cambios en la interfaz ens33:* ip add 10.10.12.2 255.255.255.252 desc link to R1

ip add 10.10.12.1 255.255.255.252 desc link to R2 no shut exit int ens34 ip add 10.10.11.2 255.255.255.252 desc link to R3 no shut exit exit write	*Cambios en la interfaz ens34:* ip add 10.10.10.1 255.255.255.252 desc link to R3 **R3** *Cambios en la interfaz ens33:* ip add 10.10.10.2 255.255.255.252 desc LAN-B *Cambios en la interfaz ens34:* ip add 10.10.11.2 255.255.255.252 desc LAN-B

Cuadro 6 Configuración de interfaces

Configuración del protocolo de enrutamiento OSPF:

En el servidor R1:

#vtysh

#conf t

#router ospf 1

#network 10.10.12.0 0.0.0.3 area 0

#network 10.10.11.0 0.0.0.3 area 0

En el servidor R2:

#vtysh

#conf t

 # router ospf 1

#network 10.10.10.0 0.0.0.3 area 0

#network 10.10.12.0 0.0.0.3 area 0

En el servidor R3:

#vtysh

#conf t

 # router ospf 1

#network 10.10.10.0 0.0.0.3 area 0

#network 10.10.11.0 0.0.0.3 area0

Las configuraciones surgten efecto automáticamente, sin necesidad de reiniciar el servicio *ospf*. Luego de su configuración se podrá verificar su configuración al ejecutar: *#show ip ospf neighbor*

Con este comando se reconocerán las rutas que lleva hacia los “vecinos” y verificar si están activos y aprendiendo las rutas adecuadas (ver figura 157).

6.5.2 Esquema 2

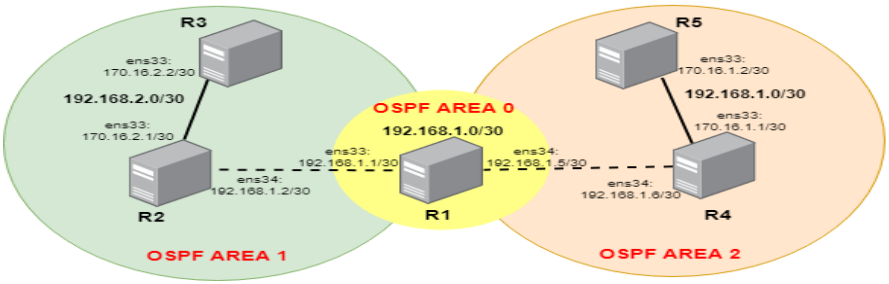


Figura 157. Esquema 2

Proceso

Se configuran las interfaces de los servidores, como lo muestra l cuadro 7:

<table>
<tr><td colspan="2">Configuración de interfaces</td></tr>
<tr><td>R1</td><td>R2</td></tr>
<tr><td rowspan="3">vtysh
conf t
log file /var/log/quagga/quagga.log
int ens33
ip add 192.168.1.1 255.255.255.252
desc link to R2
no shut
exit
int ens34
ip add 192.168.1.5 255.255.255.252
desc link to R4
no shut
exit
exit
write</td><td>Cambios en la interfaz ens33:
ip add 170.16.2.1 255.255.255.252
desc link to R3

Cambios en la interfaz ens34:
ip add 192.168.1.2 255.255.255.252
desc link to R1</td></tr>
<tr><td>R4</td></tr>
<tr><td>Cambios en la interfaz ens33:
ip add 170.16.1.1 255.255.255.252
desc link to R5

Cambios en la interfaz ens34:
ip add 192.168.1.6 255.255.255.252
desc link to R1</td></tr>
<tr><td>R3</td><td>R5</td></tr>
</table>

Cambios en la interfaz ens33: ip add 170.16.2.2 255.255.255.252 desc link to R2 **No existe la inerfaz ens34 en este servidor.*	*Cambios en la interfaz ens33:* ip add 170.16.1.2 255.255.255.252 desc link to R4 **No existe la inerfaz ens34 en este servidor.*

Cuadro 7. Configuración de interfaces

Configuración del protocolo de enrutamiento OSPF:

En el servidor R1:

#vtysh

#conf t

#router ospf 1

#network 192.168.1.0 0.0.0.3 area 0

En el servidor R2:

#vtysh

#conf t

#router ospf 1

#network 192.168.1.0 0.0.0.3 area 0

#network 170.16.2.0 0.0.0.3 area 1

En el servidor R4:

#vtysh

#conf t

#router ospf 1

#network 192.168.1.0 0.0.0.3 area 0

En el servidor R3:

#vtysh

#conf t

#router odpf 1

#network 170.16.2.0 0.0.0.3 area 1

#network 170.16.1.0.0.0.3 area 2

En el servidor R5:

#vtysh

#conf t

#router ospf 1

#network 170.16.1.0.0.0.3 area 2

Las configuraciones surten efecto automáticamente sin necesidad de reiniciar el servicio *ospf*. Luego de su configuración se podrá verificar su configuración al ejecutar: *#show ip ospf neighbor*. Con este comando se reconocerán las rutas que lleva hacia los “vecinos” y verificar si están activos y aprendiendo las rutas adecuadas.

CAPÍTULO 7: ZABBIX

7.1 Introducción ZABBIX

La necesidad de contar con un control que permita llevar a cabo la monitorización en tiempo real de todos los equipos y dispositivos conectados a una red es de suma importancia dentro de las organizaciones. El término monitorización de red describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, u otras alarmas. Es un subconjunto de funciones de la administración de redes. La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de computadoras son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificar las fallas en la red y de mostrar su comportamiento mediante el análisis y recolección de tráfico.

Hace no muchos años atrás el hablar de sistemas de monitoreo de servicios de red en sistemas operativos de red o desktop resultaba casi imposible, ya que no se tenía o era difícil conseguir las herramientas indispensables para hacerlo. Bastaba con saber que el servidor estaba operativo; la llevar a

cabo la ejecución de comandos básicos como el comando ping [1]y la dirección IP [2]del servidor.

El objetivo de todo administrador de sistemas es el de mantener las redes en pleno funcionamiento el 100% del tiempo. Las herramientas de monitoreo de red nos ayudarán a detectar posibles problemas que provocarán el colapso y/o la caída de las redes.

Es muy importante distinguir desde el principio la diferencia entre el monitoreo de red y la gestión de red. El monitoreo de red permitirá analizar y ver el estado de nuestras redes a un nivel básico. La gestión, permitirá no solo tomar acciones para paliar los problemas de nuestras redes, sino que dará una visión global de todos nuestros sistemas.

7.1.1 Justificación

Las organizaciones, independientemente del modelo o tipo de negocio que posean, deben tener un control y llevar a cabo una buena gestión sobre sus redes internas, es por esto por lo que se plantea el uso de herramientas que permitan llevar a cabo una monitorización en tiempo real de lo que sucede y acontece dentro de una red.

En el presente trabajo se aborda el monitoreo de redes, mediante la descripción de los diferentes enfoques y técnicas que se deben tener en consideración para implementar este servicio, los elementos a tomar en cuenta en un esquema de monitoreo, así como un resumen de algunas herramientas para su implementación.

Por ejemplo ¿cómo llevar el control de los servicios que se consumen por parte de los dispositivos conectados a la red?, ¿servicios tales como, proxy, correo, web y otras computadoras dentro de la intranet están en operación o activos?, ¿cómo saber si algún computador consume más

ancho de banda del permitido? Hoy existen diversos mecanismos para poder monitorear los diferentes servicios y servidores. Actualmente se pueden monitorear mediante diferentes herramientas, aquí es donde se propone la monitorización de una red mediante la herramienta Zabbix.

7.2 Manuales de Instalaciones

7.2.1 Instalación de servidor en Red Hat Enterprise Linux / CentOS

Con el apoyo de las versiones: RHEL6, Oracle Linux 6, 7 CentOS

Instalación de paquete de configuración del repositorio

Instalar el paquete de configuración del repositorio. Este paquete contiene los archivos de configuración de *yum*.

Zabbix 2.4 para RHEL6, Oracle Linux 6, CentOS 6: # *Rpm -ivh http://repo.zabbix.com/zabbix/2.4/rhel/ 7 / x86_64 / Zabbix-release-2.4-1.el7.noarch.rpm*

Instalación de paquetes de Zabbix

Instalar paquetes Zabbix. Ejemplo para el servidor Zabbix y frontal web con base de datos MySQL.

Nota: El repositorio oficial Zabbix proporciona Fping, iksemel, paquetes libssh2 también. Estos paquetes se encuentran en el directorio no compatible: # *yum install zabbix-server-mysql zabbix-web-mysql*

7.2.2 Instalar MYSQL 5.6

Utilizar los siguientes commandos de centOS:

> *yum install http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm*
>
> *yum install mysql-community-server*

systemctl start mysqld

- mysql -u root

- update user set password=PASSWORD("zabbix") where user='root';

-flush privileges;

systemctl enable mysqld.service

Scripts MySQL

mysql -uroot -pzabbix

mysql> create database zabbix character set utf8 collate utf8_bin;

mysql> grant all privileges on zabbix. to zabbix@localhost identified by 'zabbix';*

mysql> quit;

#mysql -uzabbix -pzabbix zabbix < /usr/share/doc/zabbix-server-mysql-2.4.7/create/schema.sql

#mysql -uzabbix -pzabbix zabbix < /usr/share/doc/zabbix-server-mysql-2.4.7/create/images.sql

 # mysql -uzabbix -pzabbix zabbix < /usr/share/doc/zabbix-server-mysql-2.4.7/create/data.sql

7.2.3 Creación de base de datos inicial

Crear la base de datos de usuario en Zabbix y MySQL. Revisar scripts de creación de base de datos de MySQL

Importar el esquema inicial y datos.

 # cd /usr/share/doc/zabbix-server-mysql-2.4.0/create

 # mysql -uroot zabbix < schema.sql

 # mysql -uroot zabbix < images.sql

 # mysql -uroot zabbix < data.sql

A partir proceso de servidor Zabbix editar configuración de la base de zabbix_server.conf

 # vi /etc/zabbix/zabbix_server.conf

DBHost=localhost

DBName=zabbix

DBUser=zabbix

DBPassword=zabbix

Iniciar el proceso de servidor Zabbix.

 # service zabbix-server start

7.2.4 Configuración de PHP de edición para Zabbix frontend

Archivo de configuración de Apache para Zabbix interfaz se encuentra en */etc/httpd/conf.d/zabbix.conf.* Algunas configuraciones de PHP ya están configuradas.

php_value max_execution_time 300

php_value memory_limit 128M

16M post_max_size php_value

php_value upload_max_filesize 2M

php_value max_input_time 300

 # Php_value date.timezone America / Guayaquil

Es necesario eliminar el comentario el ajuste "*date.timezone*" y establecer la zona horaria correcta para usted. Después de

cambiar el archivo de configuración, reinicie el servidor Web Apache.

7.3 Instalación de fuentes

Puede obtener la última versión de Zabbix si compila desde las fuentes.

Aquí se presenta un tutorial paso a paso para instalar Zabbix de las fuentes.

7.3.1 Instalación de demonios Zabbix

- Descargar el archivo fuente

Ir a la página de descarga Zabbix y descargar el archivo comprimido de origen. Una vez descargado, extraiga las fuentes, mediante la ejecución de: *$ tar -zxvf zabbix-2.4.0.tar.gz*

Nota: Introduzca la versión correcta Zabbix en el comando. Debe coincidir con el nombre del archivo descargado.

- Crear cuenta de usuario

Para todos los procesos daemon Zabbix, requiere un usuario sin privilegios. Si un demonio Zabbix se inicia desde una cuenta de usuario sin privilegios, se ejecutará como ese usuario. Sin embargo, si un daemon se inicia desde una cuenta 'root', cambiará a una cuenta de usuario '' Zabbix, que debe estar presente. Para crear una cuenta de dicho usuario (en su propio grupo, "Zabbix") en los sistemas Linux, ejecute:

groupadd zabbix

useradd -g zabbix zabbix

Una cuenta de usuario separada no es necesaria para la instalación frontend Zabbix.

Si Zabbix servidor y el agente se ejecutan en la misma máquina, se recomienda utilizar un usuario diferente para ejecutar el servidor que para ejecutar el agente. De lo contrario, si ambos son administrados como el mismo usuario, el agente puede acceder al archivo de configuración del servidor y cualquier usuario de nivel de administrador en Zabbix puede recuperar con bastante facilidad, por ejemplo, la contraseña de la base de datos.

Importante, correr Zabbix como root, bin, o cualquier otra cuenta con derechos especiales es un riesgo de seguridad.

- Crear la base de datos Zabbix

Para Zabbix servidor y de proxy demonios, así como frontend Zabbix, se requiere una base de datos. No es necesario para ejecutar Zabbix agente.

SQL secuencias de comandos se proporcionan para la creación de esquema de base e insertando el conjunto de datos. Base de datos de proxy Zabbix necesita solo el esquema de base de datos, mientras que el servidor Zabbix requiere también el conjunto de datos en la parte superior del esquema.

Después de haber creado una base de datos Zabbix, continúe con los siguientes pasos de la compilación de Zabbix.

- Configure las fuentes

Al configurar las fuentes para un servidor Zabbix o proxy, debe especificar el tipo de base de datos que se utilizará. Solo un tipo de base de datos puede ser compilado con un servidor Proxy o proceso a la vez.

Para ver todas las opciones de configuración compatibles, dentro del plazo extraído del directorio origen de Zabbix: *./configure --help*

Para configurar las fuentes para un servidor Zabbix y agente, es posible que encuentre algo así como:

> *./configure --enable-server --enable-agent --with-mysql --enable-ipv6 --with-net-snmp --with-libcurl --with-libxml2*
>
> *--with-libxml2 se requiere opción de configuración para el control de la máquina virtual, apoyado desde Zabbix 2.2.0.*

Para configurar las fuentes para un servidor Zabbix (con PostgreSQL, etc.), puede ejecutar: ./configure --enable-server --with-postgresql --with-net-snmp

Para configurar las fuentes de un proxy Zabbix (con SQLite, etc.), puede ejecutar: *./configure --prefix=/usr --enable-proxy --with-net-snmp --with-sqlite3 --with-ssh2*

Para configurar las fuentes de un agente Zabbix, puede ejecutar: *./configure --enable-agent*

Es posible usar la bandera -enable-static para enlazar estáticamente bibliotecas. Si va a distribuir binarios compilados entre los diferentes servidores, debe utilizar este indicador para hacer que estos binarios trabajos sin bibliotecas necesarias. Tenga en cuenta que --enable-static no funciona bajo Solaris.

El uso de la opción --enable- static, no se recomienda en la construcción de servidor.

Con el fin de crear el servidor de forma estática debe tener una versión estática de cada biblioteca externa necesaria. No hay verificación estricta para el script de configuración.

Comando de línea de los servicios públicos y zabbix_get zabbix_sender se compilan si se usa la opción -enable-agent.

Utilizar el indicador -con-IBM-DB2 para especificar la ubicación de la API de CLI.

Utilizar el indicador -con-Oracle para especificar la ubicación de la API de OCI.

- Hacer e instalar todo

Si está instalando desde SVN, que es necesario para ejecutar en primer lugar:

$ Make dbschema

make install

Este paso se debe ejecutar como usuario con permisos suficientes (comúnmente "raíz", o mediante el uso de sudo).

Ejecutar make install voluntad por defecto, instalar los binarios daemon (zabbix_server, zabbix_agentd, zabbix_proxy) en /usr/local/sbin y los binarios de cliente (zabbix_get, zabbix_sender) en / /local/bin usr.

NOTA: Para especificar una ubicación distinta de /usr/local, utilice una clave prefix en el paso anterior de la configuración de las fuentes, por ejemplo --prefix = / home / Zabbix. En este caso, se instalarán binarios demonios bajo <prefijo> / sbin, mientras que los servicios públicos bajo <prefijo> / bin. Las páginas man se instalarán bajo <prefijo> / acción.

- Revisar y editar los archivos de configuración

Para editar el archivo de configuración del agente */usr/local/etc/zabbix_agentd.conf* Zabbix, es necesario configurar este archivo para cada host con zabbix_agentd instalados. Se debe especificar la dirección IP del servidor Zabbix en el archivo. Se denegarán las conexiones desde otros hosts.

Para editar el archivo de configuración del servidor */usr/local/etc/zabbix_server.conf Zabbix*, se debe especificar el nombre de la base de datos, el usuario y la contraseña (si se utiliza alguno).

NOTA: Con SQLite la ruta completa al archivo de base de datos debe ser especificada; No se requiere de usuario DB y contraseña.

El resto de los parámetros que se adapte a sus valores por defecto. Si usted tiene una pequeña instalación (hasta diez monitoreados anfitriones) debe cambiar los parámetros por defecto si desea maximizar el rendimiento del servidor Zabbix (o poder).

Si ha instalado un proxy Zabbix, editar el archivo de configuración de proxy */usr/local/etc/zabbix_proxy.conf*

Se debe especificar la dirección IP del servidor y el nombre de host del proxy (debe ser conocido por el servidor), así como el nombre de la base de datos, el usuario y la contraseña (si se utiliza alguno).

- Poner en marcha los demonios

Ejecutar Zabbix_server en el servidor: *shell> zabbix_server*

Asegúrese de que el sistema permite la asignación de 36MB (o un poco más) de memoria compartida, de lo contrario el servidor no se inicie y se verá "No se puede asignar memoria compartida para <tipo de caché>." En el archivo de registro del servidor. Esto puede suceder en FreeBSD, Solaris 8.

Ejecutar Zabbix_agentd en todos los equipos monitorizados: *shell> zabbix_agentd*

Asegúrese de que el sistema permite la asignación de 2 MB de memoria compartida, de lo contrario el agente no se inicie y se verá "No se puede asignar memoria compartida para el

colector." En el archivo de registro del agente. Esto puede suceder en Solaris 8.

Si ha instalado Zabbix proxy, ejecute zabbix_proxy: shell> zabbix_proxy

7.4 Instalación de interfaz web Zabbix

Copia de archivos PHP

Zabbix frontend está escrito en PHP, por lo que para ejecutar un servidor web PHP se necesita el apoyo. La instalación se realiza simplemente copiando los archivos PHP de interfaces / php en el directorio de documentos del servidor web HTML.

Los lugares comunes de los documentos HTML directorios de los servidores Web Apache incluyen:

- /usr/local/apache2/htdocs (directorio por defecto cuando se instala Apache de la fuente)
- /srv/www/htdocs (OpenSUSE, SLES)
- /var/www/html (Fedora, RHEL, CentOS)
- /var/www (Debian, Ubuntu)

Se sugiere utilizar un subdirectorio en lugar de la raíz HTML. Para crear un subdirectorio y copiar archivos frontend Zabbix en ella, ejecute los siguientes comandos, reemplazan el directorio actual:

mkdir <htdocs>/zabbix

cd frontends/php

cp -a . <htdocs>/zabbix

Si instala desde SVN y planea utilizar cualquier otro idioma que no sea inglés, debe generar archivos de traducción. Para ello, ejecute: locale/make_mo.sh

Se requiere msgfmt utilty del paquete gettext.

Además, al utilizar cualquier otro idioma que no sea inglés, su localización debe estar instalado en el servidor web.

7. 5 Instalación de Frontend

• Paso 1: En su navegador, URL Zabbix abierta: *http: // <server_ip_or_name> / Zabbix*, debe ver la primera pantalla del asistente de instalación frontend (ver figura 158).

Figura 158. Instalación de Frontend paso 1

- Paso 2: Asegúrese de que se cumplen todos los requisitos previos de software (ver figura 159).

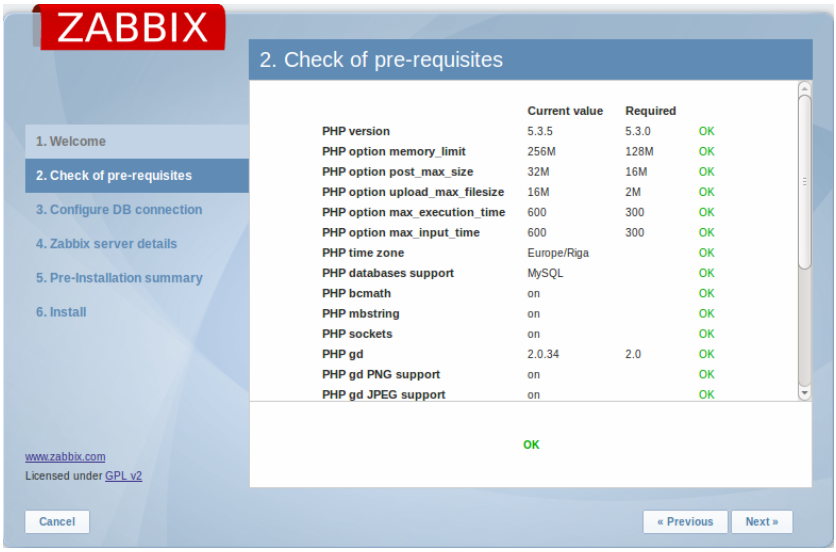


Figura 159. Instalación de Frontend paso 2

Los pre-requisitos opcionales también pueden estar presentes en la lista. Un requisito previo opcional no se muestra en naranja y tiene un estado de advertencia. Con un pre-requisito opcional fallado, el programa de instalación puede continuar.

Nota: Si hay una necesidad de cambiar el usuario o grupo de usuarios de Apache, permisos a la carpeta de la sesión deben ser verificadas. De lo contrario configuración Zabbix puede ser incapaz de continuar.

- Paso 3: Introduzca los detalles para la conexión a la base de datos. Zabbix base de datos ya debe estar creada (ver figura 160).

Figura 160. Instalación de Frontend paso 3

- Paso 4: Introduzca los detalles del servidor Zabbix (ver figura 161).

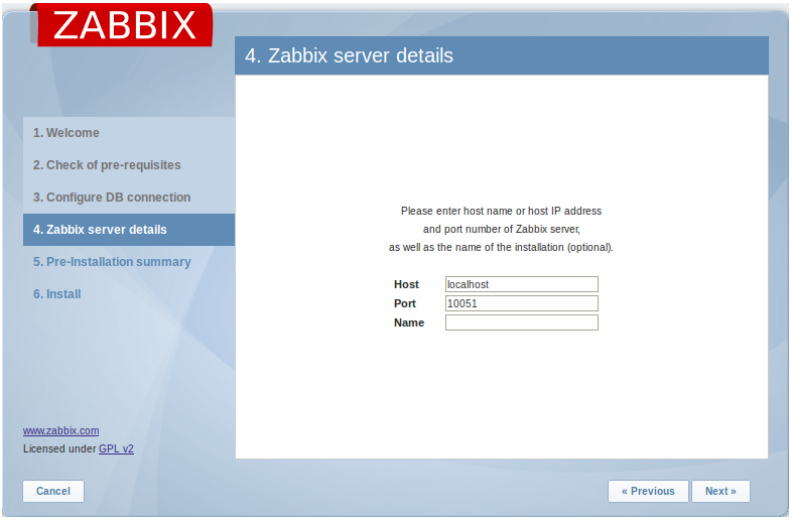


Figura 161. Instalación de Frontend paso 4

- Paso 5: Revisar un resumen de los ajustes (ver figura 162).

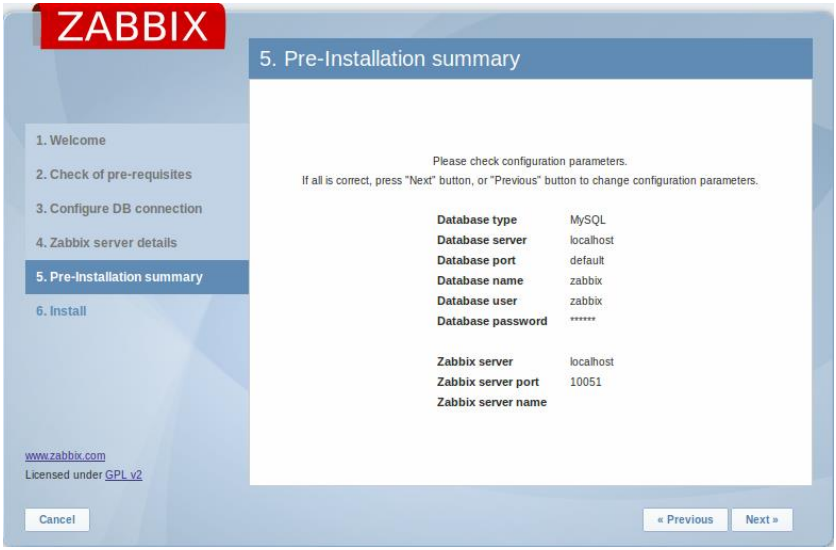


Figura 162. Instalación de Frontend paso 5

Paso 6: Descargar el archivo de configuración y colocarlo bajo *conf/* (ver figura 163).

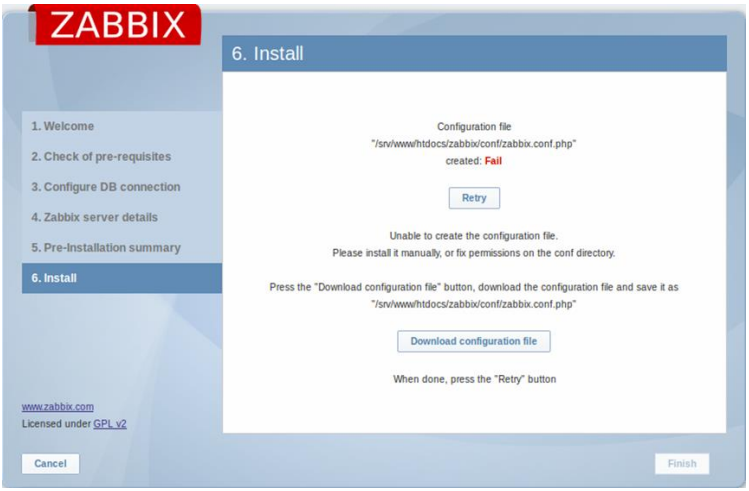


Figura 163. Instalación de Frontend paso 6.1

Nota: Proporcionar al usuario del servidor web tener acceso de escritura al directorio conf/ el archivo de configuración se guarda automáticamente y sería posible proceder al siguiente paso de inmediato (ver figura 164).

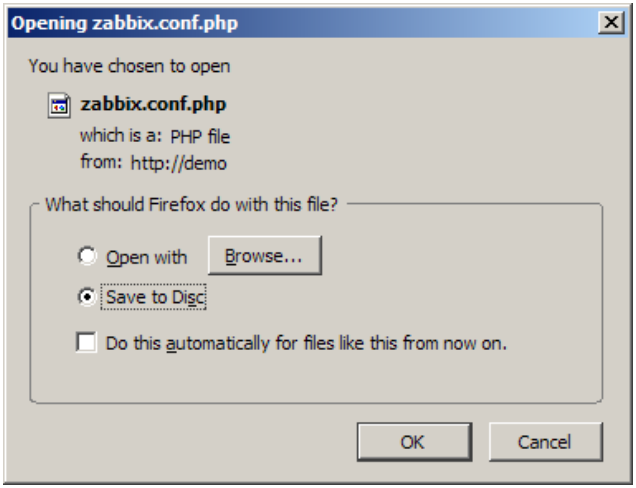


Figura 164. Instalación de Frontend paso 6.2

- Paso 7: Finalizar la instalación (ver figura 165).

Figura 165. Instalación de Frontend paso 7

- Paso 8: El frontend de Zabbix está listo. El nombre de usuario predeterminado es admin, Zabbix contraseña (ver figura 166).

Figura 166. Instalación de Frontend paso 8

7.6 Instalación de agente zabbix

- Paso 1: Añadir Obligatorio Repositorio

Antes de instalar el Agente Zabbix primer repositorio *yum* configure Zabbix usando comandos siguientes según su versión y el sistema operativo requerido.

CentOS/RHEL 7: # *rpm -Uvh http://repo.zabbix.com/zabbix/2.2/rhel/7/x86_64/zabbix-release-2.4-1.el7.noarch.rpm*

CentOS/RHEL 6: # *rpm -Uvh http://repo.zabbix.com/zabbix/2.2/rhel/6/x86_64/zabbix-release-2.2-1.el6.noarch.rpm*

- Paso 2: Instalar el agente Zabbix

Después de instalar paquetes del repositorio yum en nuestro sistema. Ahora usa siguiente comando para instalar el agente Zabbix en su Sytem Linux: # *yum install zabbix zabbix-agent*

- Paso 3: Configuración de la actualización del agente Zabbix

Como agente Zabbix ha sido instalado con éxito en nuestro sistema remoto. Ahora solo tenemos que configurar el agente Zabbix mediante la adición de IP del servidor Zabbix en su archivo de configuración /etc/zabbix/zabbix_agentd.conf

#Server=[zabbix server ip]

#Hostname=[Hostname of client system]

Server=192.168.1.11

Hostname=Server1

- Paso 4: Reinicio de Agente Zabbix

Después de la adición de IP del servidor Zabbix en el archivo de configuración, ahora reiniciar el servicio de agente mediante el siguiente comando: # */etc/init.d/zabbix-agent restart*

Para iniciar y detener Zabbix-agente de uso de los servicios en cualquier momento después de comandos.

 # /etc/init.d/zabbix-agent start

 # /etc/init.d/zabbix-agent stop

Ha instalado con éxito Zabbix Agent. Deja Agregar host en Zabbix Server para ser monitorizada.

Referencias

Barrios, J. (2016). *AlcanceLibre.org*. Recuperado de http://www.alcancelibre.org/staticpages/index.php/03-useradd-default

Capella, J. V. (2012). *Universitat Politecnica de Valencia*. Recuperado de Universitat Politecnica de Valencia: https://riunet.upv.es/handle/10251/16310

Clara, C. (2018). *Repositorio UNAD*. Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/18977/1004546304.pdf?sequence=1

Cruz, J., Mora, G., Sauza, B., Pérez, S. y Cruz, D. (2016). *Seguridad en redes LAN implementando VLAN*. Recuperado de https://repository.uaeh.edu.mx/revistas/index.php/sahagun/article/download/2355/2357?inline=1

EcuRed (2019). Recuperado de https://www.ecured.cu/Terminal_de_GNU/Linux

Fedora (s.f.). *Un sistema operativo libre*. Recuperado de https://fedoraproject.org/w/uploads/1/11/Fedora-flyer-ind-es-ES.pdf

García, S. (2010). *Experiencias con Redes Privadas de VLAN*. Recuperado de http://www.it.uc3m.es/azcorra/papers/exp_it03.pdf

Guerrero, E. (2018). *Repositorio UNAD*. Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/19030/73188424.pdf?sequence=5&isAllowed=y

León, B. (2018). *Universidad Nacional Abierta y a Distancia*. Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/18873/79767582.pdf?sequence=1&isAllowed=y

Sierra, B. (2017). *UNAD*. Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/21186/1103113587.pdf?sequence=1&isAllowed=y

Soler, R. (2017). *Universidad Nacional Abierta y a Distancia*. Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/14993/40428863.pdf?sequence=1&isAllowed=y

Soto, E. (2015). *Historia y Evolución de Ubuntu*. Recuperado de https://es.scribd.com/document/260080636/Historia-y-Evolucion-de-Ubuntu

Versiones de Fedora (2019). Recuperado de https://es.wikipedia.org/wiki/Anexo:Versiones_de_Fedora.