COMPUTACIÓN

Configuración y administración avanzada sobre el Sistema Operativo Centos 7.0



COLECCIÓN CÁTEDRA

Jairo Hidalgo
Georgina Arcos
Jeffery Naranjo

Configuración y administración avanzada sobre el Sistema Operativo Centos 7.0



Computación
Facultad de Industrias Agropecuarias y Ciencias Ambientales
Universidad Politécnica Estatal del Carchi

Jairo Hidalgo
Georgina Arcos
Jeffery Naranjo

Configuración y administración avanzada sobre el Sistema Operativo Centos 7.0



Computación
Facultad de Industrias Agropecuarias y Ciencias Ambientales
Universidad Politécnica Estatal del Carchi



Para referenciar este libro:

Hidalgo, J., Arcos, G., & Naranjo, J. (2022). *Configuración y administración avanzada sobre el Sistema Operativo Centos 7.0*. Universidad Politécnica Estatal del Carchi.

1. Computación 2. Sistemas Operativos 3. Linux 4. Centos 7.0

Clasificación Thema: JPSN - Instituciones internacionales Clasificación Dewey: 370 - Educación

321 páginas; 17 x 24cm.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
Dr. Jorge Mina – Rector
Dra. Teresa Sánchez – Vicerrectora
M. Sc. Hernán Benavides – Decano de la Facultad de Industrias Agropecuarias y Ciencias Ambientales
M. Sc. Georgina Arcos – Directora de la carrera de Computación

PROCESO EDITORIAL
M. Sc. Marco Burbano – Presidente de la Comisión de Publicaciones
Dr. Duván Ávalos – Responsable de la Unidad de Publicaciones
Lic. Fernando Pazmiño – Diagramación y diseño
M. Sc. Johana Morillo – Gestión de publicación

AVAL ACADÉMICO
M. Sc. Mauricio Rea – Universidad Técnica del Norte
M. Sc. Andrés Guerrero – Investigador independiente

DATOS DE PUBLICACIÓN
Título: *Configuración y administración avanzada sobre el Sistema Operativo Centos 7.0*
Autores: Jairo Vladimir Hidalgo Guijarro / jairo.hidalgo@upec.edu.ec / https://orcid.org/0000-0001-8165-0192 – Georgina Guadalupe Arcos Ponce / georgina.arcos@upec.edu.ec / https://orcid.org/0000-0002-9955-9554 – Jeffery Alex Naranjo Cedeño / jeffer .naranjo@upec.edu.ec / https://orcid.org/0000-0002-7631-4175.
Concepto y diseño de portada: Lic. Fernando Pazmiño
Imagen de portada: freepik.com
Comentario de contratapa: M.Sc. Jhony Enríquez Herrera
DOI: https://doi.org/10.32645/9789942914804
ISBN: 978-9942-914-80-4
Disponibilidad digital: https://www.publicacionesupec.org/index.php/carchi
Edición: Primera, marzo de 2022
© Universidad Politécnica Estatal del Carchi
© Jairo Vladimir Hidalgo Guijarro
© Georgina Guadalupe Arcos Ponce
© Jeffery Alex Naranjo Cedeño

Calle Antisana y Avenida Universitaria, Tucán, Carchi, Ecuador.
Tel: 06 2 224 079 / 06 2 224 080 / 06 2 224 081 Ext: 1300 / 1301
publicaciones@upec.edu.ec / publicacionesupec@gmail.com

Ecuador, Tulcán. Noviembre de 2021

Prohibida la reproducción de este libro, por cualquier medio,
sin la previa autorización por escrito de los propietarios del copyright.

Contenido

INTRODUCCIÓN

CAPÍTULO 1: INTRODUCCIÓN A CENTOS 7

Introducción 22
Distribuciones de CentOS 23
Directorios y sistemas de archivos 24
Instalación de Linux Centos 7.0. en máquina virtual (virtual box 5.2.8) 25
Creación de usuarios, carpetas y directorios 38
Pasos para la creación de un nuevo usuario: 41
Paso para crear directorios o archivos y cambiarles sus permisos de lectura, escritura 43
Borrar un directorio o archivo 44
Pasos para el cambio de permisos archivos o directorios 44
Comando PROC, TOP, FREE, PS 46
/PROC 47
FREE 49
PS 49
TOP 52
Recuperación de la clave root 52
Pasos de recuperación 52
Partición de HDD en Centos 7.0 57
Lista de Comandos 57
Borrar una partición 58

Crear una nueva partición 58
Formatear una partición 58
Comprobar el tamaño de una partición 58
Corregir la tabla de particiones 59
Pasos a seguir 59
Configuración de interfaces de red en Centos 7.0 65
Pasos para la configuración 65
Configuración de un Servidor FTP en Centos 7.0 68
El servicio FTP 69
Instalación servidor FTP 69
Crear el usuario para el acceso por FTP 72

CAPÍTULO 2: INTRODUCCIÓN A SAMBA
Introducción 74
Funcionamiento Samba 4.6.2 74
Instalación de Samba 4.6.2 75

CAPÍTULO 3: INTRODUCCIÓN DE MOODLE 3.O
Introducción 83
Instalación de Moodle 3.0 84

CAPÍTULO 4: INTRODUCCIÓN DE SQUID 3.5
Introducción 98
Instalación de Squid 3.5 99

CAPÍTULO 5: INTRODUCCIÓN DE SSH
Introducción 106
Instalación y configuración de SSH 106
SSH desde un cliente Windows 109

CAPÍTULO 6: INTRODUCCIÓN DE NETDA
Introducción 113
Instalación y configuración de Netdata 114
Resultados 120

CAPÍTULO 7: INTRODUCCIÓN DE VNC
Introducción 124
Instalación configuración de VNC 124

CAPÍTULO 8: INTRODUCCIÓN DE WEBMIN 1.7
Introducción 134
Instalación y configuración de WEBMIN 1.7 138

CAPÍTULO 9: INTRODUCCIÓN DE JOOMLA 3.8
Introducción 145
Instalación y configuración de Joomla 3.8 145

CAPÍTULO 10: INTRODUCCIÓN DE WINE 1.7
Introducción 160
Instalación y configuración de Wine 1.7 160
Configuración de Wine 1.7 164

CAPÍTULO 11: INTRODUCCIÓN DE IPSEC
Introducción 168
Instalación y configuración de IPESEC 169
Cliente 175

CAPÍTULO 12: INTRODUCCIÓN DE NFS
Introducción 191
Instalación y configuración de NFS 192

CAPÍTULO 13: INTRODUCCIÓN DE OPENVPN
Introducción 200
Instalación y configuración de host a host 200

CAPÍTULO 14: INTRODUCCIÓN A CONFIGURACION DE SERVIDORES
Introducción a servidores 207
Servidor en Linux Ubuntu server 8.04 207
Configuración de Red 212

Configuración Del Servidor Web 215
Servidor FTP 219
Crear del usuario para el acceso por FTP 222
Conectar al cliente desde otra máquina 223

CAPÍTULO 15: CONFIGURACIÓN DE SISTEMAS OPERATIVOS DE SOFTWARE LIBRE

Instalación de Linux Ubuntu 255
Qué es Kali Linux 230
Instalación de Kali Linux en la máquina virtual y cambio de contraseña del root 230
Debian 9.3.0 246
¿Qué es Debian 9.3.0? 246
¿Para qué sirve Debian 9.3.0? 246
Instalación Debian 9.3.0 247
Instalación y configuración de openvpn de host a red desde un cliente FEDORA 268
Comandos de centos7.0 286
Información del sistema 286
Apagar, reiniciar o cerrar sesión 288
Gestionar archivos y directorios 288
Encontrar archivos 291
Montando un sistema de ficheros 292
Espacio en disco 293
Usuarios y grupos 293
Permisos en ficheros 294
Atributos especiales en ficheros 296
Archivos y ficheros comprimidos 296
Paquetes rpm (Red Hat, Fedora y similares) 298
Actualizador de paquetes yum (Fedora, Redhat y otros) 300
Gestión de paquetes deb (Debian, Ubuntu y otros) 301
Actualizador de paquetes apt y aptitude (Debian, Ubuntu y otros) 302
Ver el contenido de un fichero 303
Manipulación de texto 303

Establecer caracteres y conversión de ficheros 305
Análisis del sistema de ficheros 305
Formatear un sistema de ficheros 306
Partición de sistema swap 306
Salvas 306
CDROM 308
Trabajo con la red (LAN Y WIFI) 309
Redes de Microsoft Windows (Samba) 311
Cortafuegos (iptables) 311
Monitoreando y depurando 313
Seguridad y Cifrado 314
Otros comandos útiles 315

REFERENCIAS BIBLIOGRÁFICAS

ACERCA DE LOS AUTORES

A toda la comunidad académica de la Universidad Politécnica Estatal del Carchi que ha hecho posible la culminación del presente libro.

A los estudiantes de Cuarto Nivel de la Unidad de Análisis de Sistemas Operativos del periodo académico marzo 2018 - agosto 2018 de la carrera de ingeniería en Computación.

A todos ellos, un agradecimiento especial.

Introducción

Este libro se ha creado con el fin de proporcionar a los usuarios interesados en la instalación y administración del sistema operativo una fuente de consulta que incluye los procesos y procedimientos, explicados paso a paso para la utilización y configuración de servidores a través de la utilización del Sistema Operativo Linux Centos 7.0, constituyéndose en un aporte para estudiantes, docentes y público en general.

El texto está dispuesto en 16 capítulos que se subdividen en 45 temas.

- En el capítulo I se hace una introducción a Centos 7.0, su instalación, configuración de interfaces y creación de usuarios.

- El capítulo II hace una introducción a Linux Ubuntu y el cambio de contraseña ROOT.

- En el capítulo III se desarrolla el tema Samba, instalación y gestión de usuarios.

- En el capítulo IV y V se realiza una breve introducción a Debian y Moodle.

- El capítulo VI contiene una introducción a Squid.
- El capítulo VII presenta la forma de instalar ssh en Linux.
- En el capítulo VIII se describe a Netdata,
- En el capítulo IX se realiza una introducción a VNC.
- El capítulo X se trabaja con webmin y su configuración.
- En el capítulo XI se realiza una introducción de Joomla, instalación y su configuración.
- En el capítulo XII se realiza una introducción a wine 7
- En el capítulo XIII se habla de IPESEC.
- El capítulo XIV realiza una introducción a los sistemas de archivos NFS en Linux.
- En el capítulo XV se encuentra una introducción a Open vpn, como se configurará, sus tipos y sus diversos clientes.

El capítulo final hace una introducción a los servidores Ubuntu y FTP.

Cada capítulo muestra de manera práctica los temas a tratar, por lo que el estudiante debe analizar y comprender cada práctica y concepto propuesto en cada unidad, lo que le permitirá desarrollar la habilidad de auto aprendizaje de un profesional en formación.

En sus primeras páginas descubrirá una guía práctica de la instalación y configuración del sistema operativo dentro de una máquina virtual; además, podrá encontrar otras características del sistema que se demandan para la gestión y administración de servidores, redes y usuarios tanto en línea como locales.

Por último, el libro cuenta con un glosario de los términos más frecuentes que se utilizan lo que permitirá interactuar de manera más fácil con los usuarios y profesionales de Linux.

CAPÍTULO 1:
INTRODUCCIÓN A CENTOS 7



En este capítulo usted encontrará:

- *Introducción a Centos 7.0*
- *Instalación de Linux Centos 7.0 en la máquina virtual (virtual box).*
- *Creación de usuarios, carpetas y directorios.*
- *Comando PROC, TOP, FREE, P.*
- *Recuperación de la clave root*
- *Partición de HDD en Centos 7.0-linux.*
- *Configurar las interfaces de red en Centos 7.0*
- *Servidor FTP en Centos 7.0*

Introducción

CentOS (Community Enterprise Operating System) es una distribución de Linux que vio la luz en marzo de 2004 como un proyecto de código abierto. La comunidad de Linux basó su desarrollo en los paquetes fuente de la ditribución comercial de Red Hat Enterprise (RHEL), la cual solo puede ser utilizada con la adquisición de contratos de soporte. CentOS aprovechó el código fuente de RHEL durante su creación, puesto que Red Hat como proveedor de RHEL estaba obligado a publicar el código fuente de los componentes integrados como unos recursos open source. **Stallings, W. (2005). *Sistemas Operativos Aspectos internos y principios de diseño.* Pearson**

CentOS, en todas sus versiones publicadas, se apoya a nivel binario de los lanzamientos de RHEL, siendo compatibles, sin restricciones y sin la necesidad de un compilador extra. En el Governing Board del 2014, Red Hat y el equipo de desarrollo del proyecto CentOS se reunieron para realizar de forma conjunta el desarrollo y distribuciones futuras.

CentOS, como plataforma corporativa, está destinada principalmente a ser implementada en empresas y organizaciones de gran tamaño. Por esta razón, la distribución de Linux puede ser utilizada por el sector privado, a pesar de que esta nunca fue una prioridad del equipo de desarrollo. CentOS ha sido adoptado en mayor medida como un sistema operativo destinado a acoger servidores web por las facilidades que este ofrece, según w3techs.com (enero 2017), solo Ubuntu y Debian se utilizan con mayor frecuencia.

CentOS, como una solución corporativa, cuenta con características valiosas para sus usuarios. La plataforma se desarrolla de forma continua dando soporte al software más reciente y compatibilidad a las aplicaciones más antiguas. En el aspecto de la seguridad también nos ofrece una detección proactiva de vulnerabilidades, porque su código fuente cuenta con un elevado nivel de seguridad gracias a que soporta la extencion del Kernel SELinux

Desde los orígenes de CentOS, todos sus lanzamientos han ido de la mano de las publicaciones de RHEL notándose esto en los números de sus respectivas versiones, por ejemplo RHEL 6.2 y CentOS 6.2, manteniendo ciclos largos de mantenimiento y soporte; está previsto por parte de CentOS desde la versión 5.1 brindar un soporte general de hasta 7 años y un suministro de actualizaciones de seguridad de hasta 10 años (hasta la versión 5.0 eran solo 4 y 7 años).

Al igual que RHEL, CentOS cuenta con el gestor gráfico Anaconda para su instalación, así como "YUM" a manera de gestor de software y "RPM" como gestor de paquetes. A pesar de que se cuenta con los componentes de Red Hat y que los programas se ejecuten en RHEL, es común que no se cuente con las certificaciones y apoyo de los fabricantes, por lo cual no se garantiza el correcto funcionamiento en CentOS.

Distribuciones de CentOS

Tabla 1

Distribuciones de CentOs

Lanzamientos de CentOS	Arquitecturas	RHEL base	Fecha de lanzamiento de CentOS	Fecha de lanzamiento de RHEL
6.4 - LiveCD	i386, x86-64	6.4	2013-05-22	
6.4 - LiveDVD	i386, x86-64	6.4	2013-05-22	
6.4 - MinimalCD	i386, x86-64	6.4	2013-03-09	
6.4	i386, x86-64	6.4	2013-03-09	2013-02-21
7	x86-64	7.0	2014-07-07	2014-06-10
7.1503	x86-64	7.0	2015-03-31	
7.1511	x86-64	7.0	2015-12-14	
CentOS 8.0-1905	x86-64		2019-09-24	
CentOS 8.1-1911	x86-64		2020-01-15	
CentOS 8.2-2004	x86-64		2020-06-15	
CentOS 8.5-2111	x86-64		2021-11-16	

Fuente https://www.centos.org/

Directorios y sistemas de archivos

Para CentOS, todo elemento, ya sea un directorio, un fichero o un dispositivo, es un fichero. Aunque a un dispositivo se lo llame nodo, este seguirá siendo un fichero.

Los sistemas de ficheros de Linux y Unix se organizan en una estructura jerárquica, de tipo árbol. El nivel más alto del sistema de ficheros es el directorio raíz, el cual se representa por un slash "/". Todos los demás ficheros y directorios estarán bajo el directorio raíz.

Por ejemplo, /home/proyecto1/ejemplo.odt representa la ruta completa al fichero ejemplo.odt que está en el directorio proyecto1, que a su vez está bajo el directorio home, que por su parte está bajo el directorio raíz (/).

Por debajo del directorio raíz (/) hay un importante grupo de directorios común a la mayoría de las distribuciones de GNU/Linux. A continuación, hay una lista de los directorios que aparecen generalmente bajo el directorio raíz (/):

- */bin* - Aplicaciones binarias importantes
- */boot* - Ficheros de configuración del arranque, núcleos y otros ficheros necesarios para el arranque (boot) del equipo.
- */dev* - Los ficheros de dispositivo
- */etc* - Ficheros de configuración, scripts de arranque, etc.
- */home* - Directorios personales (home) para los diferentes usuarios.
- */initrd* - Usado cuando se crea un proceso de arranque initrd personalizado.
- */lib* - Librerías del sistema (libraries)
- */lost+found* - Proporciona un sistema de "perdido+encontrado" (lost+found) para los ficheros que existen debajo del directorio raíz (/).
- */media* - Particiones montadas (cargadas) automáticamente en el disco duro y medios (media) extraíbles como CDs, cámaras digitales, etc.

- */mnt* - Sistemas de archivos montados manualmente en el disco duro.
- */opt* - Proporciona una ubicación donde instalar aplicaciones opcionales (de terceros).
- */proc* - Directorio dinámico especial que mantiene información sobre el estado del sistema, incluyendo los procesos actualmente en ejecución
- */root* - Directorio personal del usuario root (superusuario); también llamado "barra-root".
- */sbin* - Binarios del sistema.
- */srv* - Puede contener archivos que le sirven a otros sistemas.
- */sys* - Archivos del sistema (system).
- */tmp* - Temporary files.
- */usr* - Aplicaciones y archivos a los que puede acceder la mayoría de los usuarios.
- */var* - Archivos variables como archivos de registros y bases de datos.

Instalación de Linux Centos 7.0. en la máquina virtual (virtual box 5.2.8)

Pasos para la instalación

Para instalar Centos 7.0 en la máquina virtual se deben tener en cuenta los siguientes requisitos:

- La ISO del sistema Centos 7.0
- Tener instalada la máquina virtual en este caso VirtualBox 5.2.8.

Paso 1: Abrir VirtualBox:

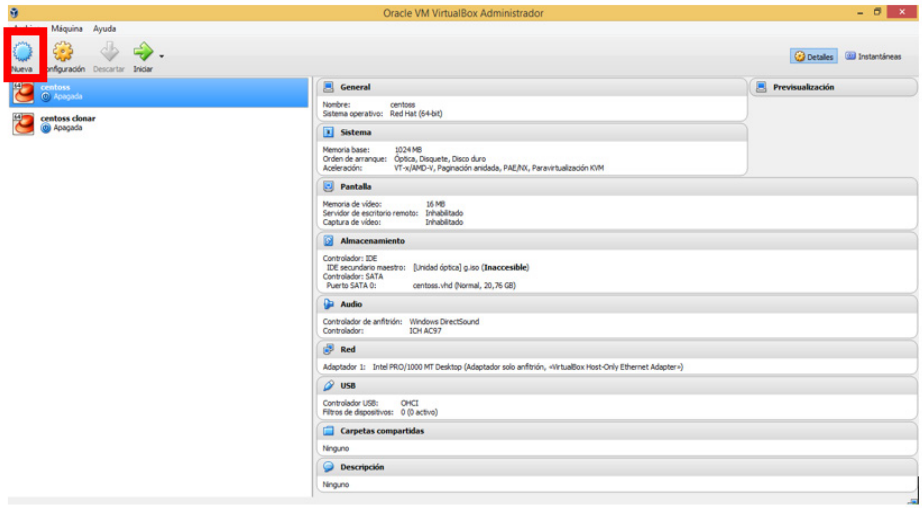


Figura 1: Pantalla de inicio de Virtual Box 5.2.8.

Paso 2: Desde la pantalla anterior, hacemos clic en el botón "Nueva", que nos permitirá crear una nueva máquina virtual:

En esta pantalla, hay que elegir los siguientes valores:

- Nombre: Centos 7.0
- Tipo: Linux
- Versión: Red Hat (64 bits)

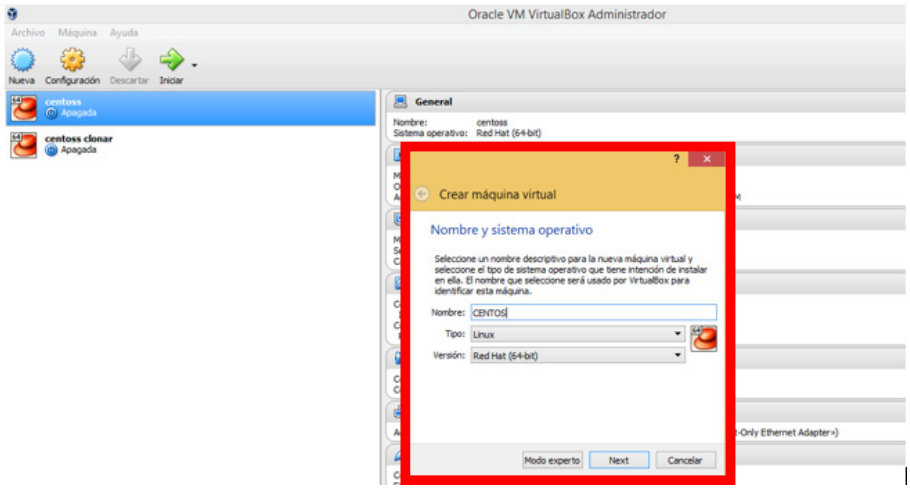


Figura 2: Pantalla de inicio para la instalación de nueva máquina virtual.

Paso 3: A continuación, pulse sobre el botón "Siguiente". En esta pantalla, hay que seleccionar la memoria que se le asignará a la máquina virtual, que deberá ser como mínimo de 1024 MB; y pulsaremos sobre el botón "Siguiente".

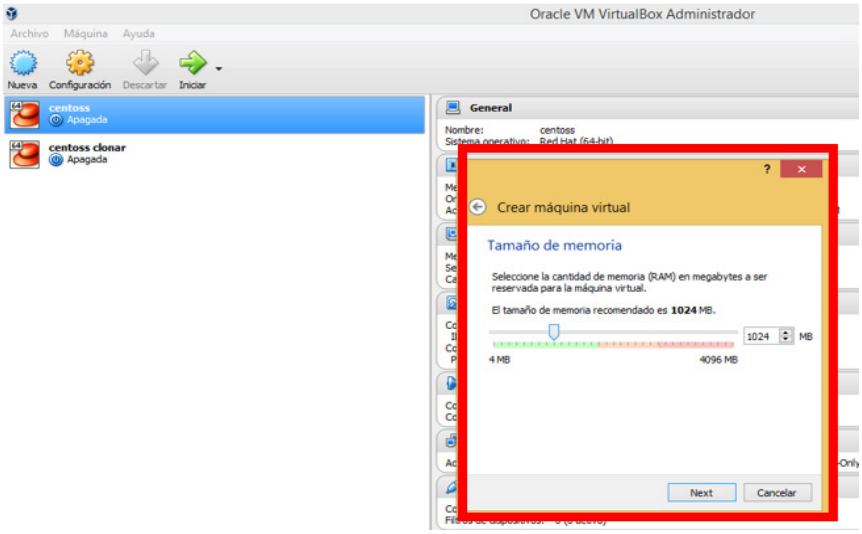


Figura 3: Asignación de memoria a la máquina virtual.

Paso 4: En esta pantalla, se elige la opción "crear un disco duro virtual ahora" y pulsaremos el botón "Crear".

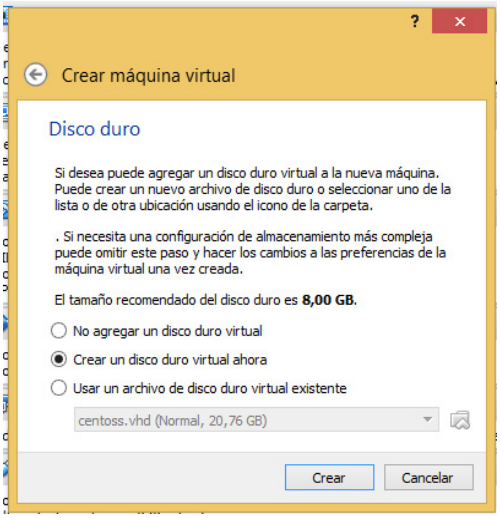


Figura 4: Creación del disco virtual.

Paso 5: Elegiremos la primera opción "VDI (VirtualBox Disk Image)" y pulsaremos el botón "Siguiente".

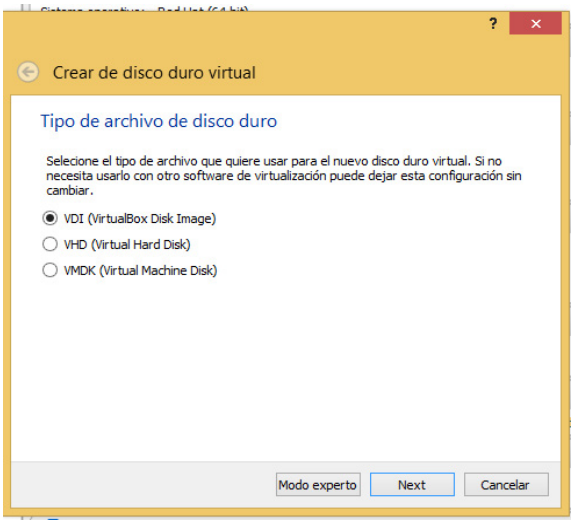


Figura 5: Selección del tipo de archivo a instalar (ISO).

Paso 6: Seleccione la primera opción, "Reservado dinámicamente", y pulse el botón "Siguiente".

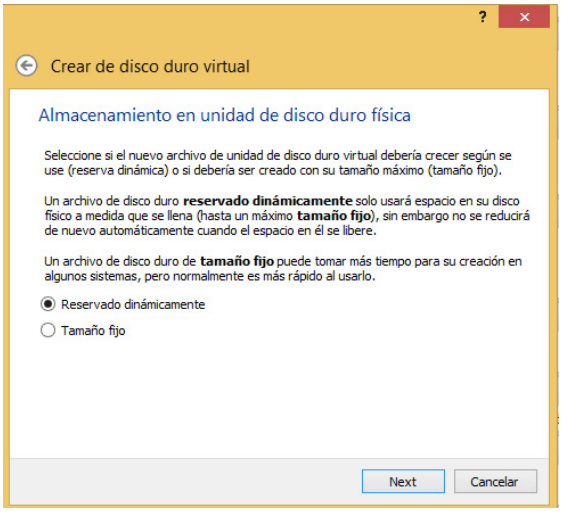


Figura 6: Selección del tamaño del disco duro a usar la máquina virtual.

Paso 7: Estableceremos el nombre de la imagen "Centos 7.0", y el tamaño en 8.00 GB. Después pulsaremos sobre el botón "Crear".

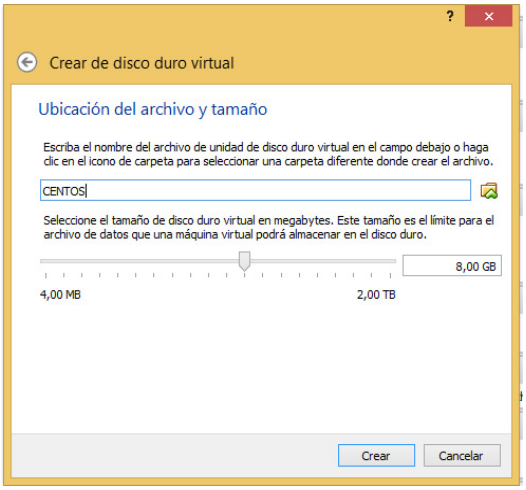


Figura 7: Creación de máquina virtual de Centos 7.0.

Paso 8: Observaremos en el inicio de VirtualBox la máquina virtual con el nombre de Centos 7.0

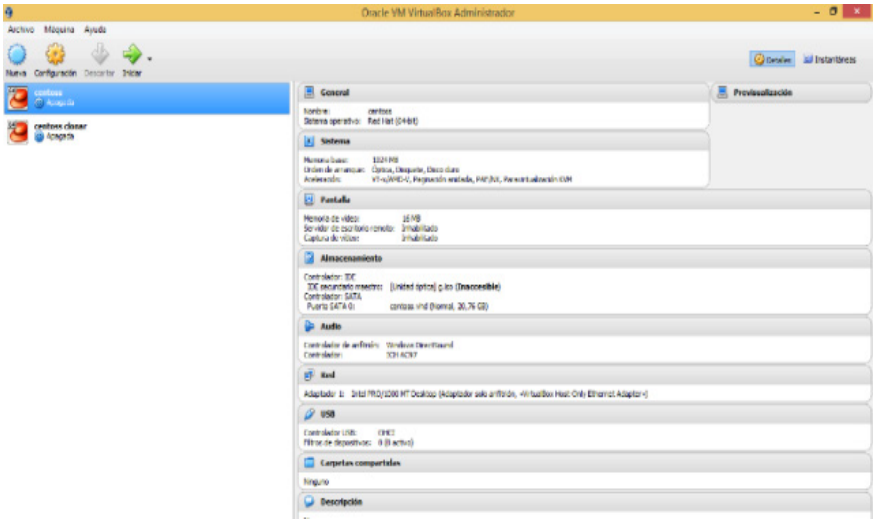


Figura 8: Vista de creación máquina virtual Centos 7.0.

Paso 10: Primer arranque de Centos 7.0. La máquina virtual de Centos 7.0 con Saltos pre-instalado ya está lista para ser usada. Para ello, pulsaremos sobre el botón "Iniciar".

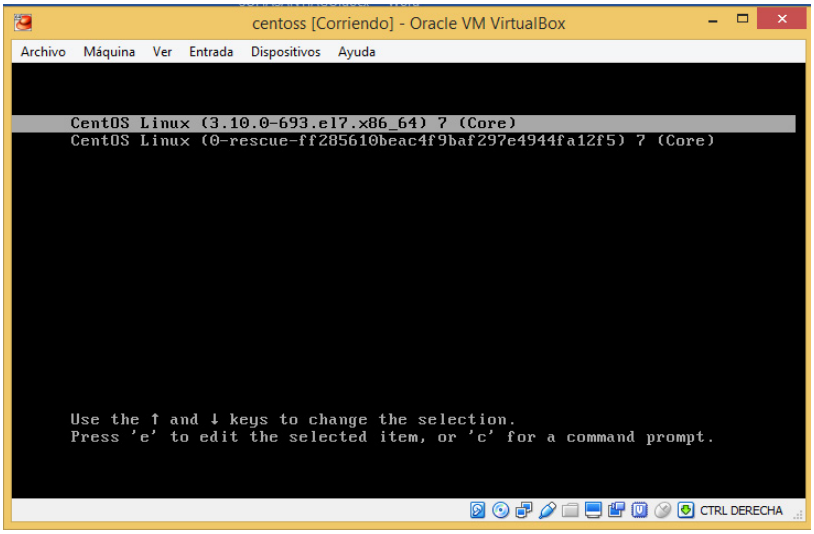


Figura 9: Arranque de Centos 7.0.

Paso 11: La primera pantalla de inicio será la configuración del idioma. Escogemos el idioma. Y hacemos clic en el botón "Continuar".

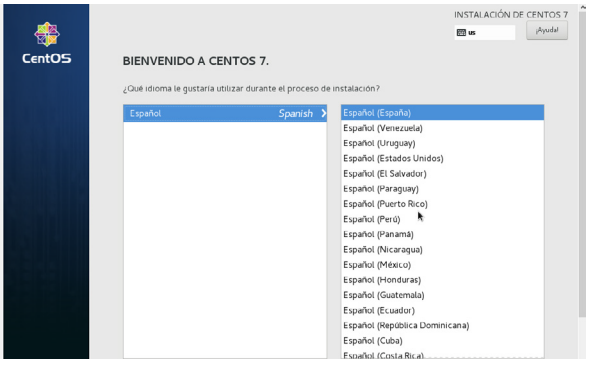


Figura 10: Seleccionamos el idioma a utilizarse.

Paso 12: Seleccionamos el punto de montaje en el sistema, el cual debe tener las especificaciones adecuadas de tamaño para el correcto funcionamiento.

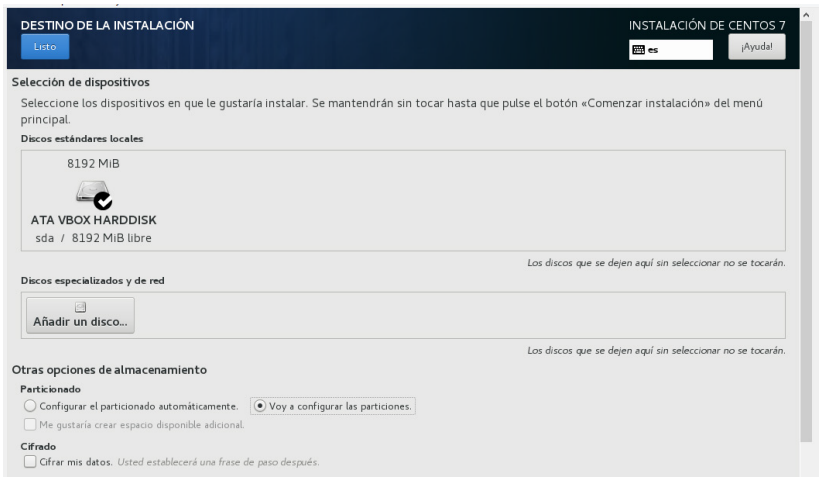


Figura 11: Selección de partición personalizada.

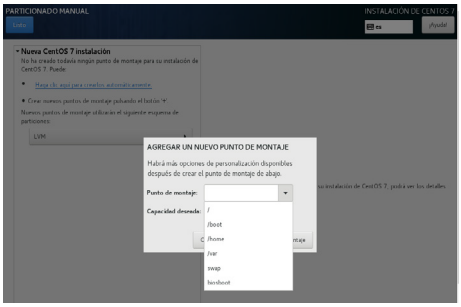


Figura 12: Selección del tipo de partición.

Descripción de los puntos de montaje

a. /boot: En este directorio se copiarán todos los archivos necesarios para el arranque del sistema operativo que se encuentre instalado en el equipo, cualquier versión que esta sea. Es fundamental que esté colocado sólo, en una partición primaria. El tamaño de la partición en la que se colocará este punto de montaje tiene que

ser aproximadamente de 150 MB cada tres sistemas operativos instalados. El tipo de formato de la partición en donde se colocará puede ser ext3, ext4, o btrfs a partir de fedora 16.

b. /(root): En este punto de montaje se irán copiando los archivos que hacen funcionar en su totalidad. No es imprescindible que el archivo esté solo, en una partición independiente, pero hay que tener en cuenta que con cada nueva instalación que hagamos, este punto de montaje se formatea, se sobrescribe y se pierden todos los datos anteriores. Pensando en un equipo de uso personal, recomendamos que el tamaño de la partición en donde coloquemos este punto de montaje no sea inferior a los 9 GiB, y tampoco es necesario que supere los 15 GiB. El tipo de formato que pide es ext3, ext4, o btrfs.

c. /home: En este punto de montaje se irán guardando todos los archivos personales del usuario. Por archivos personales no sólo tenemos que entender aquellos que utilizamos cotidianamente para nuestro trabajo, o estudio, o pasatiempos (textos, películas, fotos, música, entre otros), sino que tenemos que incluir a los archivos de configuración, o de estilo, o de apariencia, o nuestras preferencias a la hora de utilizar tal o cual programa. Es muy útil que coloquemos a este punto de montaje solo, en una partición independiente. De esta manera, llegado el caso de una nueva instalación, no es necesario formatearlo, y conservaremos todos nuestros archivos y todas nuestras configuraciones intactas. Caso contrario, cada vez que instalamos una nueva versión, tenemos que crear nuevamente este punto de montaje, formatearlo, sobrescribirlo, perder todos sus datos, y reconfigurar nuevamente todo lo que ya teníamos configurado. El tamaño de la partición en donde alojaremos este punto de montaje. Y el formato puede ser ext3, ext4, o btrfs a partir de fedora 15.

d. /swap: Este punto de montaje no necesita formato y se utilizará para dos cosas:

1. Si el equipo se queda con el acceso a la memoria ocupado, el sistema utilizará el espacio asignado en swap para "descongestionar, las capacidades saturadas de la memoria RAM".

2. Si usamos las funciones "suspender" o "hibernar" de nuestro equipo en lugar de apagarlo, en swap se volcará toda la información de nuestra sesión activa, de modo tal que nuestro equipo se "despierte" instantáneamente cuando lo indiquemos. Hay una fórmula muy conocida acerca del espacio de esta partición y es que debe tener "el doble que nuestra memoria RAM". Esta fórmula es de antigua data, y hoy en día, debido a la cantidad de memoria RAM de la que podemos disponer, es un tanto exagerada. A la partición que utilicemos para colocar este punto de montaje, no es necesario destinarle más que 4 GiB de espacio.

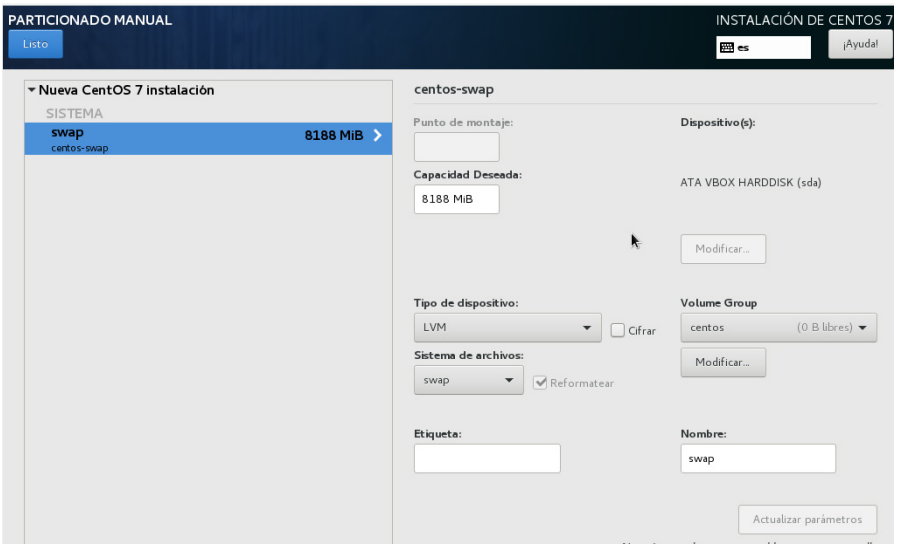


Figura 13: Establecer el sistema de archivos de la partición con el botón listo.

Paso 13: Llegamos a la pantalla de Resumen de Instalación. Hacemos clic al botón "Destino de la instalación".

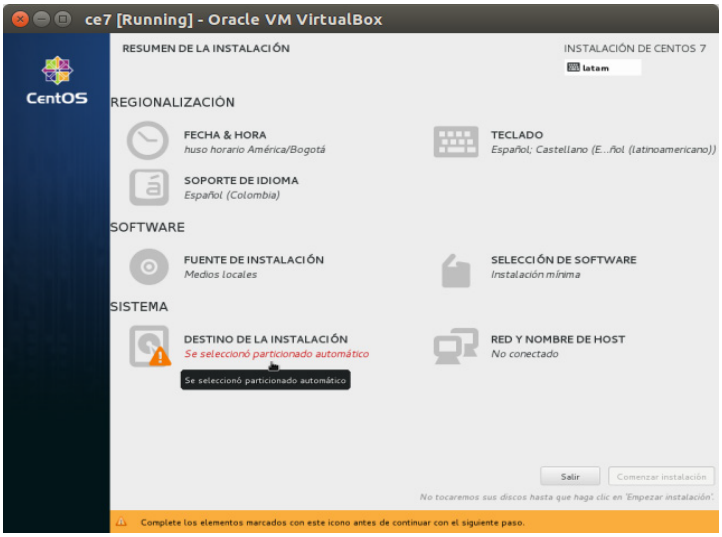


Figura 14: Pantalla de Resumen de Instalación.

Paso 14: Veremos los discos donde podemos instalar; por lo general, será un único disco, el cual debe estar seleccionado. En caso de querer un esquema diferente de particiones, este es el momento de hacerlo. Nos regresamos dando clic al botón "Listo".



Figura 15: Pantalla de selección de disco o particiones.

Paso 15: Nuevamente en el Resumen de Instalación, hacemos clic al botón "Red" y nombre de host.

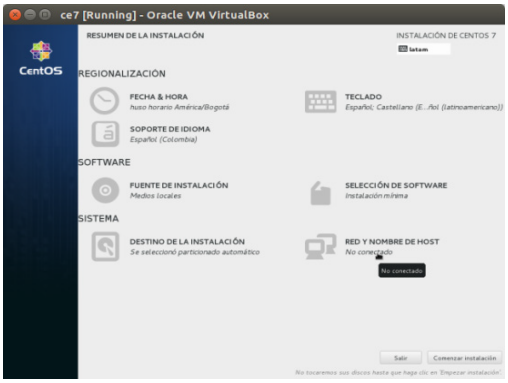


Figura 16: Pantalla de Resumen de Instalación.

Paso 16: Nuestro equipo se conectará a la red y nos mostrará los datos obtenidos vía DHCP. Hacemos clic al botón "Listo".

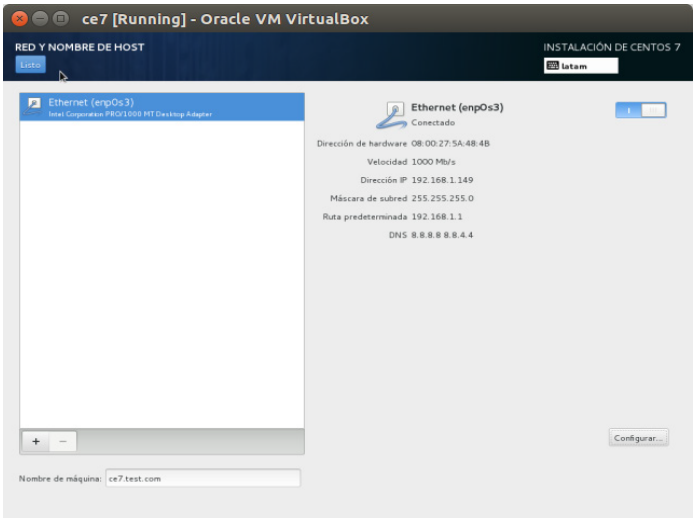


Figura 17: Activación de la tarjeta de red.

Paso 17: Ya estamos listos para comenzar a instalar. Hacemos clic al botón "Comenzar instalación".

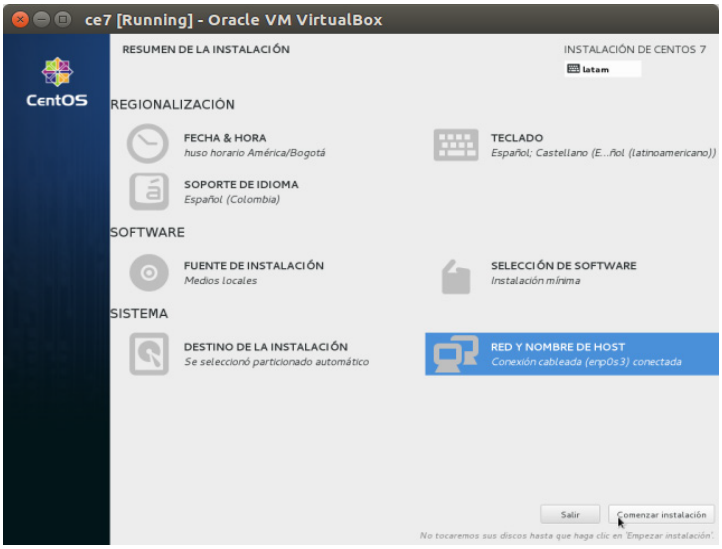


Figura 18: Inicio de instalación de Centos 7.0.

Paso 18: Mientras se instala, hacemos clic al botón "Contraseña de root", para habilitar la contraseña del superusuario; de igual manera, creamos un Usuario con sus respectivas credenciales de acceso.

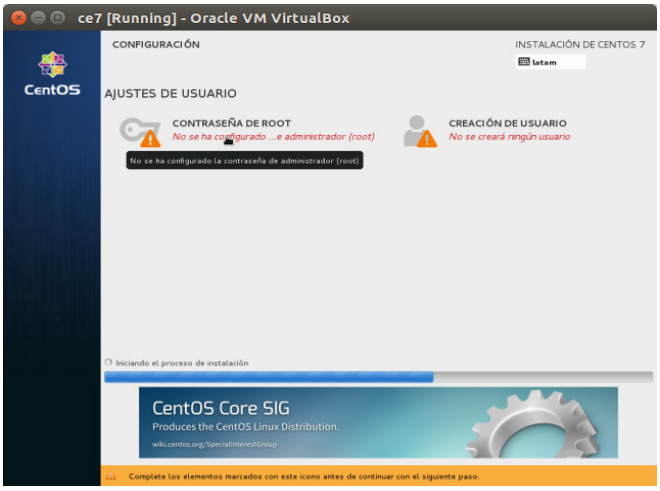


Figura 19: Configuración de contraseña root.

Paso 19: Escribimos dos veces una contraseña lo suficientemente compleja en las cajas de texto y hacemos clic al botón "Listo".

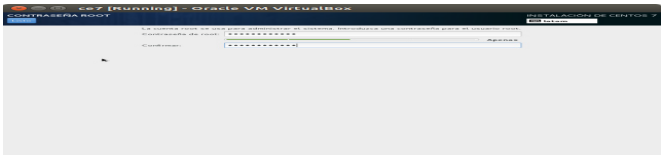


Figura 20: Ingreso de contraseña root.

Paso 20: Si deseamos, por seguridad, trabajar desde otro usuario, podríamos crearlo desde la opción "Creación de usuario".

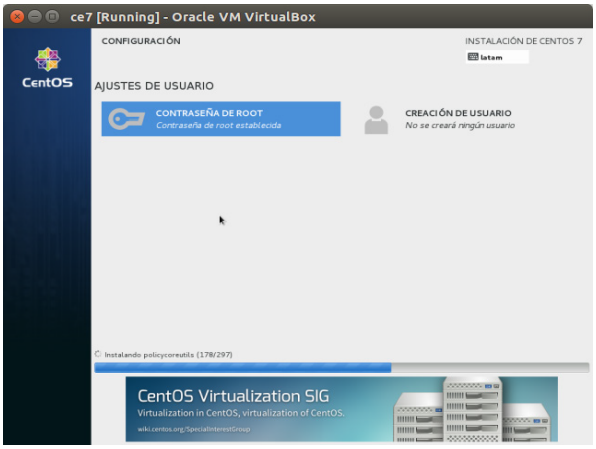


Figura 21: Instalación de Centos 7.0.

Paso 21: Una vez instalado Centos 7.0, este se reiniciará y aparecerá el usuario registrado con su respectiva casilla para ingresar contraseña.

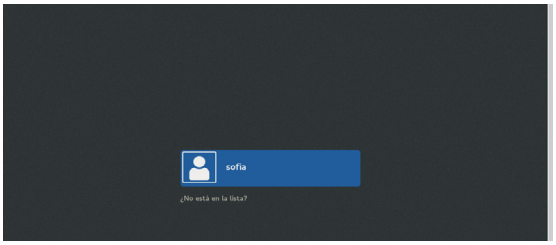


Figura 22: Usuario y contraseña.

Paso 22: Inicio del Sistema.

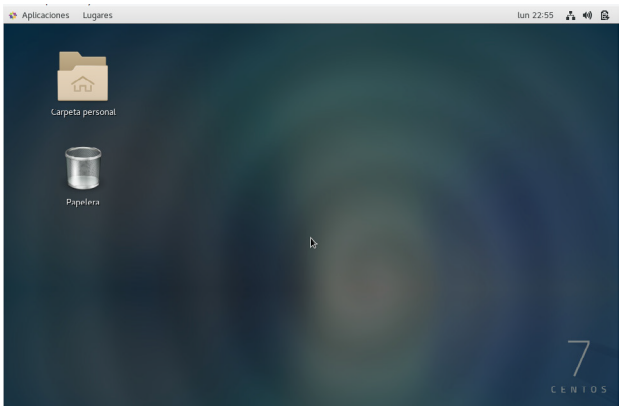


Figura 23: Pantalla de Inicio de Centos 7.0.

Creación de usuarios, carpetas y directorios

Usuario

Usuario, en informática *user*, es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema; además, se utiliza para clasificar a diferentes privilegios, permisos a los que tiene acceso un usuario o grupo de usuario, para interactuar o ejecutar con el ordenador o con los programas instalados en este.

El beneficio de crear usuarios y ubicarlos en un cierto grupo en el Sistema Operativo Centos7 es que ayuda a identificar y autentificar a un individuo con el sistema, permitiendo garantizar permisos de archivos y carpetas, facilitando el trabajo al administrador del sistema.

Directorio

En informática, un directorio (también llamado carpeta), es un contenedor virtual de archivos de datos. Los directorios están organizados de manera jerárquica partiendo de un directorio raíz (/) del que van colgando el resto de los directorios.

Pasos de creación de Usuarios

Paso 1: Visualizaremos la ubicación del usuario, su directorio y descripción existentes en el sistema con el siguiente comando:

Comando: cat/etc/passwwd:

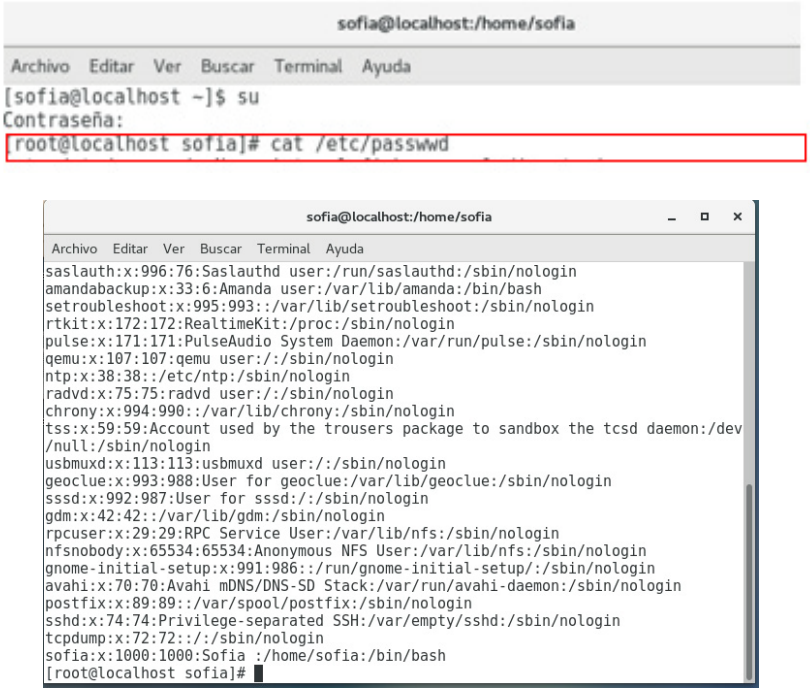
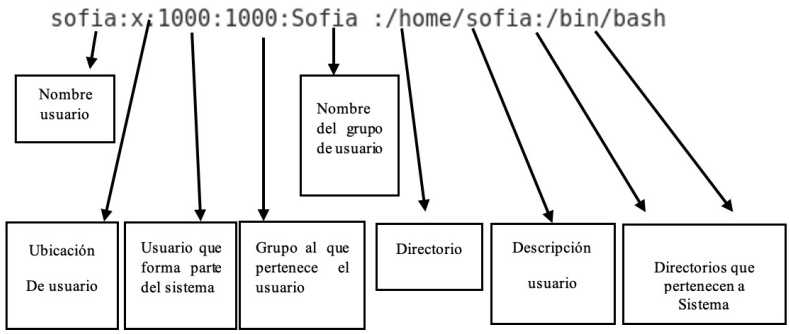


Figura 24: Ubicación *del usuario su directorio y descripción.*



Paso 2: Observación del usuario y contraseña del sistema. La contraseña está encriptada, siendo imposible descubrirla con el siguiente comando:

Comando: cat /etc/shadow:

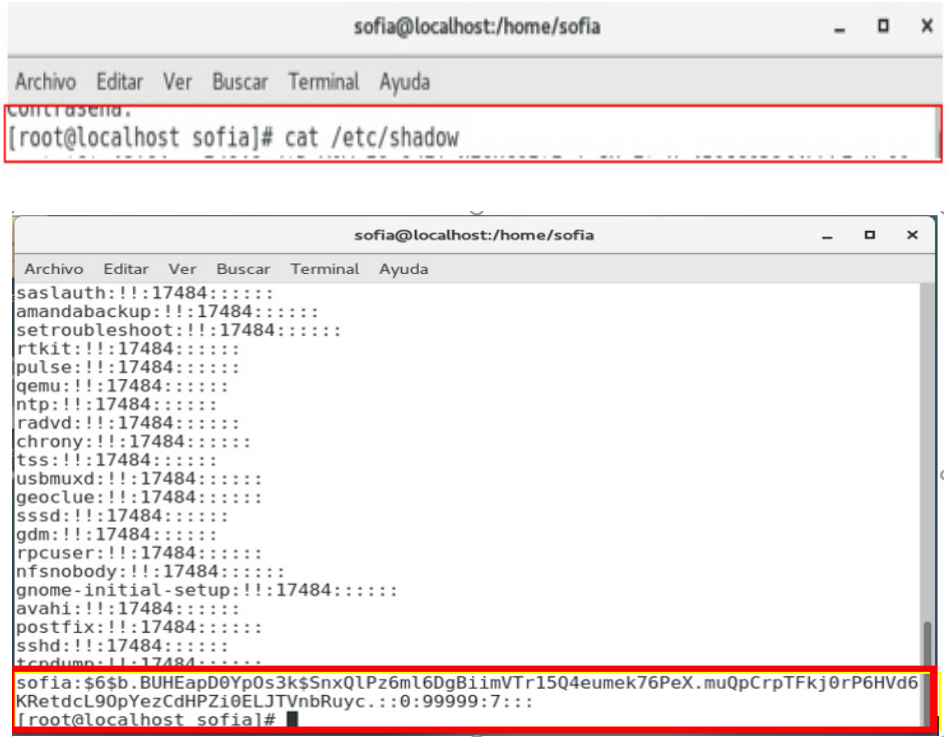


Figura 25: Usuario y Contraseña encriptada.

Paso 3: Identificación del grupo al que pertenece el usuario en el siguiente comando:

Comando: cat /etc/group

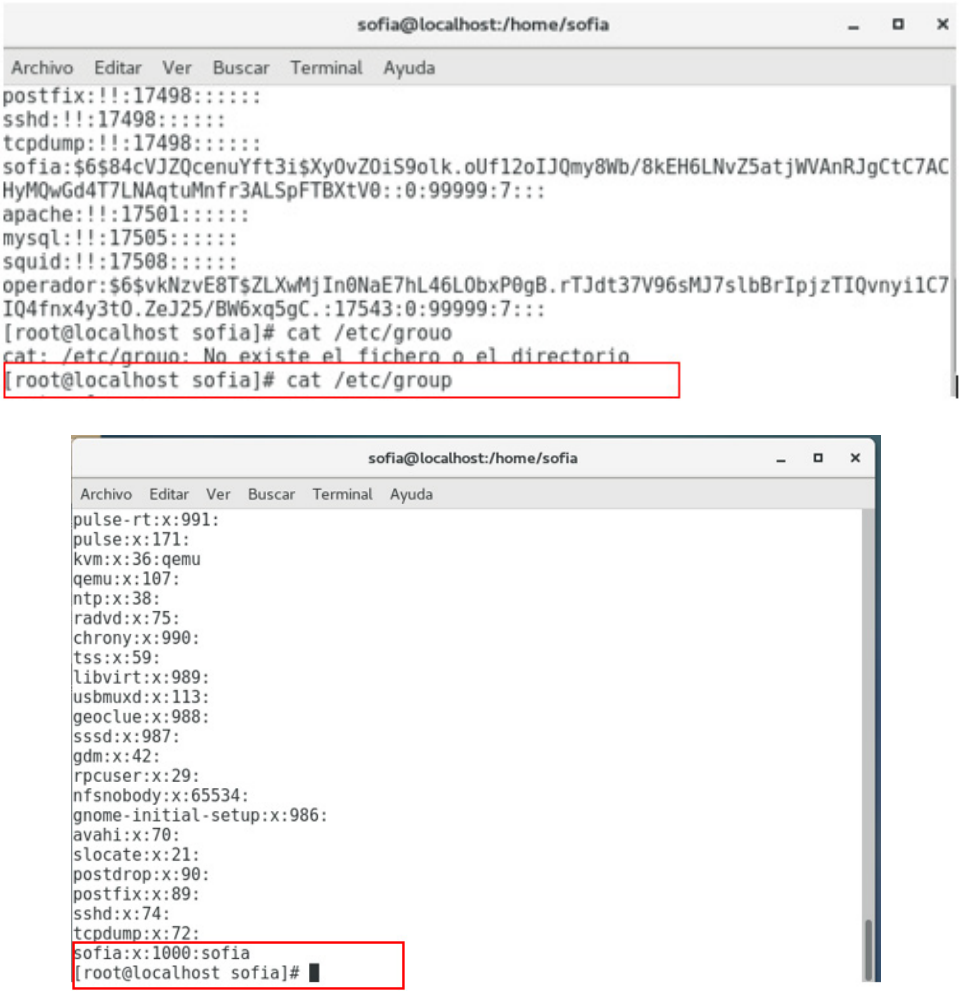


Figura 26: Grupo de usuario

Pasos para la creación de un nuevo usuario:

Paso 1: Añadir nuevo usuario al sistema con el nombre de usuario especificado con el siguiente comando:

Comando: useradd



Figura 27: Creación de usuario llamado clientes.

Paso 2: Crear contraseña para el nuevo usuario con el siguiente comando:

Comando: passwd nombre de usuario.

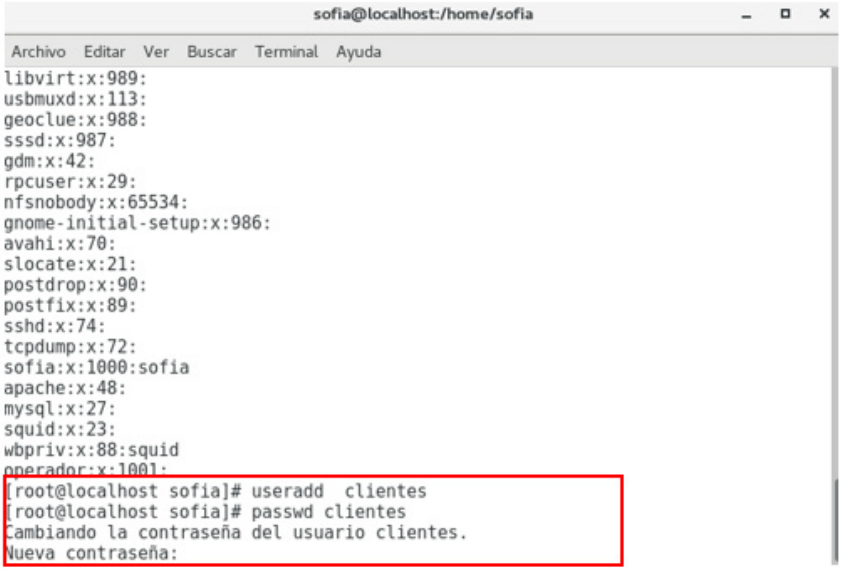


Figura 28: Creación de contraseña para usuario clientes.

Paso para crear directorios o archivos y cambiarles sus permisos de lectura, escritura

Paso 1: Para crear un directorio utilizaremos un comando junto con el nombre del directorio y la ubicación de este.

Comando: mkdir

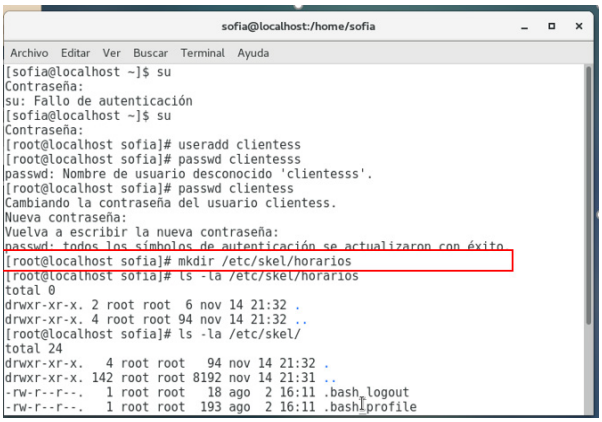


Figura 29: Creación de carpeta o directorio llamado horarios.

Paso 2: Este paso no es obligatorio. El comando sirve para identificar si tienes algún archivo dentro del directorio con el siguiente comando:

Comando: ls -la /etc/skel/horarios

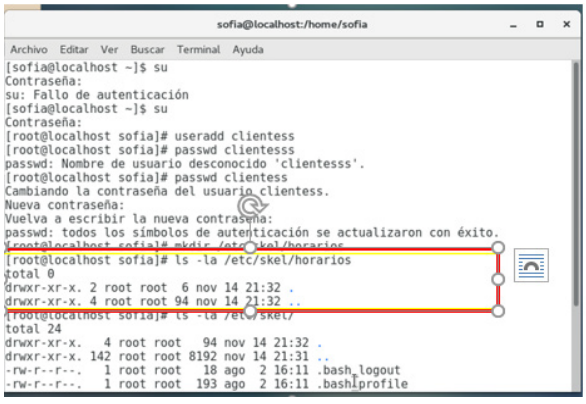


Figura 30: Vista de archivos dentro del directorio horarios.

Borrar un directorio o archivo

Para ello usamos el comando **rm-r** con el nombre el directorio.

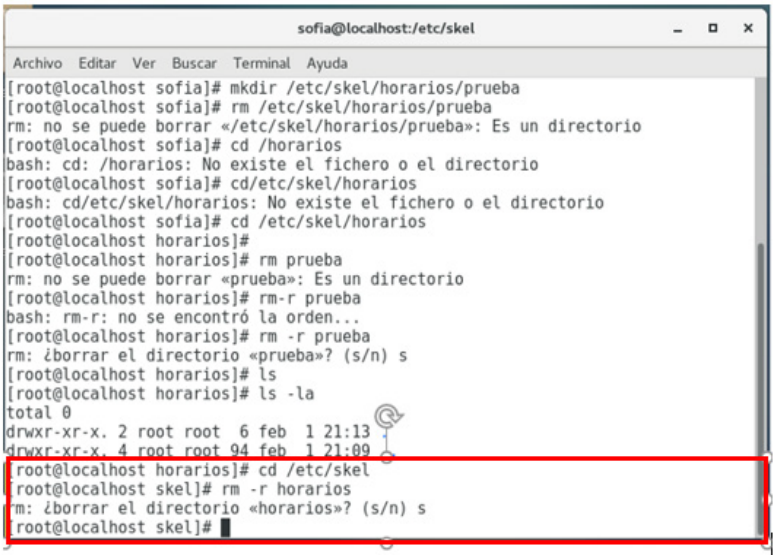


Figura 31: Borrar el directorio horario.

Pasos para el cambio de permisos archivos o directorios

Sintaxis

chmod [Opciones] [permiso_descripción] archivo

Opciones

- c muestra los archivos a los que se les han modificado los permisos.
- f hace que no aparezca en pantalla ningún mensaje de error.
- v muestra los cambios efectuados en los permisos de archivos.
- R cambia los permisos de los archivos de todos los subdirectorios.

```
total 4
drwx------.  5 Clientes Santiago  128 nov  7 13:21 Clientes
drwx------.  4 root     root       93 nov  7 13:48 hola
drwx------. 15 Santiago Santiago 4096 nov  7 13:19 Santiago
[root@localhost home]# usermod -u 0 Santiago
usermod: el UID «0» ya existe
[root@localhost home]# ls -l
total 4
drwx------.  5 Clientes Santiago  128 nov  7 13:21 Clientes
drwx------.  4 root     root       93 nov  7 13:48 hola
drwx------. 15 Santiago Santiago 4096 nov  7 13:19 Santiago
[root@localhost home]# usermod -g 0 Santiago
[root@localhost home]# ls -l
total 4
drwx------.  5 Clientes Santiago  128 nov  7 13:21 Clientes
drwx------.  4 root     root       93 nov  7 13:48 hola
drwx------. 15 Santiago root     4096 nov  7 13:19 Santiago
[root@localhost home]# usermod -g 0 Clientes
[root@localhost home]# ls -l
total 4
drwx------.  5 Clientes root  128 nov  7 13:21 Clientes
drwx------.  4 root     root   93 nov  7 13:48 hola
drwx------. 15 Santiago root 4096 nov  7 13:19 Santiago
[root@localhost home]#
```

Figura 32: Permisos de lectura y escritura de un archivo.

chmod u+xr manual_linux

El usuario tendrá los permisos de lectura y ejecución sobre el archivo manual_linux

Descripción

Para utilizar eficazmente el comando chmod, debe especificarse la configuración de los permisos, utilizando el comando: ls –lrt, conforme lo podemos observar en la figura 33.

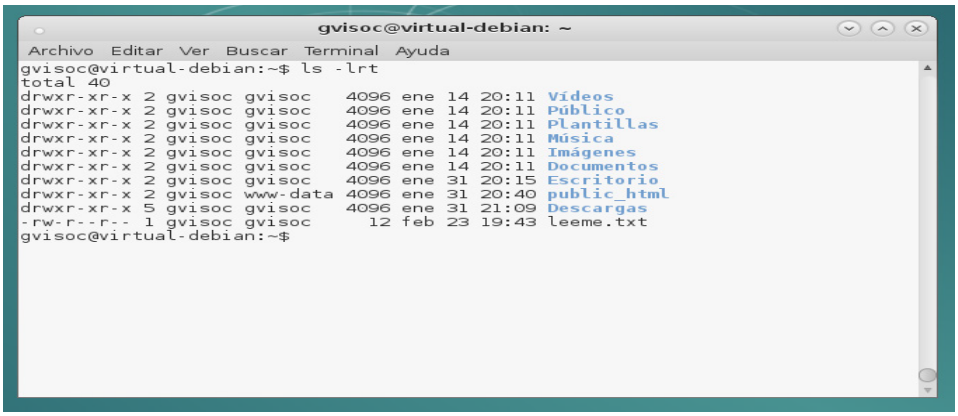


Figura 33: Visualización de los permiso que tienen los direcorios y archivos.

El formato para utilizar chmod es el siguiente:

chmod permiso_usuario permiso_grupo permiso_otros

Ejemplo: supongamos que creamos el archivo permiso. txt y queremos que el usuario tenga todos los permisos, el grupo los permisos de lectura y ejecución y finalmente que el resto de los usuarios tenga sólo el permiso de ejecución.

Para el usuario: lectura r = 4, escritura w = 2, ejecución x =1; sumados = 7

Para el grupo: lectura r= 4, escritura w = 0, ejecución x = 1; sumados = 5

Para el resto de los usuarios: lectura r = 0; escritura w = 0, ejecución x = 1; sumados = 1

El comando sería: chmod 751 permisos.txt

En la lista detallada de los archivos de un directorio (usando el comando ls), el permiso de lectura escritura y ejecución del usuario, grupo y otros se mostrarán a través de la secuencia rwxrwxrwx. Cuando algún permiso no está activado aparece un guion en su reemplazo.

Comando PROC, TOP, FREE, PS

Los procesos juegan un papel muy importante en las distribuciones Linux, ya que son los que consumirán estos recursos en entornos de producción. Por ello, administrarlos y gestionarlos correctamente es de vital importancia, porque estos procesos y la gestión que hace el sistema sobre ellos hacen posible mantener funcionando el servidor, sin necesidad de reiniciar después de un cambio o actualización importante. Esto es uno de los puntos más importantes por los que Linux gobierna el 90% de los servidores alrededor del mundo.

Los procesos son aquellos que ocupan un área de memoria; estos pueden almacenar datos como también almacenar códigos. Se ejecutan bajo un UID y un GID, tienen un número de procesos (PID). Los procesos tienen diferentes estados, como son: running, sleeping, stopped, waiting for a disk, zombie.

/PROC

Variables del kernel, utilizado para leer la información del kernel, configura parámetros del kernel

/proc/meminfo

Utilizando el comando cat /proc/meminfo nos permite observar la información de la memoria utilizada actualmente.

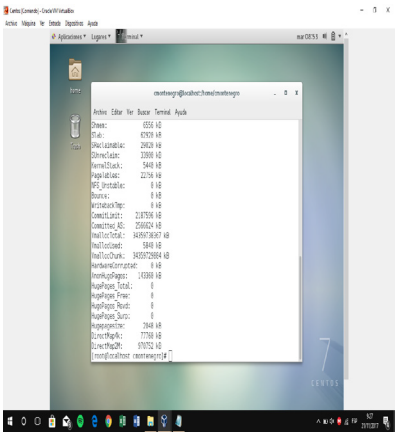


Figura 34: Comando cat /proc/meminfo.

/proc/cpuinfo

Utilizando el comando cat /proc/cpuinfo se puede observar la información tanto del computador como del procesador, un dato interesante es que nos permite ver los "bogomips", los cuales nos dan a conocer la velocidad interna con la que trabaja el CPU.

```
stepping        : 8
cpu MHz         : 2166.658
cache size      : 1024 KB
physical id     : 0
siblings        : 1
core id         : 0
cpu cores       : 1
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 11
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
pat pse36 clflush mmx fxsr sse sse2 syscall nx rdtscp lm constant_tsc rep_good n
opl xtopology nonstop_tsc pni pclmulqdq monitor ssse3 cx16 sse4_1 sse4_2 x2apic
movbe popcnt rdrand hypervisor lahf_lm 3dnowprefetch
bogomips        : 4333.31
clflush size    : 64
cache_alignment : 64
address sizes   : 36 bits physical, 48 bits virtual
power management:
```

Figura 35: comando cat /proc/cpuinfo.

/proc/cmdline

Utilizando el comando cat /proc/cmdline permite identificar la versión del núcleo, además del lenguaje con el cual fue configurado en la instalación.

```
[root@localhost cmontenegro]#
[root@localhost cmontenegro]# cat /proc/cmdline
BOOT_IMAGE=/vmlinuz-3.10.0-514.el7.x86_64 root=/dev/mapper/cl-root ro crashkerne
l=auto rd.lvm.lv=cl/root rd.lvm.lv=cl/swap rhgb quiet LANG=es_EC.UTF-8
[root@localhost cmontenegro]# _
```

Figura 36: comando cat /proc/cmdline.

ls -l /proc/

Determina los procesos que están corriendo en el sistema.

```
[root@localhost cmontenegro]#
[root@localhost cmontenegro]# ls -l /proc/12/
ls: no se puede leer el enlace simbólico /proc/12/exe: N
 directorio
total 0
dr-xr-xr-x. 2 root root 0 nov 21 09:18 attr
-rw-r--r--. 1 root root 0 nov 21 09:18 autogroup
-r--------. 1 root root 0 nov 21 09:18 auxv
-r--r--r--. 1 root root 0 nov 21 09:18 cgroup
--w-------. 1 root root 0 nov 21 09:18 clear_refs
-r--r--r--. 1 root root 0 nov 21 08:28 cmdline
-rw-r--r--. 1 root root 0 nov 21 09:18 comm
-rw-r--r--. 1 root root 0 nov 21 09:18 coredump_filter
-r--r--r--. 1 root root 0 nov 21 09:18 cpuset
lrwxrwxrwx. 1 root root 0 nov 21 09:18 cwd -> /
-r--------. 1 root root 0 nov 21 09:18 environ
lrwxrwxrwx. 1 root root 0 nov 21 09:18 exe
dr-x------. 2 root root 0 nov 21 09:18 fd
dr-x------. 2 root root 0 nov 21 09:18 fdinfo
-rw-r--r--. 1 root root 0 nov 21 09:18 gid_map
-r--------. 1 root root 0 nov 21 09:18 io
-r--r--r--. 1 root root 0 nov 21 09:18 limits
-rw-r--r--. 1 root root 0 nov 21 09:18 loginuid
dr-x------. 2 root root 0 nov 21 09:18 map_files
```

Figura 37: Pantalla con los resulados utilizand el comando ls -l /proc.

FREE

free -m

Determina el consumo de memoria en el servidor y de la memoria swap.

```
[root@localhost cmontenegro]# free -m
              total        used        free      shared  buff/cache   available
Mem:            992         484         136           6         371         329
Swap:          1639           1        1638
[root@localhost cmontenegro]#
```

Figura 38: Comando free -m.

PS

Comando que nos permite visualizar en la pantalla los procesos que se están ejecutando en el sistema.

ps a

Utilizando el comando "**ps a**" podemos ver todos los procesos del terminal. La primera columna PID nos indica el número que tiene el proceso, el estado en el que se encuentra, el tiempo de operación.

```
[root@localhost cmontenegro]# ps a
  PID TTY      STAT   TIME COMMAND
 1045 tty1     Ss+    0:27 /usr/bin/Xorg :0 -background none -noreset -audit 4 -
 4647 pts/0    Ss     0:00 bash
 4694 pts/0    S      0:00 su
 4702 pts/0    S      0:00 bash
 6382 pts/0    R+     0:00 ps a
[root@localhost cmontenegro]# _
```

Figura 39: comando ps a.

ps x

Utilizando el comando "**ps x**" se puede observar todos los procesos que no se encuentran en el terminal.

```
  956 ?        Ssl    0:00 /usr/sbin/gdm
  958 ?        Ss     0:03 /usr/sbin/crond -n
  962 ?        Ss     0:00 /usr/sbin/sshd
 1045 tty1     Ss+    0:28 /usr/bin/Xorg :0 -background none -noreset -audit 4 -
 1545 ?        Ss     0:00 /usr/libexec/postfix/master -w
 1620 ?        S      0:00 /sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/de
 2280 ?        Ss     0:00 /usr/bin/perl /usr/libexec/webmin/miniserv.pl /etc/we
 2341 ?        Ssl    0:00 /usr/libexec/upowerd
 2452 ?        Ssl    0:00 /usr/libexec/packagekitd
 2456 ?        Ss     0:00 /usr/sbin/wpa_supplicant -u -f /var/log/wpa_supplican
 2523 ?        Ssl    0:00 /usr/lib/udisks2/udisksd --no-debug
 2799 ?        Sl     0:01 gdm-session-worker [pam/gdm-password]
 4694 pts/0    S      0:00 su
 4702 pts/0    S      0:00 bash
 5242 ?        Ss     0:00 /usr/sbin/atd -f
 5533 ?        R      0:01 [kworker/0:0]
 5534 ?        S<     0:00 [kworker/0:0H]
 5736 ?        S      0:00 [kworker/0:1]
 5776 ?        S      0:00 [kworker/u2:1]
 6205 ?        S<     0:00 [kworker/0:2H]
 6408 ?        S      0:00 sleep 60
 6409 ?        S<     0:00 [kworker/0:1H]
 6410 pts/0    R+     0:00 ps x
```

Figura 40: comando ps x.

ps f

Utilizando el comando "**ps f**" podemos ver todos los procesos en forma de árbol.

```
[root@localhost cmontenegro]# ps f
  PID TTY      STAT   TIME COMMAND
 4694 pts/0    S      0:00 su
 4702 pts/0    S      0:00  \_ bash
 6608 pts/0    R+     0:00      \_ ps f
 1045 tty1     Ss+    0:28 /usr/bin/Xorg :0 -background none -noreset -audit 4 -
[root@localhost cmontenegro]#
```

Figura 41: comando ps f

ps u

Utilizando el comando "**ps u**" se pueden observar los procesos que están corriendo bajo el sistema.

```
[root@localhost cmontenegro]# ps u
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1045  0.7  2.7 238416 27752 tty1     Ss+  08:29   0:29 /usr/bin/Xorg :
root      4694  0.0  0.3 212204  4048 pts/0    S    08:51   0:00 su
root      4702  0.0  0.2 118228  2828 pts/0    S    08:51   0:00 bash
root      6828 68.0  0.1 151056  1816 pts/0    R+   09:38   0:00 ps u
[root@localhost cmontenegro]#
```

Figura 42: comando ps u

ps aux

Utilizando el comando "**ps aux**" podemos ver el tamaño de memoria utilizada por cada proceso.

```
cmonten+  3266  0.0  1.6 754804 16352 ?        Sl   08:32   0:00 /usr/bin/gnome-
cmonten+  3269  0.0  1.2 644928 12748 ?        SNl  08:32   0:00 /usr/libexec/tr
cmonten+  3270  0.0  0.9 470236  9808 ?        SNl  08:32   0:00 /usr/libexec/tr
cmonten+  3275  0.0  1.0 636824 11152 ?        SNl  08:32   0:00 /usr/libexec/tr
cmonten+  3319  0.0  0.6 471848  6232 ?        Sl   08:32   0:00 /usr/libexec/gv
cmonten+  3372  0.0  4.7 1006512 47868 ?       Sl   08:32   0:01 /usr/libexec/ev
cmonten+  3417  0.0  0.3 319544  3904 ?        Sl   08:32   0:00 /usr/libexec/ib
cmonten+  3495  0.0  0.2 178508  2592 ?        Sl   08:33   0:00 /usr/libexec/dc
cmonten+  3985  0.0  0.3 312708  3372 ?        Sl   08:41   0:00 /usr/libexec/gv
cmonten+  4642  0.3  1.9 555272 20044 ?        Sl   08:50   0:09 /usr/libexec/gn
cmonten+  4646  0.0  0.0   8480   708 ?        S    08:50   0:00 gnome-pty-helpe
cmonten+  4647  0.0  0.2 118224  2780 pts/0    Ss   08:50   0:00 bash
root      4694  0.0  0.3 212204  4048 pts/0    S    08:51   0:00 su
root      4702  0.0  0.2 118228  2828 pts/0    S    08:51   0:00 bash
root      5242  0.0  0.0  25844   916 ?        Ss   09:02   0:00 /usr/sbin/atd -
root      5533  0.0  0.0      0     0 ?        S    09:08   0:01 [kworker/0:0]
root      5736  0.0  0.0      0     0 ?        S    09:13   0:00 [kworker/0:1]
root      5776  0.0  0.0      0     0 ?        S    09:14   0:00 [kworker/u2:1]
root      6409  0.0  0.0      0     0 ?        S<   09:29   0:00 [kworker/0:1H]
root      6500  0.0  0.0      0     0 ?        R    09:31   0:00 [kworker/0:2]
root      6636  0.0  0.0      0     0 ?        S<   09:35   0:00 [kworker/0:0H]
root      6854  0.0  0.0 107896   604 ?        S    09:39   0:00 sleep 60
root      6871  0.0  0.1 151056  1812 pts/0    R+   09:40   0:00 ps aux
[root@localhost cmontenegro]#
```

Figura 43: comando ps aux

TOP

Cumple la misma función que el ps solo que se refresca a intervalos (c3/S)

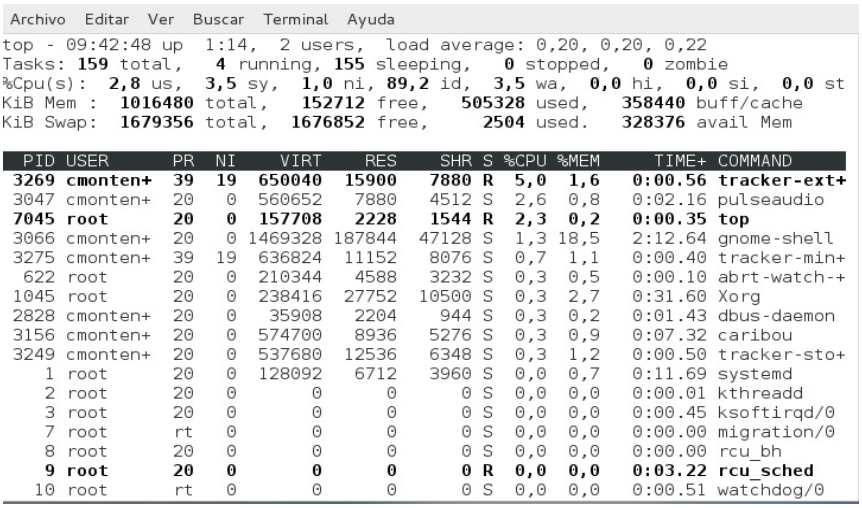


Figura 44: Función Top

Recuperación de la clave root

A continuación de presenta la recuperación de la clave root mediante líneas de código. En primer lugar, se debe dejar en claro que esto no es un fallo de seguridad de Linux, sino una funcionalidad para iniciar el equipo en caso de emergencias. Sin embargo, en caso de utilizarlo en un entorno crítico, como un servidor de una empresa, la seguridad se debe complementar con otras medidas de seguridad, acceso restringido al equipo, contraseña en la BIOS y contraseña en el GRUB.

Pasos de recuperación

Paso 1 : Lo que hacemos es reiniciar al equipo y al cargar GRUB para escoger el sistema operativo; nos colocamos en la que corresponde a nuestra distribución y pulsamos la tecla “e”, que nos direccionará a un menú para entrar al modo de edición.

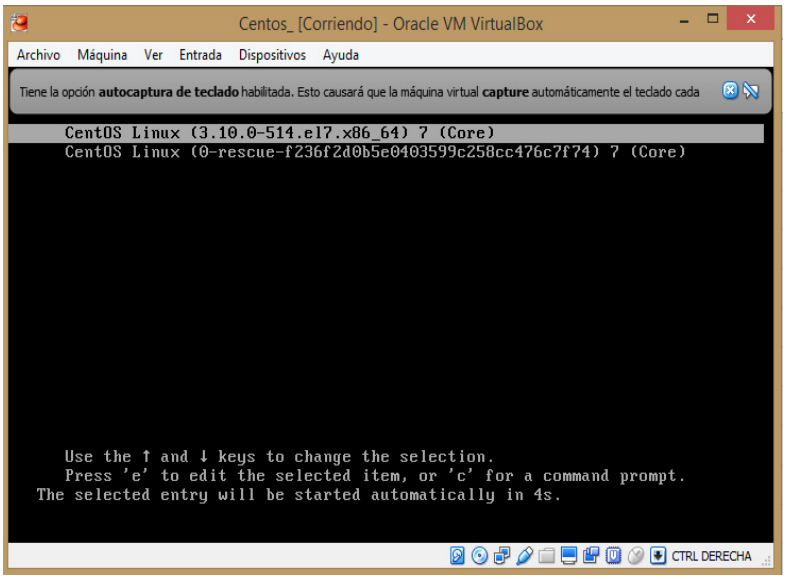


Figura 45: Ventana de carga de centos en GRUB

Paso 2: A continuación procedemos a pulsar:

Ctrl + x

Se reinicia el sistema y arranca nuevamente el sistema.

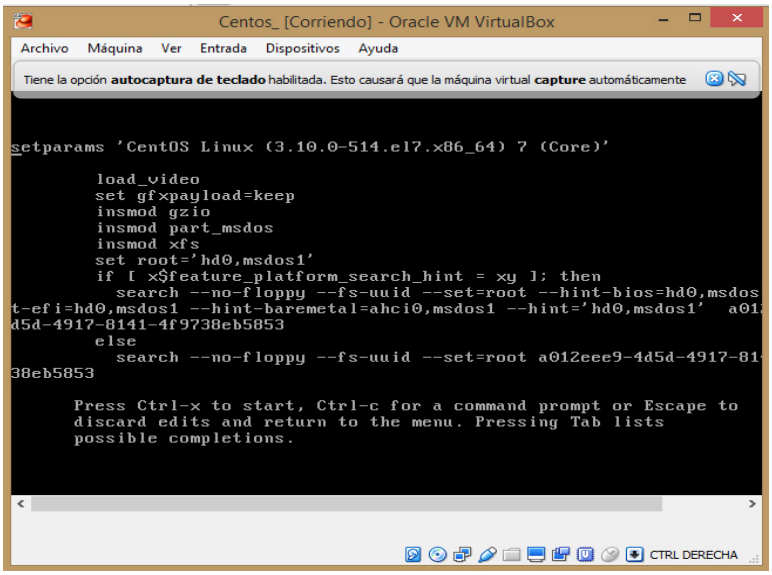


Figura 46: Reinicio de sistema.

Paso 3: Una vez reiniciado, ubicaremos la línea linux16 donde podemos visualizar la palabra **root** que tendremos que cambiar por lo siguiente:

rw init=/sysroot/bin/sh y tecleamos el comando

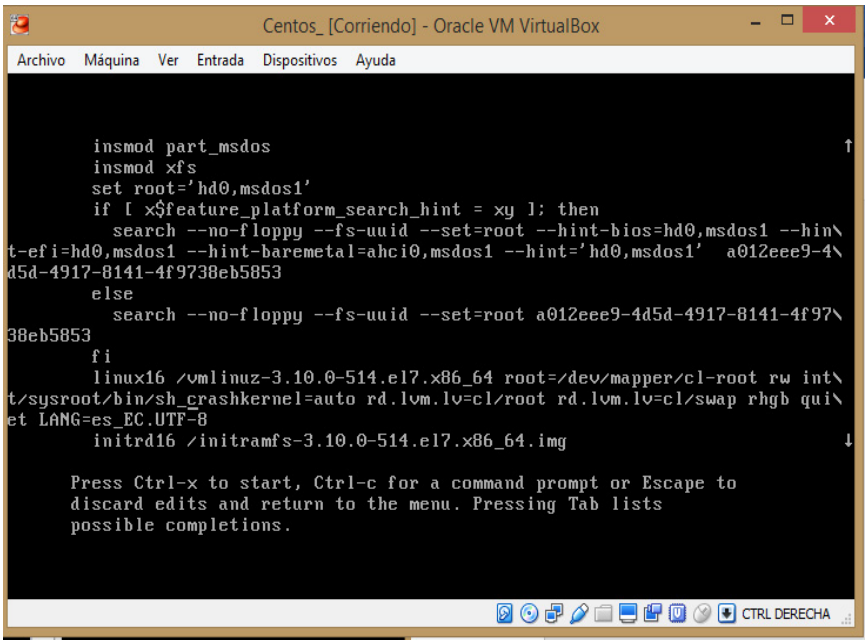


Figura 47: Ya reiniciado el sistema

A continuación procedemos a pulsar:

Ctrl + x

Se reinicia el sistema y arranca el sistema.

Paso 4:

Escribimos **chroot /sysroot** para iniciar el cambio de la contraseña en el **bin**

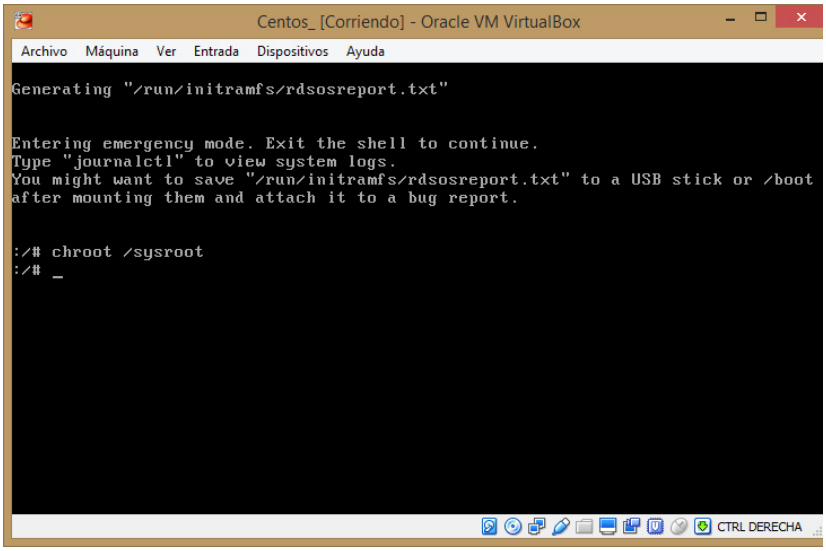


*Figura 48: Ventana del cambio de la contraseña en el **bin**.*

Paso 5: En el siguiente paso digitamos el comando:

passwd root + Enter

Escribimos la nueva contraseña, repetimos la contraseña para que compruebe que son iguales.

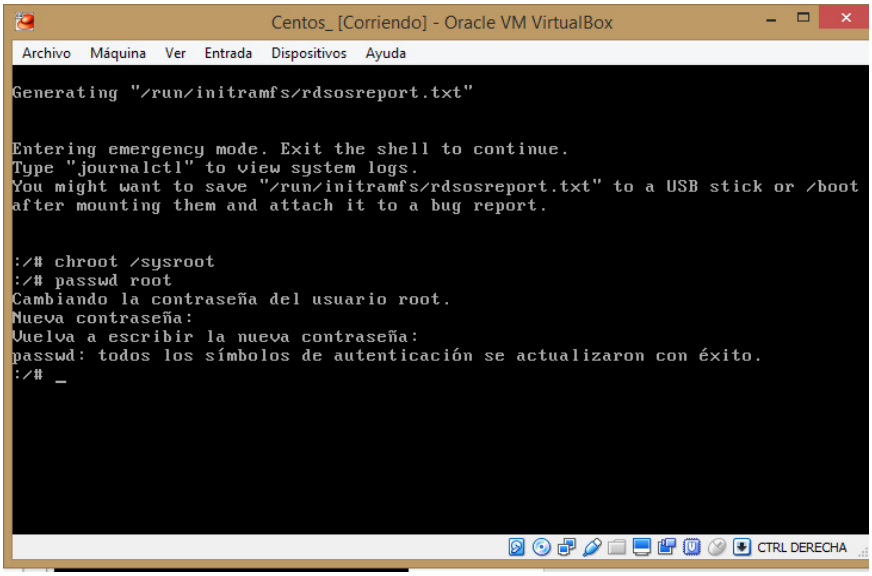


Figura 49: Ventana del cambio de contraseña.

Paso 6: Podemos ver que la contraseña se ha actualizado correctamente. Ahora el otro paso es actualizar la información selinux ejecutando el siguiente comando:

Escribimos el comando **touch /. autorelabel** para guardar los cambios

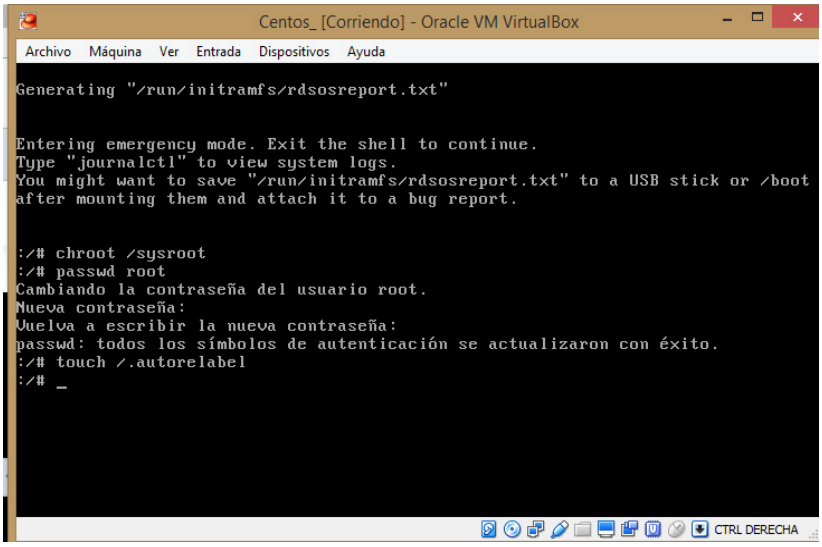


Figura 50: Ventana en donde guardamos los cambios realizados.

Paso 7: Escribimos **exit** para salir del editor. Digitamos **reboot** para reiniciar el sistema, y ya tememos cambiada la contraseña.

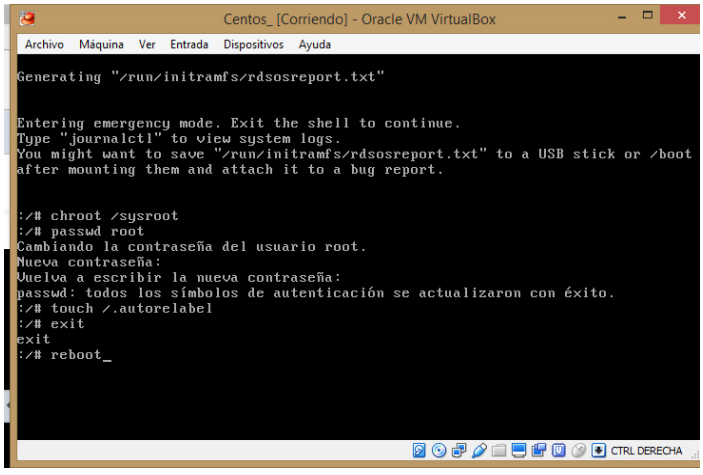


Figura 51: reiniciamos el sistema una vez cambiada la contraseña.

El momento que iniciemos el **súper usuario** ya tenemos que ingresar con la nueva contraseña.

Partición de HDD en Centos 7.0

Al igual que dentro de los sistemas operativos Windows, donde encontramos un disco C:/ y D:/, por lo general el primero es donde se carga el sistema operativo y el segundo destinado a almacenamiento, podemos tener en Linux específicamente en Centos 7.0 particiones de disco, para gestionar de mejor manera nuestros archivos, según lo vayamos a requerir. Dentro de Linux es sabido que la mayor parte de acciones son realizadas a través de consola o, como le conocemos mejor, la "Terminal".

Lista de Comandos

fdisk (válido para fixed disk o format disk) es uno de los comandos más importantes que deberíamos conocer, puesto que en caso de no contar con interfaz gráfica de por medio (cosa muy habitual en las distribuciones destinadas a servidores por el mejor aprovechamiento de los recursos).

fdisk –l.- Muestra todas las particiones existentes en nuestro sistema, pasaremos el argumento "-l", que hará que se listen ordenadas por el nombre del dispositivo.

fdisk –l /dev/sdb. - Para ver todas las particiones de un único disco, al comando anterior añadiremos el nombre de dicho disco.

Si queremos ver todas las opciones que nos ofrece fdisk, únicamente deberemos pasar el comando seguido de una unidad de disco (para darle algo sobre lo que trabajar).

fdisk /dev/sdb. - Una vez estemos en el menú de fdisk, pulsaremos 'n' (new o nueva) para crear la nueva partición. Lo siguiente que nos pedirá será que tipo de partición deseamos crear, extendida (también llamada lógica) o primaria.

mkfs. ext4 /dev/sdb5.- Mediante ext4 le estamos indicando a la aplicación que formato de archivos nos interesa aplicar a la partición, se ha elegido sdb5 (otro valor que podrá variar en su sistema) por seguir con el ejemplo anteriormente usado.

fdisk /dev/sdb. - A continuación, ya dentro del menú, pulsamos 'x' para acceder a las opciones avanzadas de fdisk. Lo siguiente que haremos será pulsar 'f' (fix) que indicará a la aplicación que queremos reparar la tabla de particiones. Pulsaremos 'w' para escribir los datos.

Borrar una partición

Si lo que queremos es borrar una partición en concreto (por ejemplo, /dev/sdb2), primeramente, deberemos seleccionar el disco en el que podemos encontrarla, que siguiendo el caso del ejemplo sería /dev/sdb.

Crear una nueva partición

Si contamos con espacio sin usar en nuestro disco duro, podemos asignar ese espacio a una nueva partición. Como en las anteriores acciones, primeramente, deberemos acceder al menú pasando como argumento el nombre del disco duro sobre el que queremos trabajar.

Formatear una partición

Después de haber creado una nueva partición, no debemos olvidar darle formato.

Comprobar el tamaño de una partición

Después de formatear la partición, podremos comprobar el tamaño que le asignamos mediante el argumento '-s' que nos mostrará los bloques que ocupa la misma.

Corregir la tabla de particiones

Se nos puede plantear la situación de que borramos particiones intermedias, por ejemplo, si tenemos particionado el disco con sda1, sda2, sda3, sda4 y sda5; y tenemos que eliminar sda3 y sda4. Esto puede ocasionar recibir un error como este "Partition table entries are not in disk order".

Pasos a seguir

Paso 1: Antes de todo, hay que asignar una unidad de almacenamiento en la máquina virtual.

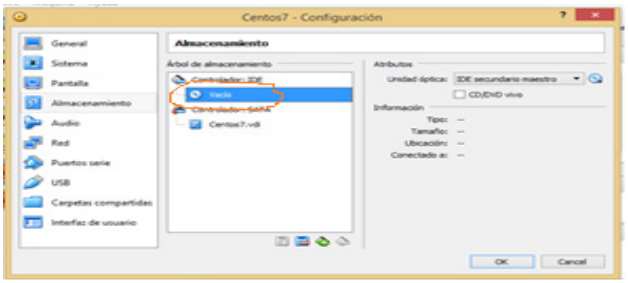


Figura 52: Terminal de Centos 7.0

Iniciamos asignando a la máquina que está en la parte interna del simulador un nombre donde vamos a crear la partición nueva.

Paso 2: Abrir la terminal de Centos 7.0 para ejecutar los comandos mencionados en la lista de comandos.

Paso 3: Ejecutamos fdisk -l en el terminal.

fdisk -l para ver todas las unidades que tenemos en nuestro sistema

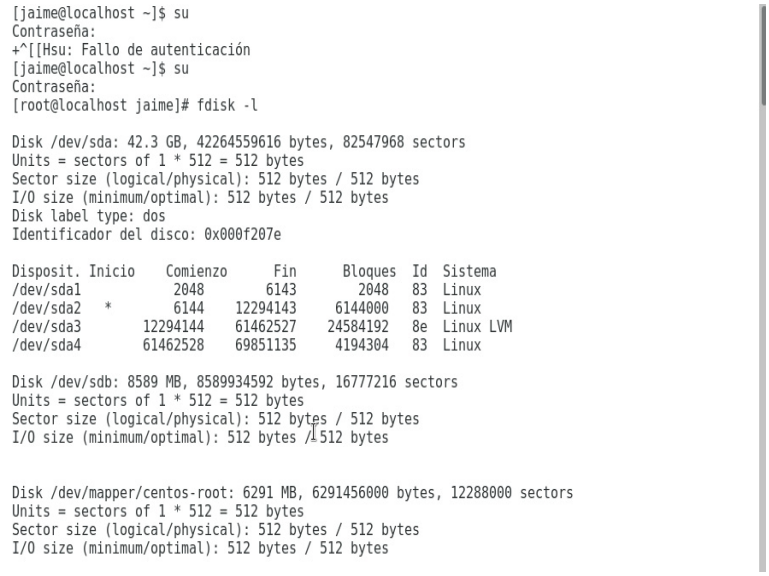


Figura 53: Comando fdisk -l en el terminal.

Paso 4: En esta parte nos colocamos en el disco que creamos anteriormente en el Paso 1 en la máquina virtual, que en este caso Fdisk /dev/sdb sirve para seleccionar la unidad que creamos y empezar a asignarle espacio.

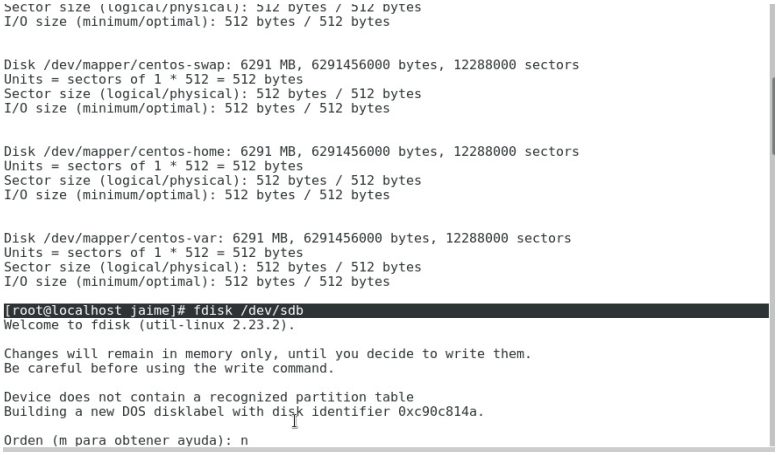


Figura 54: Fdisk /dev/sd.

Paso 5: En esta parte asignamos una partición de tipo primaria y le asignamos todo en espacio del disco

***P*=** partición primaria

***E*=** partición extendida

```
Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0xc90c814a.

Orden (m para obtener ayuda): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Número de partición (1-4, default 1): 1
Primer sector (2048-16777215, valor predeterminado 2048): 2048
Last sector, +sectors or +size{K,M,G} (2048-16777215, valor predeterminado 16777215): 16777215
Partition 1 of type Linux and of size 8 GiB is set

Orden (m para obtener ayuda): w
¡Se ha modificado la tabla de particiones!

Llamando a ioctl() para volver a leer la tabla de particiones.
Se están sincronizando los discos.
[root@localhost jaime]# fdisk -l

Disk /dev/sda: 42.3 GB, 42264559616 bytes, 82547968 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Identificador del disco: 0x000f207e
```

Figura 55: Partición Primaria.

Paso 6: En este paso procedemos a formatear nuestra unidad creada.

```
Disk /dev/sda: 42.3 GB, 42264559616 bytes, 82547968 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Identificador del disco: 0x000f207e

Disposit. Inicio    Comienzo      Fin      Bloques  Id  Sistema
/dev/sda1            2048        6143        2048   83  Linux
/dev/sda2   *        6144    12294143     6144000   83  Linux
/dev/sda3        12294144    61462527    24584192   8e  Linux LVM
/dev/sda4        61462528    69851135     4194304   83  Linux

Disk /dev/sdb: 8589 MB, 8589934592 bytes, 16777216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Identificador del disco: 0xc90c814a

Disposit. Inicio    Comienzo      Fin      Bloques  Id  Sistema
/dev/sdb1            2048    16777215     8387584   83  Linux

Disk /dev/mapper/centos-root: 6291 MB, 6291456000 bytes, 12288000 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Figura 56: Formateo.

Paso 7: Para poder utilizar la nueva partición, lo primero que se hace es formatear; para ello se utiliza el comando mkfs con el tipo de extensión de la partición y la ubicación de esta juntamente con el nombre de la partición.

```
[root@localhost jaime]# mkfs.ext4 /dev/sdb1
mke2fs 1.42.9 (28-Dec-2013)
Etiqueta del sistema de ficheros=
OS type: Linux
Tamaño del bloque=4096 (bitácora=2)
Tamaño del fragmento=4096 (bitácora=2)
Stride=0 blocks, Stripe width=0 blocks
524288 inodes, 2096896 blocks
104844 blocks (5.00%) reserved for the super user
Primer bloque de datos=0
Número máximo de bloques del sistema de ficheros=2147483648
64 bloque de grupos
32768 bloques por grupo, 32768 fragmentos por grupo
8192 nodos-i por grupo
Respaldo del superbloque guardado en los bloques:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: hecho
Escribiendo las tablas de nodos-i: hecho
Creating journal (32768 blocks): hecho
Escribiendo superbloques y la información contable del sistema de ficheros: hecho
```

Figura 57: Utilización el comando mkfs

Paso 8: Una vez ubicada la partición, lo que hacemos es montarla con el comando mount /dev/sbd1/mnt y nos proyectará en la pantalla la afirmación que la partición está montada.

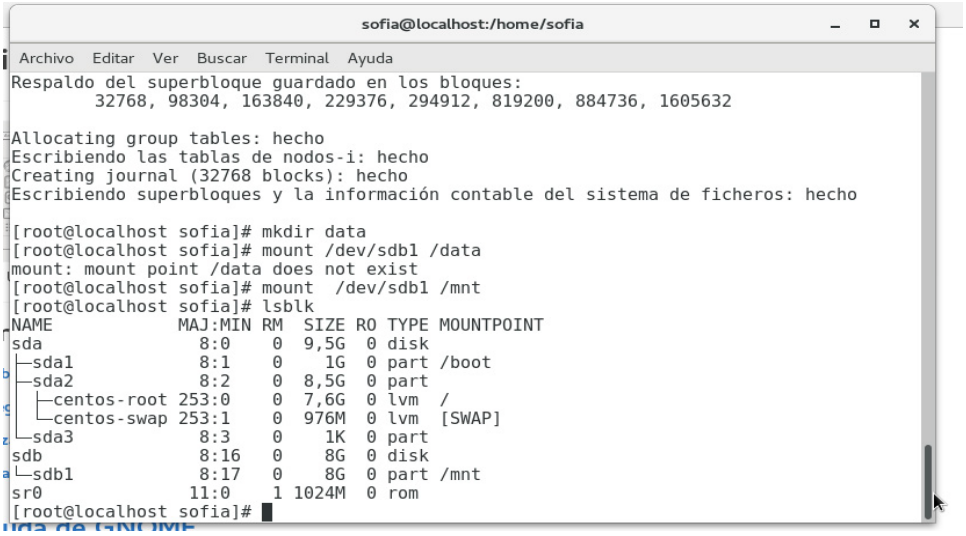


Figura 58: Aplicación de comando mount /dev/sbd1/mnt

Paso 9: Para que la partición sea permanente se debe utilizar un comando vim /etc/fstb, con el cual se desplegará otra pantalla en donde tendremos que poner el disco en los tipos de particiones permanente; esto se hace de forma manual a través del siguiente comando:

vim /etc/fstab

Paso 10: Vim /etc/fstab sirve para crear el sistema de ficheros. Para poder insertar la partición, lo que hacemos es dar clic en la vocal i para poder insertar y seguidamente escribimos /dev/sdb1 defaults 00 y hacemos enter.

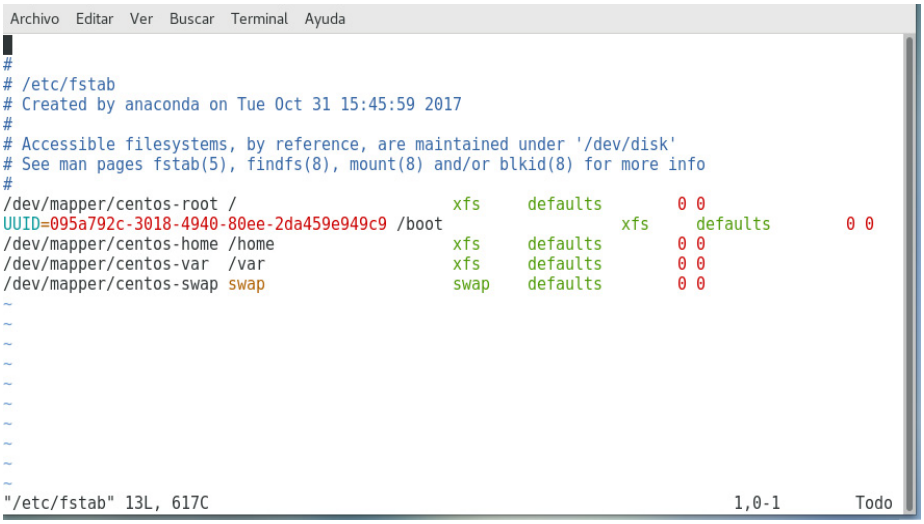


Figura 59: Aplicación de Vim /etc/fstab.

Paso 10: Para poder guardar estos cambios presionamos las teclas esc:wq y regresaremos a la pantalla inicial.

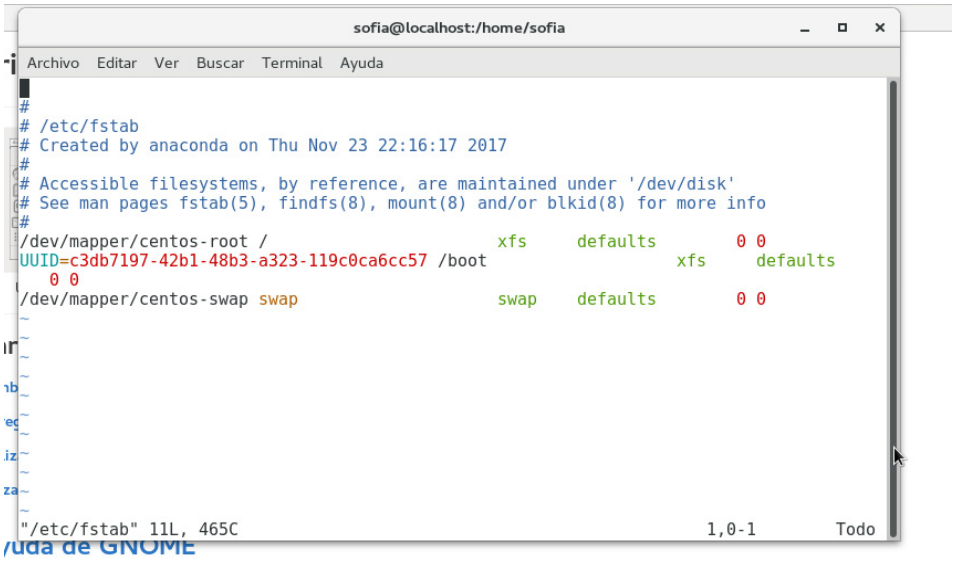


Figura 60: Guardar cambios

Paso 11: Aquí verificamos si creamos correctamente la partición.

```
[root@localhost jaime]# mkdir DIRECTORIODATA
[root@localhost jaime]# mount /dev/sdb1 /DIRECTORIODATA
mount: mount point /DIRECTORIODATA does not exist
[root@localhost jaime]# mount /dev/sdb1 /mnt
[root@localhost jaime]# lsblk
NAME            MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda               8:0    0 39,4G  0 disk
├─sda1            8:1    0    2M  0 part
├─sda2            8:2    0  5,9G  0 part /boot
├─sda3            8:3    0 23,5G  0 part
│ ├─centos-root 253:0    0  5,9G  0 lvm  /
│ ├─centos-swap 253:1    0  5,9G  0 lvm  [SWAP]
│ ├─centos-home 253:2    0  5,9G  0 lvm  /home
│ └─centos-var  253:3    0  5,9G  0 lvm  /var
└─sda4            8:4    0    4G  0 part
sdb               8:16   0    8G  0 disk
└─sdb1            8:17   0    8G  0 part /mnt
sr0              11:0    1 1024M  0 rom
[root@localhost jaime]# vin /etc/fstab
bash: vin: no se encontró la orden...
[root@localhost jaime]# vin /etc/fstab
bash: vin: no se encontró la orden...
[root@localhost jaime]# vim /etc/fstab
```

Figura 61: Ventana que nos indica la partición creada.

Configuración de interfaces de red en Centos 7.0

Esta interfaz ofrece un conjunto de operaciones que son las mismas para todos los tipos de hardware y, básicamente, trata con el envío y la recepción de paquetes. Los nombres de las interfaces son diferentes, y es importante identificarlas; para ello puede utilizar el comando **ip add** en el que solicitará la dirección IP del sistema y en la salida del comando se mostrará el nombre de cada interfaz.

Pasos para la configuración:

Paso 1: Ejecutamos el comando ip add en nuestra consola:

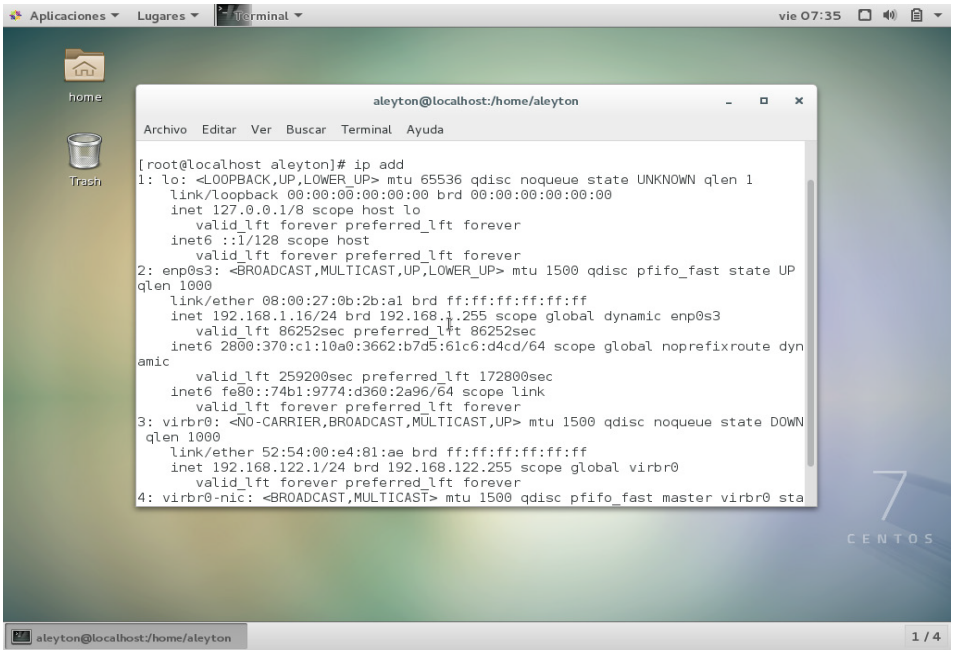


Figura 62: Interfaces de Red

Como se puede observar en pantalla, la salida de este comando es posible que no vea ninguna interfaz eth0 o eth1 como en versiones anteriores de CentOS, en vez de esto verá secuencias como la del ejemplo “enp0s3.

Estos nuevos identificadores se crean son base en ciertas reglas y patrones que ahora se tienen en cuenta para nombrar los dispositivos de red.

Paso 2: El siguiente paso por realizar es localizar el archivo de configuración de la interfaz que se va a modificar, por lo que se debe ir a la siguiente **ruta: /etc/sysconfig/network-scripts/**

Paso 3: Una vez ahí se buscará el archivo con el nombre que se habrá localizado anteriormente con el comando "ip add", en este ejemplo es enp0s3; y se lo hace con el comando "ls"

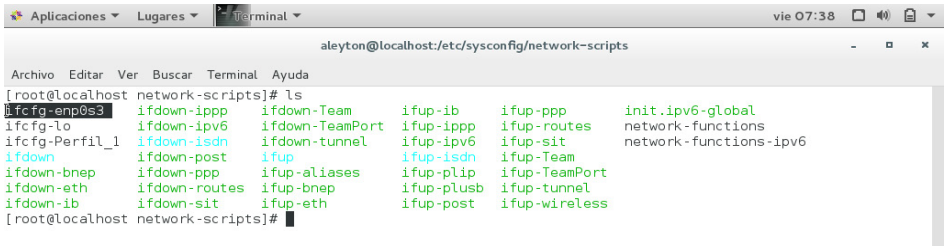


Figura 63: Interfaz de configuración.

Este archivo llamado ifcfg-enp0s3 se encuentra la configuración de la interfaz de red y se lo debe editar con el comando: "nano ifcfg-enp0s3".

Los parámetros en este archivo deben ser editados según lo que indique su proveedor de internet; o si es un servidor de prueba, el administrador puede determinar una IP adecuada para su red local.

BOOTPROTO: determina el tipo de configuración que tiene la interfaz, puede ser none (ninguna), static (estática) o dhcp (asignación de ip dinámica por dhcp) por lo general en un servidor siempre se debe configurar como static.

IPV6INIT e IPV6_AUTOCONF indica si desea activar el protocolo IP versión 6 y que se autoconfigure, en el ejemplo seleccionamos que no lo usaremos y que no se configure.

ONBOOT: si la interfaz de red que estás configurando debe de levantarse de forma automática cuando arranca el servicio network, entonces debe configurar esta opción como "yes", de lo contrario el servidor arrancará y la interfaz permanecerá desactivada hasta que manualmente la active. Recuerde que Centos 7.0 siempre configura esta opción como "no", por lo que no tendrá conexión a la red por default en la interfaz de red.

IPADDR0: es la primera dirección IP de la interfaz, recuerde que puede haber varias.

PREFIX0: es el pefijo de red, antes llamado NETMASK de la primera IP, recuerde que puede haber varias.

GATEWAY0: es la puerta de enlace o la pasarela de la primera IP y puede haber varias.

DNS1: es la dirección IP del servidor de resolución de nombres de dominio

Paso 4: Se debe desactivar el Network Manager.

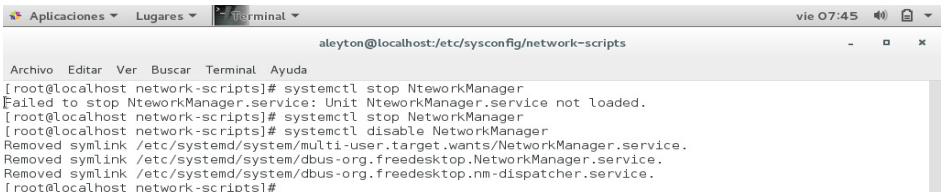


Figura 64: Network Manager.

Por último, se debe reiniciar el servicio de red con el comando: "systemctl restart ntework. service".

Y en este momento se debe tener activa la interfaz de red con la ip que se haya configurado. Para verificar el estado de la interfaz de red hay que ejecutar el comando ip add show, así:

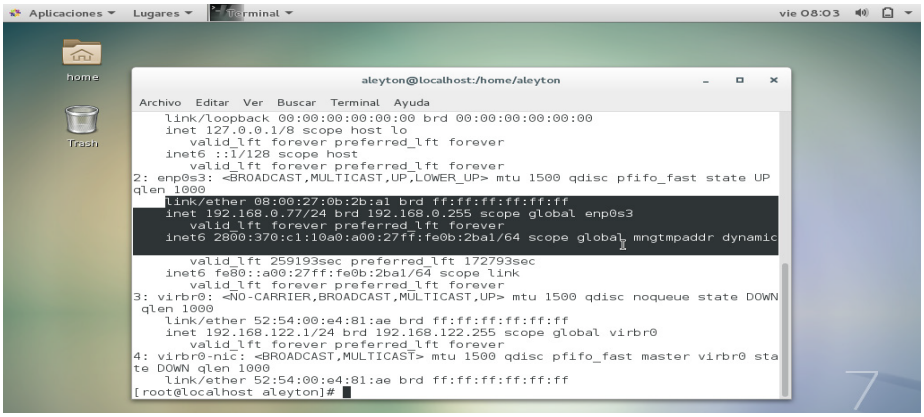


Figura 65: Comando ip add show.

Configuración de un Servidor FTP en Centos 7.0

FTP significa "File Transfer Protocol", Protocolo para la Transferencia de Archivos; un servidor FTP es un programa especial que se ejecuta en un servidor conectado normalmente en Internet (aunque puede estar conectado en otros tipos de redes, LAN, MAN, etc.). Su función es permitir el desplazamiento de datos entre diferentes servidores / ordenadores.

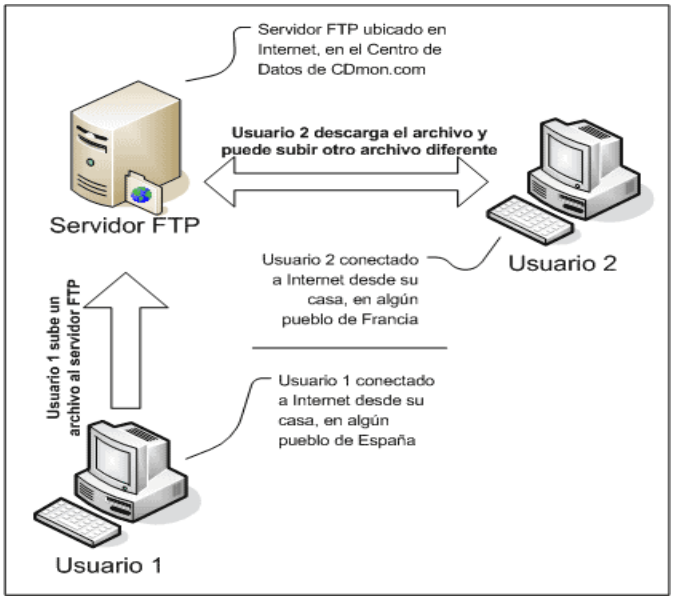


Figura 66: Diagrama FTP.

El servicio FTP

Permite implementar servicios de archivos mediante protocolo FTP, caracterizándose principalmente porque se trata de un sistema muy seguro, a la vez muy sencillo de configurar. Se puede instalar el paquete correspondiente, al servidor vsftpd, en un ordenador con Linux, desde el terminal, se distribuye bajo licencia libre GNU GPL

Instalación servidor FTP

Paso 1: Para la Instalación vsftpd usaremos el siguiente comando:

Comando: yum -y install vsftpd

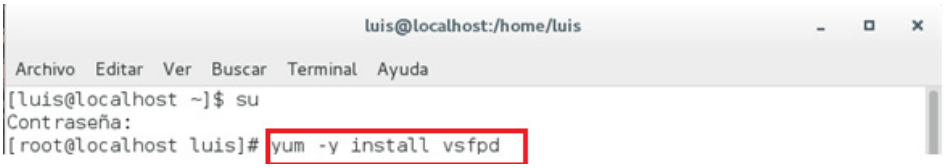


Figura 67: Descarga de los paquetes del servidor.

Paso 2: A continuación, accederemos al archivo de configuración usando el editor vim; para ello, ingresamos esta línea y veremos lo siguiente, con el comando:

Comando: vim /etc/vsftpd/vsftpd.conf

y editamos lo siguiente

allow_writeable_chroot=YES

pasv_enable=Yes

pasv_min_port=40000

pasv_max_port=40100

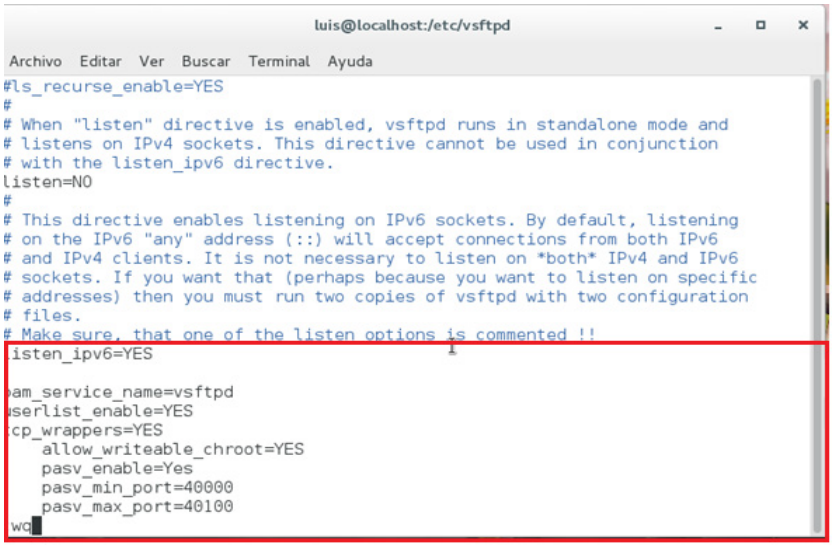


Figura 68: Vista de edición del archivo vsftpd.conf.

Paso 3: Reiniciamos el servicio con el comando:

Comando: systemctl restart vsftpd.service

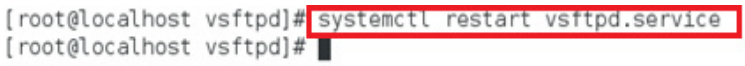


Figura 69: Vista de reinicio del servicio.

Paso 3: Ensamblamos el servicio para que se ejecute correctamente con el comando:

Comando: systemctl enable vsftpd.service

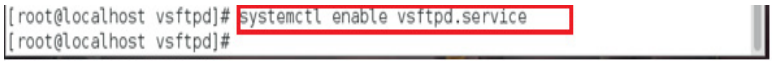


Figura 70: vista de ensamblado del servicio.

Paso 4: Se tiene que permitir que el Firewall habilite el acceso vía FTP; ingresamos el siguiente comando: **Comando: firewall-cmd --permanent --add-service=ftp**

```
[root@localhost vsftpd]# firewall-cmd --permanent --add-service=ftp
Warning: ALREADY_ENABLED: ftp
success
[root@localhost vsftpd]#
```

Figura 71: vista del permiso de acceso del firewall.

Paso 5: Posteriormente recargamos el servicio usando el comando:

Comando: firewall-cmd –reload

```
[root@localhost vsftpd]# firewall-cmd --reload
success
[root@localhost vsftpd]#
```

Figura 72: vista del reinicio del firewall.

Paso 6: Recordemos que SELinux (Security-Enhanced Linux) es un módulo de seguridad que permite aplicar políticas de seguridad para el acceso de los usuarios. Para habilitarlo en Centos 7.0 ingresaremos el siguiente comando:

Comando: setsebool -P ftp_home_dir on

```
[root@localhost vsftpd]# setsebool -P ftp_home_dir on
setsebool:  SELinux is disabled.
[root@localhost vsftpd]#
```

Figura 73: vista del aplicar las políticas de Linux.

De esta forma hemos habilitado permisos de FTP dentro de Centos 7.0

Crear el usuario para el acceso por FTP

Para poder gestionar correctamente los permisos de los usuarios, crearemos usuarios locales en el servidor, para así gestionar los permisos de acceso, pudiendo utilizar y transferir documentos de un lado a otro entre cliente y servidor.

A continuación, crearemos el usuario cliente1 el cual será el usuario a utilizar para acceder vía FTP a Centos 7.0, y lo crearemos en la ruta /sbin/nologin para evitar que el Shell acceda al servidor

Paso 1: En este caso ingresaremos lo siguiente:

Comandos: useradd -m cliente1 -s /sbin/nologin

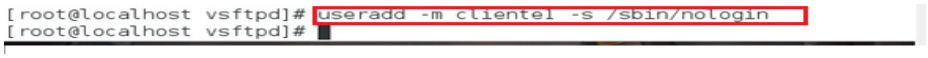


Figura 74: Creación del de un nuevo usuario

Paso 2: Establecemos la contraseña usando el comando: **passwd cliente1**

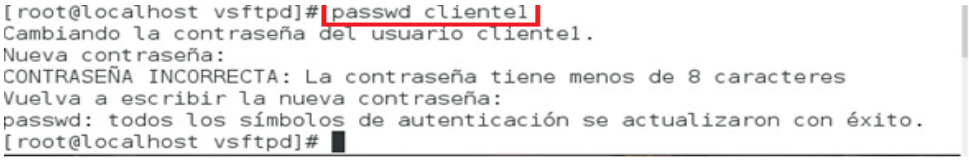


Figura 75: cambio de contraseña del cliente1.

CAPÍTULO 2:
INTRODUCCIÓN A SAMBA



En este capítulo usted encontrará:

- *Introducción a Samba 4.6.2.*
- *Funcionamiento de Samba 4.6.2.*
- *Instalación de Samba 4.6.2*
- *Permisos locales adecuados para los recursos compartidos.*
- *Gestión de usuarios, grupos y permisos.*

Introducción

Samba es una implementación de código abierto del protocolo Server Message Block (SMB), corresponde a un protocolo de red perteneciente a la capa de aplicación en el modelo OSI, desarrollado por IBM en sus inicios. Actualmente el desarrollo es continuado por Microsoft. Samba nos permite compartir archivos, información y/o equipos entre nodos de una red de computadores que usan principalmente un sistema operativo Microsoft Windows. Samba es una implementación del protocolo SMB, junto con otros protocolos de Capa de aplicación, orientado a sistemas operativos Unix/GNU-Linux, con la finalidad, al igual que el protocolo SMB, de compartir archivos e información con sistemas Windows.

Funcionamiento Samba 4.6.2

Implementa los protocolos NetBIOS y SMB. A su vez utiliza dos demonios (programas que se ejecutan en segundo plano): smbd y nmdb: [Ref4]

- Smdb (Samba Daemon): Permite la compartición de archivos e impresoras sobre una red SMB, y proporciona autentificación y autorización de acceso para clientes SMB; ofrece los dos modos de compartición de recursos existentes en Windows: o Modo basado en usuarios o modo user (propio de los dominios Windows NT

o 2000) o Modo basado en recursos o modo share (propio de Windows 3.11/95)

- Nmdb (Network Management DataBase): Permite que el sistema Unix participe en los mecanismos de resolución de nombres propios de Windows (WINS), lo que incluye: o anuncio en el grupo de trabajo o gestión de la lista de ordenadores del grupo de trabajo o contestación a peticiones de resolución de nombres o anuncio de los recursos compartidos.

Pasos para la Instalación de Samba 4.6.2

Utilizamos el comando "yum install samba samba-client".

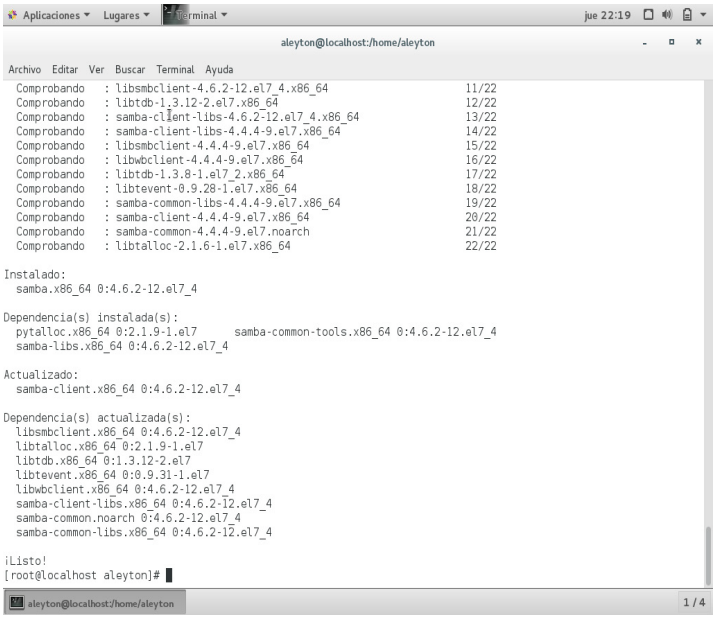


Figura 76: Proceso de Intalación de Samba.

Una vez instalado, habilitamos utilizamos los comandos "systemctl start smb" y "systemctl enable smb", para habilitar el servicio de Samba.

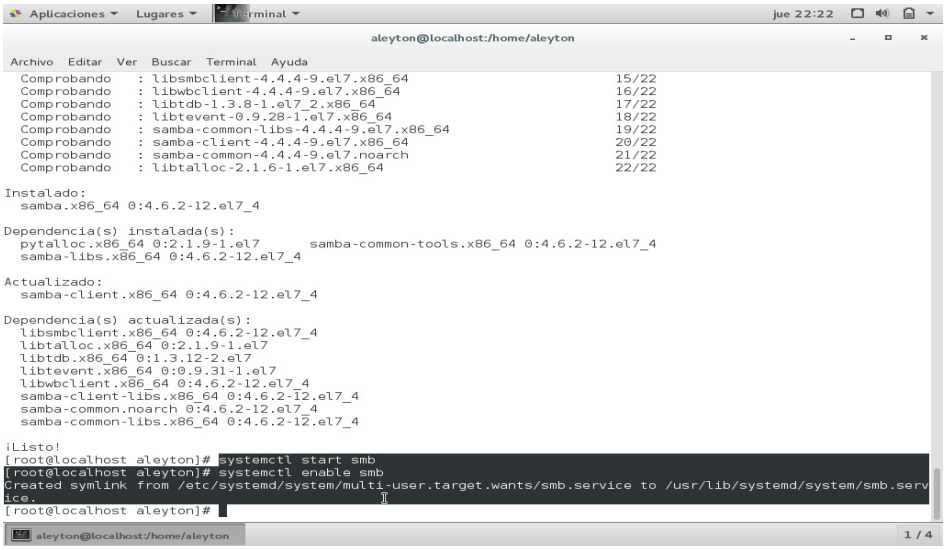


Figura 77: Inicio y habilitación de Samba.

Mediante el comando "smbclient –L 127.0.0.1", ingresamos de forma anónima en Samba y podemos observar los usuarios que se tiene creado.

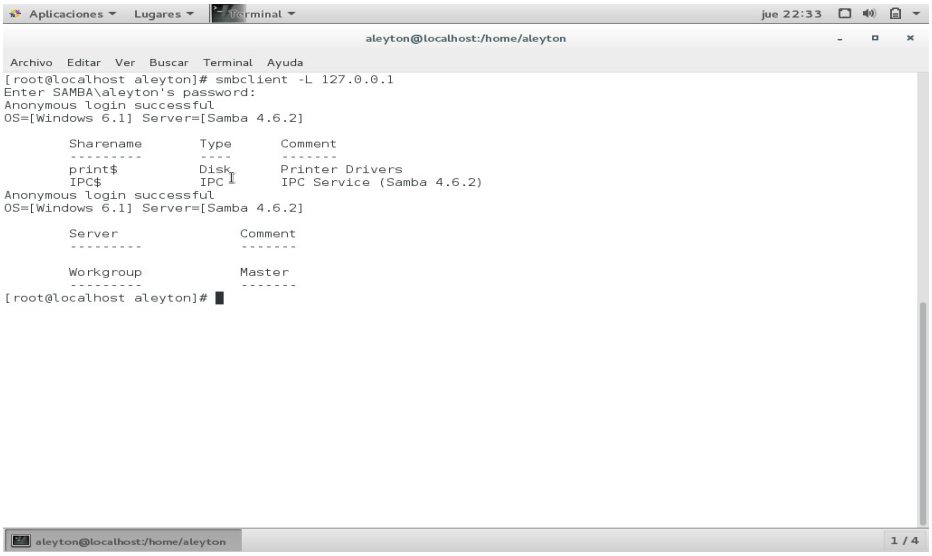


Figura 78: Usuarios de Samba.

Con el comando "useradd –s /sbin/nologin (nombre del usuario)" creamos un nuevo usuario y con el comando "passwd (nombre del usuario)", asignamos una contraseña al usuario creado.

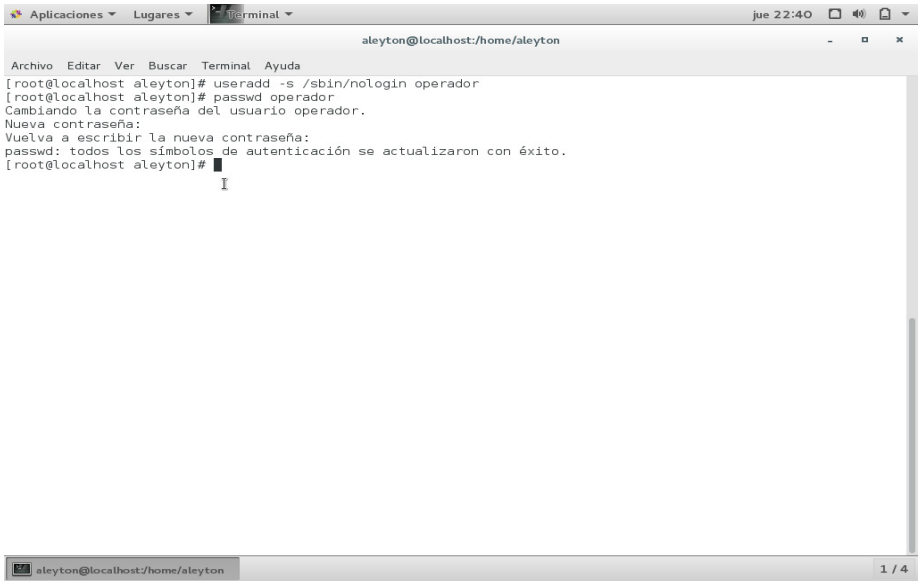


Figura 79: Contraseña asignada al usuario operador.

Con el comando "smbpasswd –L –a (nombre del usuario)", añadimos un nuevo usuario en Samba y asignamos una contraseña.

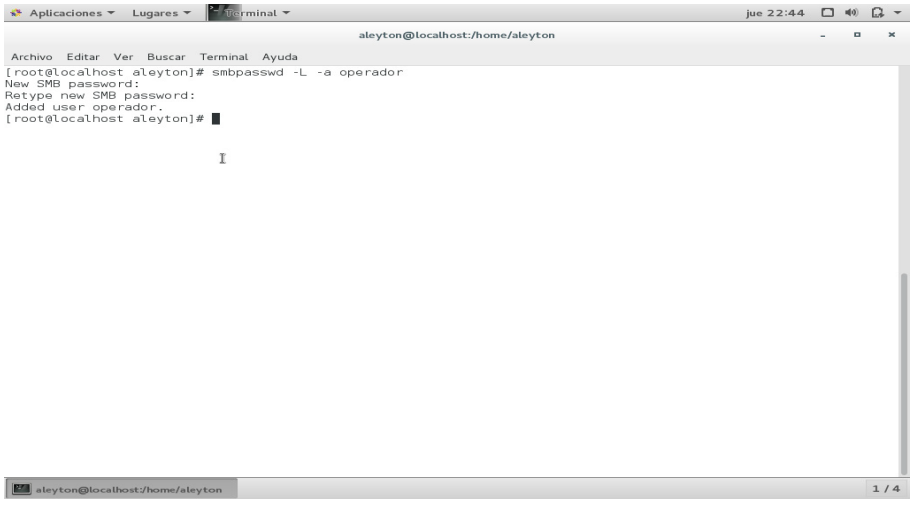


Figura 80: Comando en el terminal de CentOS.

Se vuelve a digitar el comando "smbclient 127.0.0.1 –U (nombre del usuario)" y se ingresa la contraseña para poder observar que el usuario que creamos ha sido añadido a Samba.

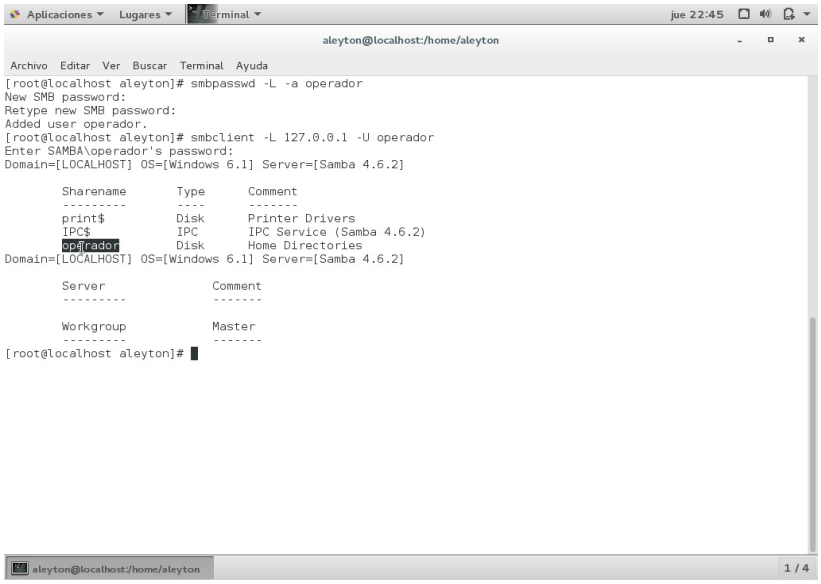


Figura 81: Usuario creado con el nombre de "operador".

Otorgamos los permisos de lectura y escritura a través del comando "setsebool –P samba_export_all_rw 1". Conforme lo podemos observar en la figura 82.

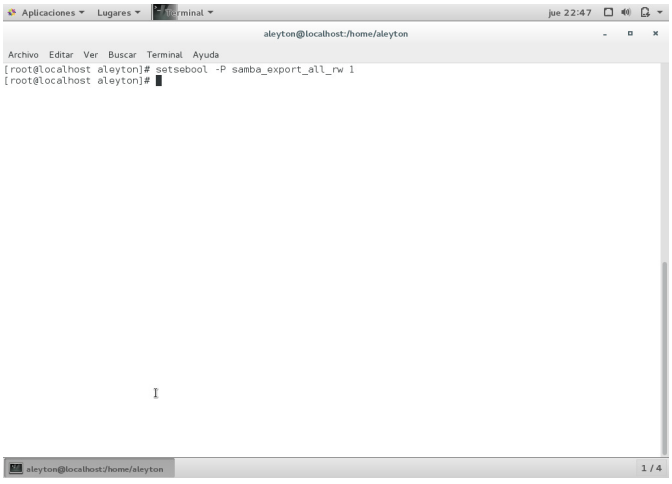


Figura 82: comando "setsebool –P.

2.2.8 Accedemos al cliente para configurar Samba por medio del comando "ssh root@(ip del cliente)".

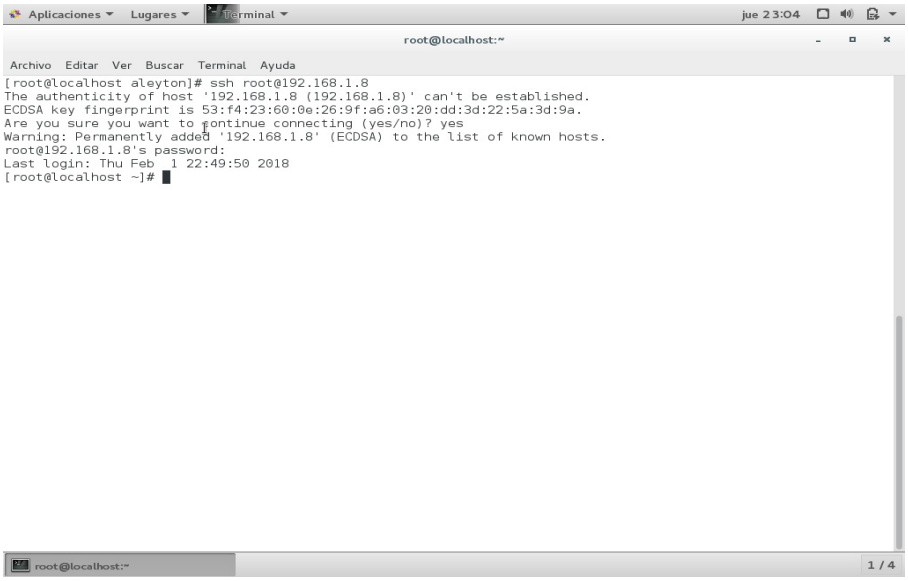


Figura 83: ssh root@(ip del cliente).

Ingresamos el comando "yum install samba-client", e instalamos Samba en el cliente.

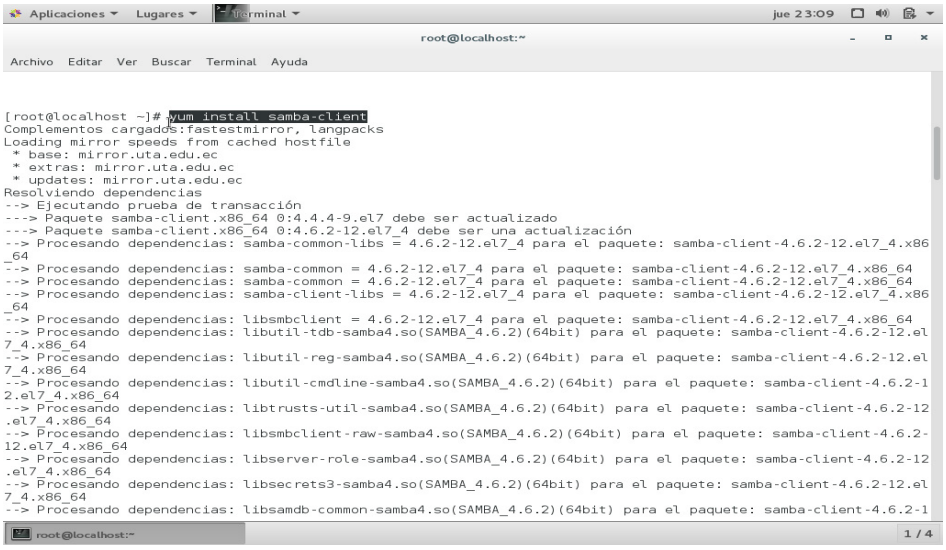


Figura 84: Proceso de Instalación Samba Cliente.

A través del cliente, ingresamos el comando “smbclient –L (ip del servidor) –U (usuario creado)” y se puede observar los usuarios de Samba que están creados en el servidor.

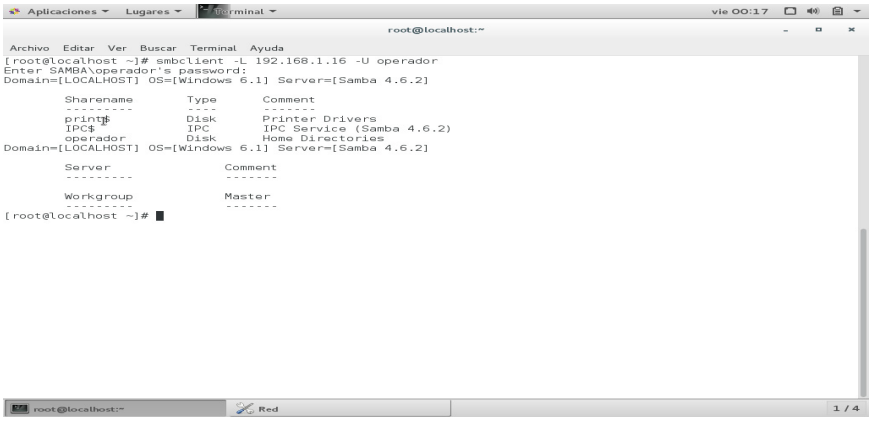


Figura 85: Usuarios de Samba creados en el servidor.

Montamos el usuario en el cliente con el comando “mount –o username= (usuario creado), password= (contraseña creada) //(ip del servidor) / (usuario creado)/mnt

mount -o username=operador, password=romeo1998

Paso 12: Una vez ejecutado esto, se comprueba que la configuración esté correctamente realizada creando archivos y directorios con los comandos “mkdir /mnt/d” y “touch /mnt/f” y se revisa que se hayan creado con el comando “ls /mnt”. Se sale del cliente con el comando “logout” y se escribe el comando “ls /mnt” y si muestra los archivos creados en el cliente, se habrá realizado la configuración de manera correcta.

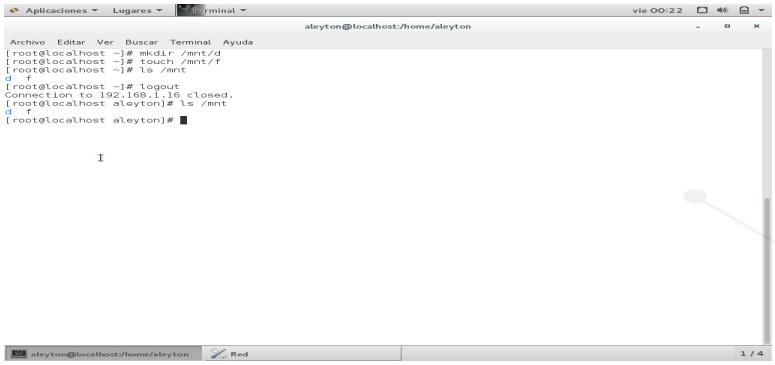


Figura 86: Creación de directorios desde el cliente bajo la configuración de Samba.

CAPÍTULO 3:
INTRODUCCIÓN DE MOODLE 3.O



En este capítulo usted encontrará:

- *Introducción a Moodle 3.0.*
- *Gestor de Base de Datos MaríaDB.*
- *PHP.*
- *HTTP APACHE.*

Introducción

Moodle es una aplicación web que ofrece un ambiente de tipo educativo virtual, que integra un sistema de gestión de cursos de distribución libre. Ayuda a los educadores a crear comunidades de aprendizaje en línea. Este tipo de plataformas tecnológicas también se conoce como: **LCMS (Learning Content Management System).** Para integrar Moodle con CentOS se utilizan varios componentes para su instalación y configuración, en el sistema operativo Centos intervienen componentes como mariaDb, Php, Http Apache, SELinux.

MariaDB es un sistema de gestión de bases de datos derivado de MySQL con licencia GPL. Es desarrollado por Michael (Monty) Widenius (fundador de MySQL) y la comunidad de desarrolladores de software libre.

PHP es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico. Fue uno de los primeros lenguajes de programación del lado del servidor que se podían incorporar directamente en el documento HTML en lugar de llamar a un archivo externo que procese los datos.

HTTP Apache es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows,

Macintosh y otras, que implementa el protocolo HTTP/1.12 y la noción de sitio virtual.

Security--Enhanced Linux (**SELinux**) es un módulo de seguridad para el kernel Linux que proporciona el mecanismo para soportar políticas de seguridad para el control de acceso, incluyendo controles de acceso obligatorios como los del Departamento de Defensa de Estados Unidos.

Pasos para la instalación de Moodle 3.0

Paso 1: Ingresar a la máquina virtual, como usuario **root.**

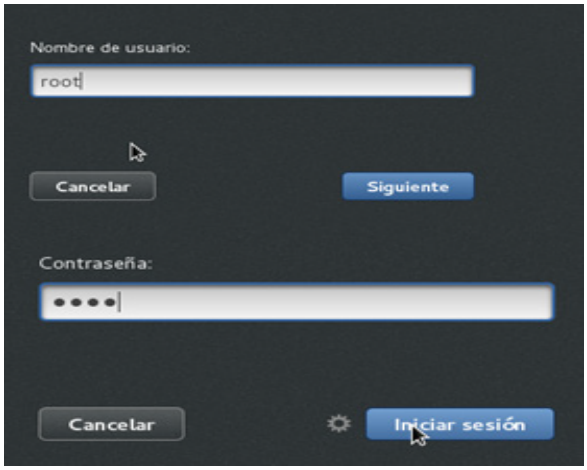


Figura 87: Máquina virtual.

Paso 2: En la terminal ingresamos **su - ,** para cambiar de usuario

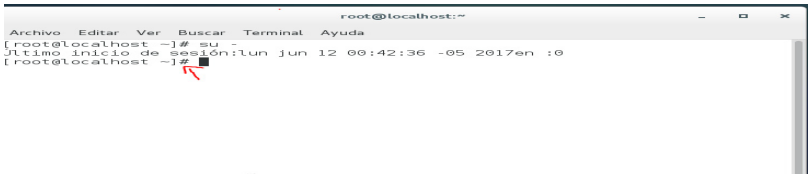


Figura 88: Comando su -

Paso 3: Para la actualización del sistema operativo, insertamos el siguiente comando, **yum update –y,** recordemos que debemos tener conexión a internet.

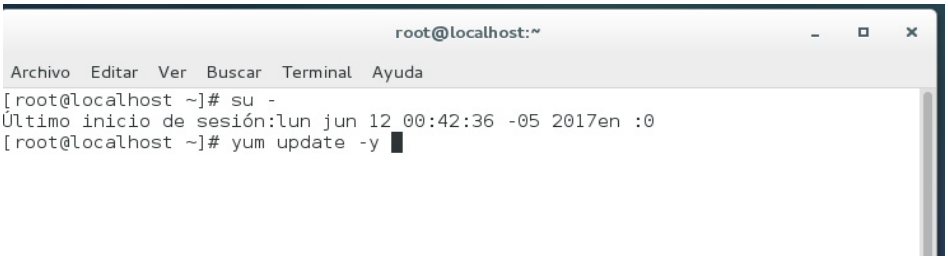


Figura 89: Comando yum update -y

Paso 4: En caso de que exista algún error al intentar realizar la descargar, utilizamos el siguiente comando, **yum clean all** (realiza la limpieza de todo el cache de YUM (metadatos, paquetes, etc.) y después volver a ejecutar el comando **yum update –y**

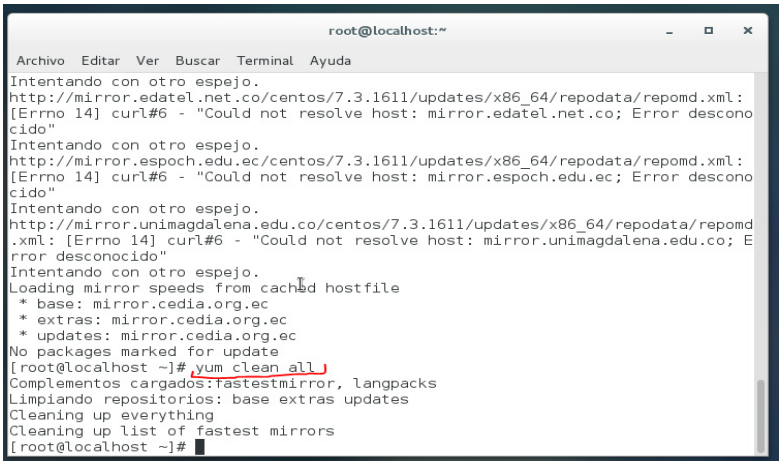


Figura 90: Comando yum clean all.

Paso 5: Instalamos los paquetes httpd mariadb mariadb-server php php-mysql

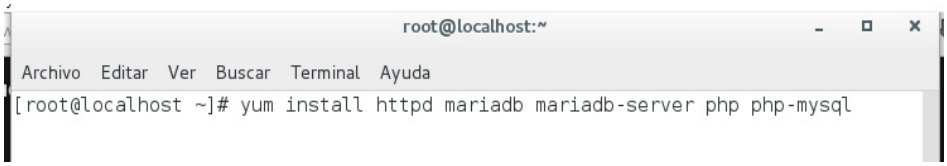


Figura 91: Instalación de Mariadb

Paso 6: Instalamos los siguientes paquetes adicionales:



Figura 92: Instalación de paquete php.

Paso 7: Iniciar servicios httpd y mysql.

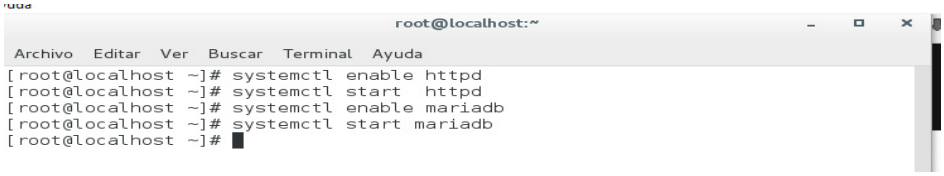


Figura 93: Iniciar servicios httpd y mysql

Paso 8: Creamos las contraseña de administrador para la base de datos.

mysqladmin -u root password 123

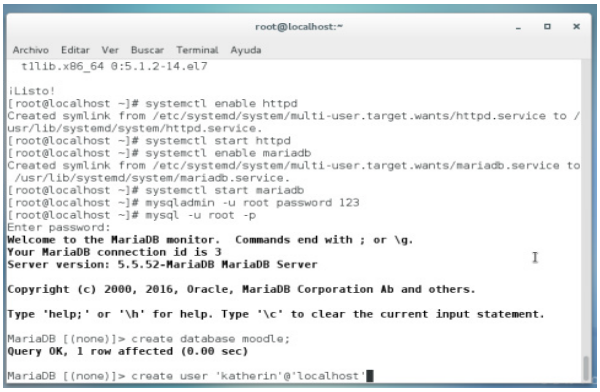


Figura 94: Comando para la creación de la contraseña en mysql

Paso 9: Creamos la base de datos con el nombre "moodle", un usuario de base de datos en este caso "katherin", asignamos todos los privilegios de base de datos para el usuario recién creado.

mysql -u root -p

MariaDB [(none)]> create database moodle;

MariaDB [(none)]> create user 'katherin'@'localhost' identified by '123';

MariaDB [(none)]> grant all priviledges on moodle.* to 'katherin'@'localhost';

MariaDB [(none)]> flush privileges;

MariaDB [(none)]> exit

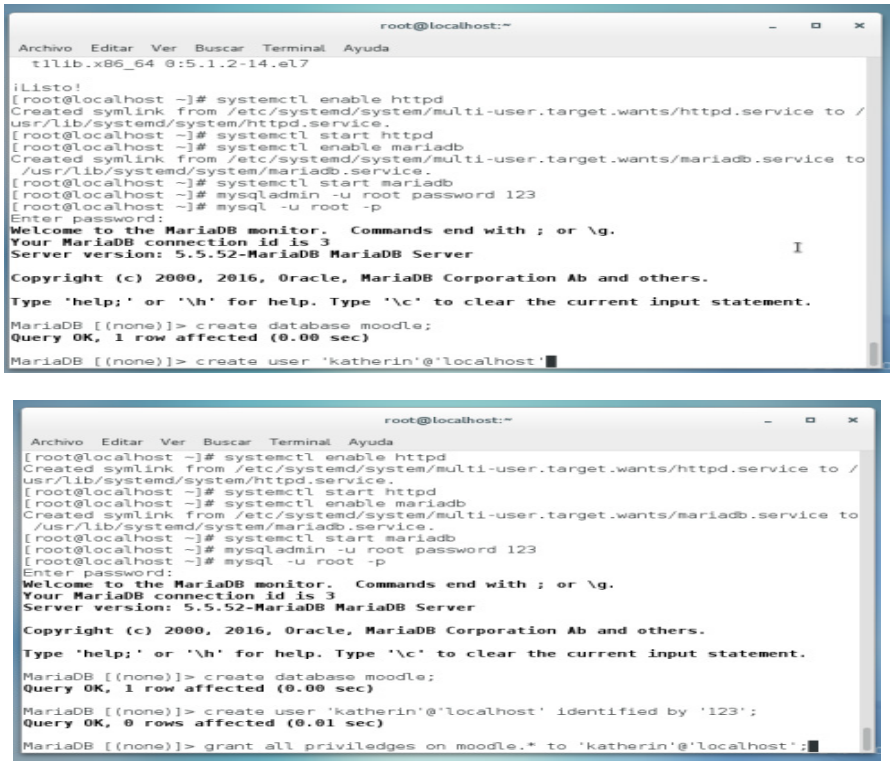


Figura 95: Creación de la base de datos y el usuario.

Paso 10: Descargamos la versión de Moodle deseada, en este caso 3.0, y configurar los servicios web.

```
# cd  /var/www/html

# wget https://download.moodle.org/stable30/moodle-3.0.tgz

# tar -xvf moodle-3.0.tgz

# chown -R apache:apache /var/www/html/moodle

# chmod -R 777 /var/www/html/moodle
```

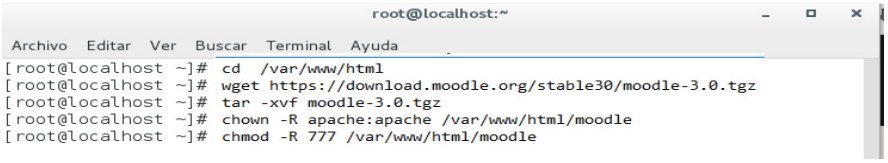


Figura 96: Descarga de Moodle.

Paso 11: Creamos un directorio de datos para moodle en /var / www/ nombrado como 'moodledata' que será utilizado por moodle, darmos los permisos necesarios, conforme lo podemos observar en la figura 97.

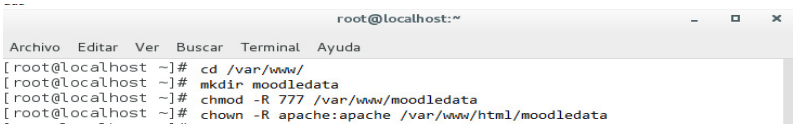


Figura 97: Creación de un director de datos.

Paso 12: Reiniciar servicios httpd. Utilizamos el comando: **systemctl restart httpd**

En nuestro navegador colocamos la siguiente dirección: localhost/moodle.

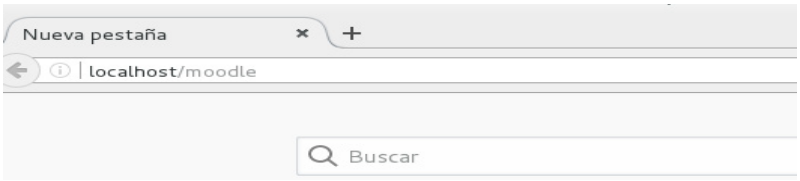


Figura 98: Navegador en máquina virtual.

Paso 13: Se inicia el proceso de instalación de Moodle.

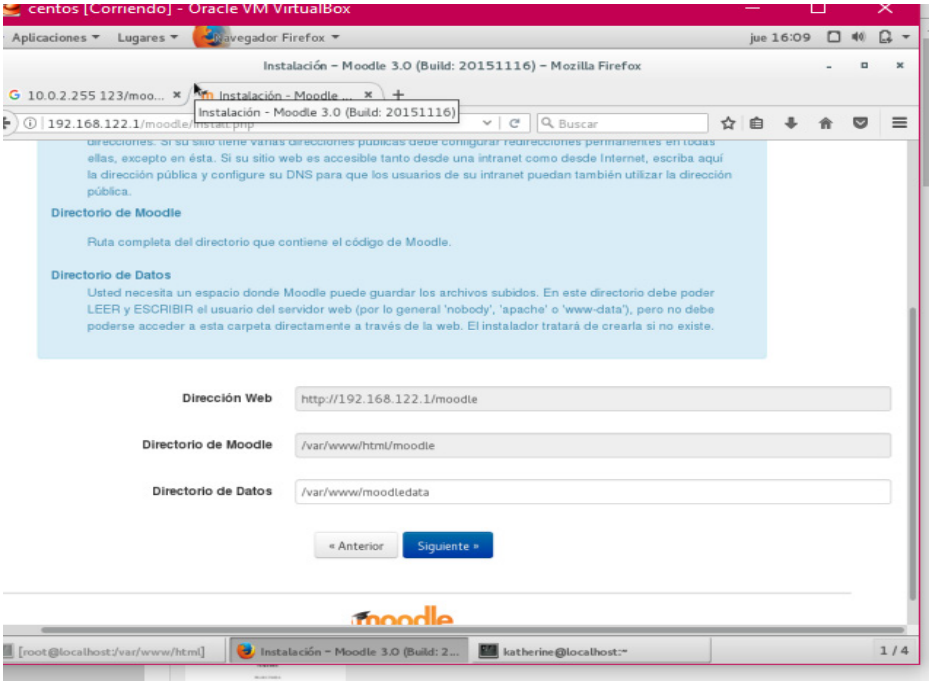


Figura 99: Iniciando Instalación.

En caso de que salga un mensaje acerca de que el directorio no tiene los permisos, realizamos lo siguiente:

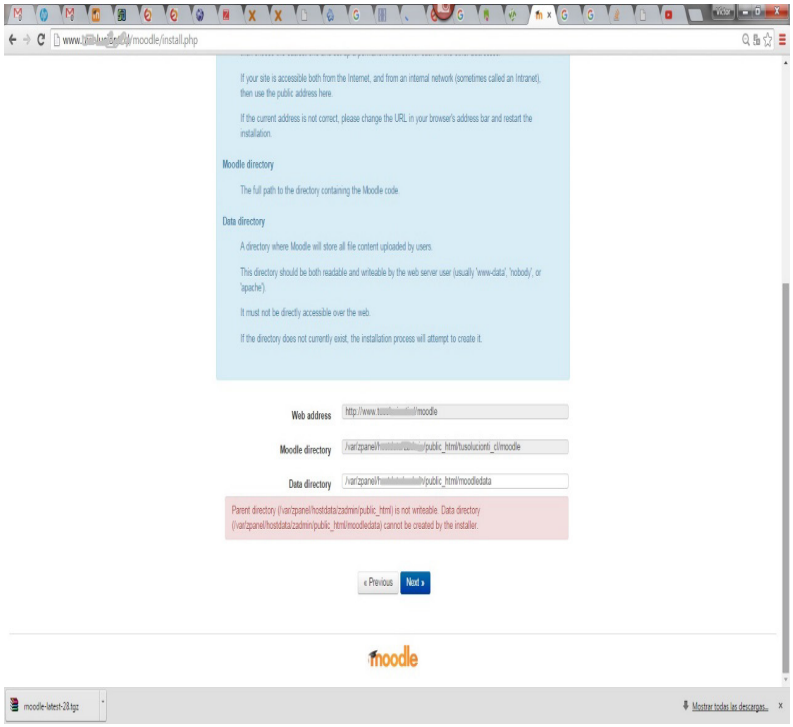


Figura 100: Mensaje en caso de no tener los permisos.

Opción b)
Crear un archivo gedit con lo siguiente:
Y guardarle en el *archivo raíz, o sea, en la carpeta Moodle*

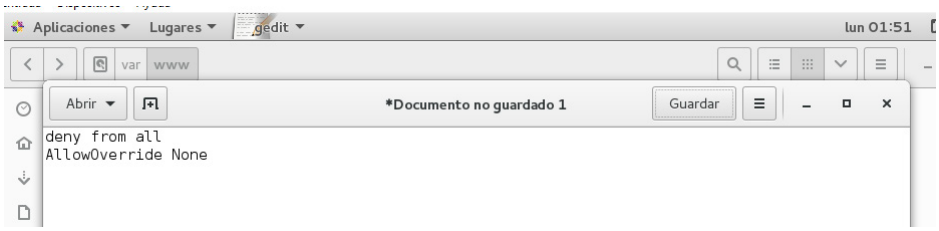


Figura 101: Crear archivo gedit.

Opción c):

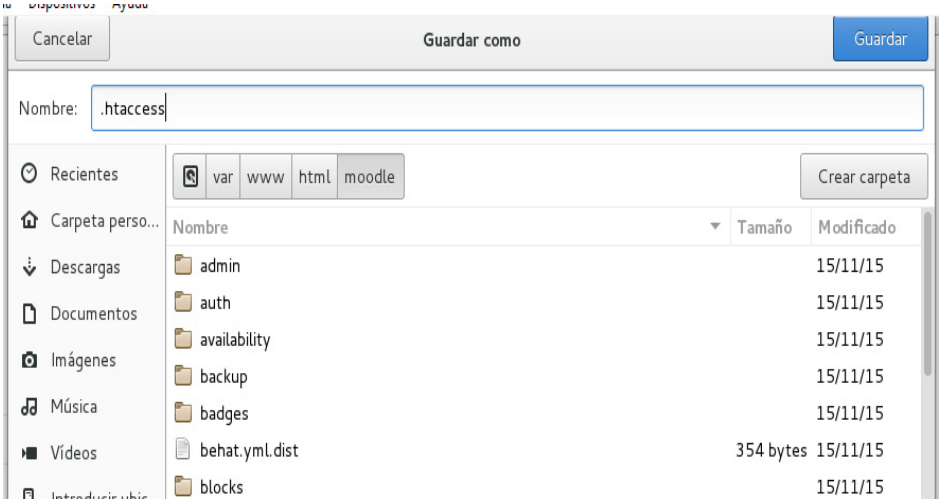


Figura 102: Guardar como.

Y si el error aún continúa hacer lo siguiente: entramos a la terminal y ponemos el siguiente comando*: **chcon –Rvu system_u -t httpd_sys_content_rw_t /var/www/moodledata/**, procedemos a reiniciarl el servidor: **systemctl restart httpd***

Paso 14: actualizamos el navegador.

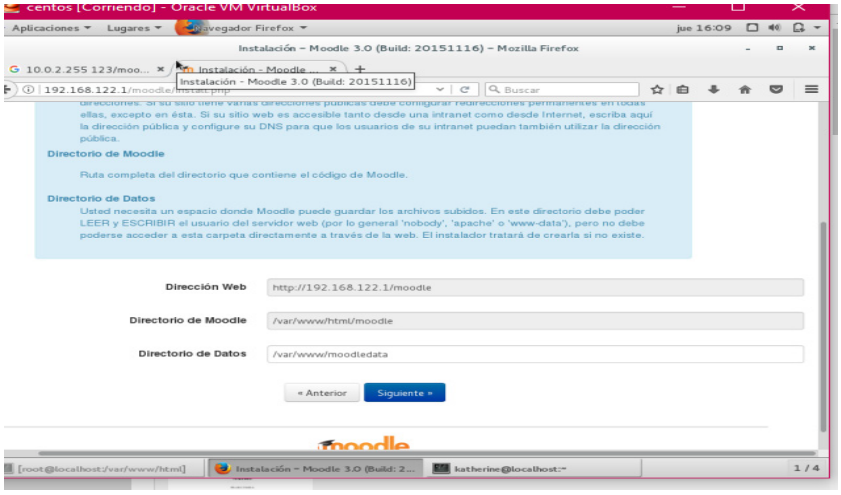


Figura 103: actualizamos el navegador.

Paso 15: Llenar los campos, la base de datos, el usuario de la base de datos, contraseña, de la base de datos, como se creó en el paso 9.

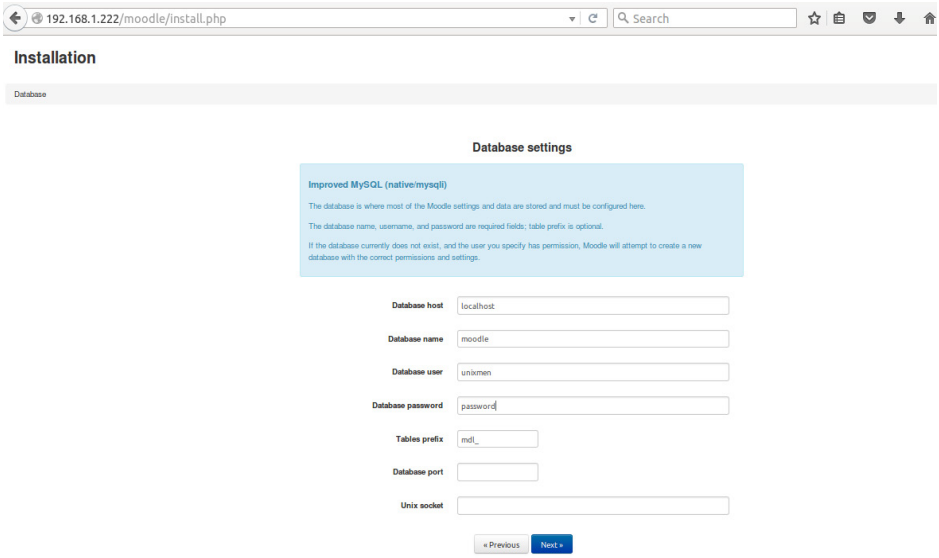


Figura 104: Llenado de datos.

Y si sale esta advertencia:



Figura 105: Finalización de configuración.

Se debe copiar ese código en un documento (bloc de notas/ gedit) y guardar en el directorio raíz (Moodle), clic en finalizar.

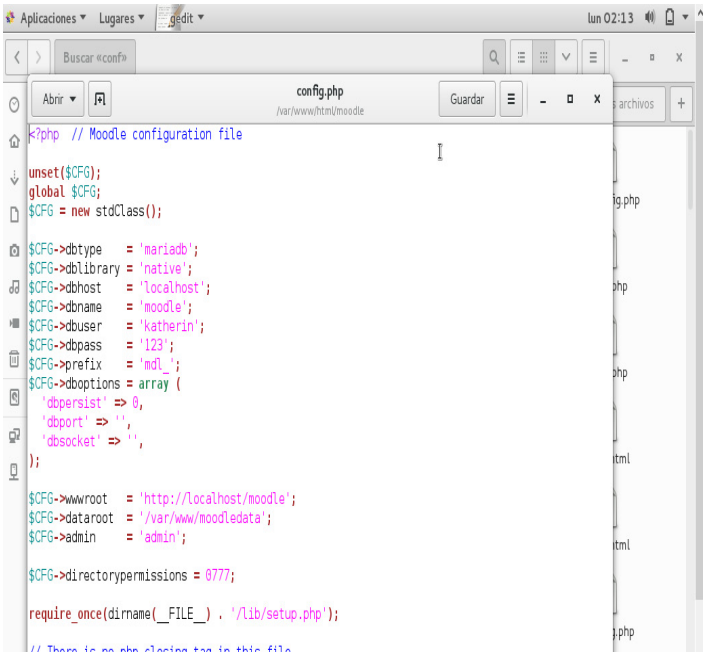


Figura 106: código en un documento (bloc de notas/gedit).

Paso 16: Presionamos en continuar:

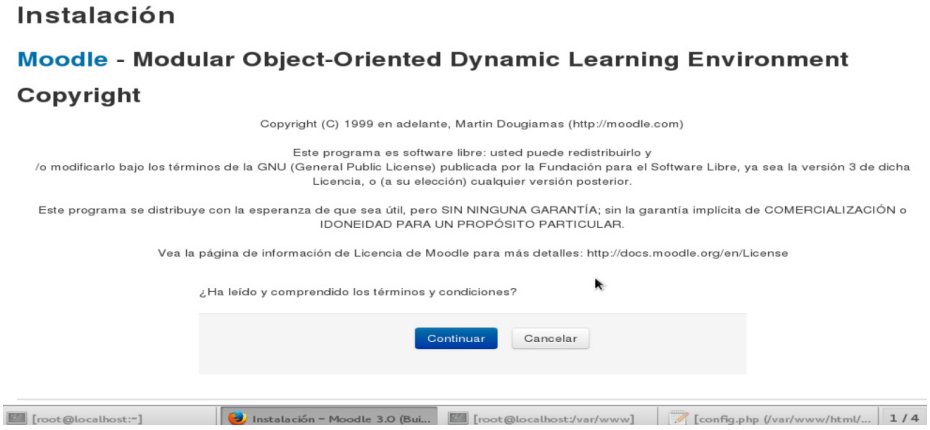


Figura 107: Pantalla de instalación de Moodle.

Paso 17: Todo debe estar en verde, eso significa que todos los requerimientos están instalados.

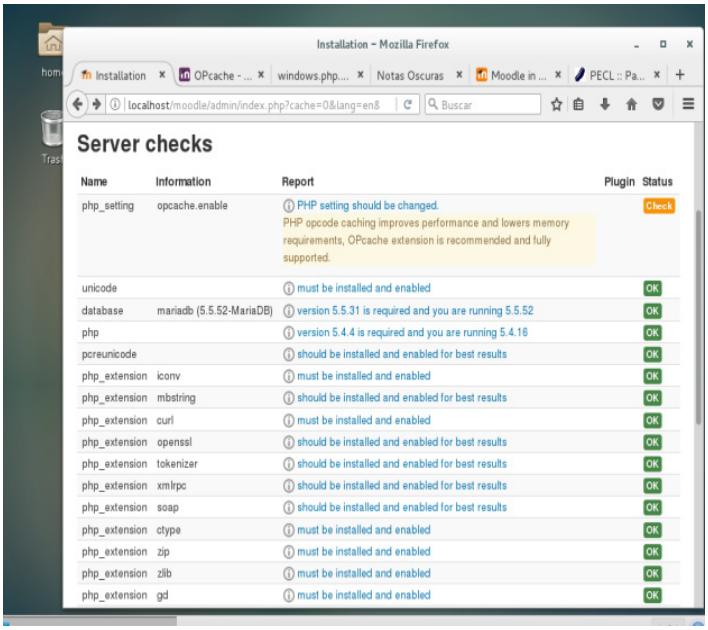


Figura 108: Verificación de los requerimientos instalados.

Paso 18: Clic en continuar.

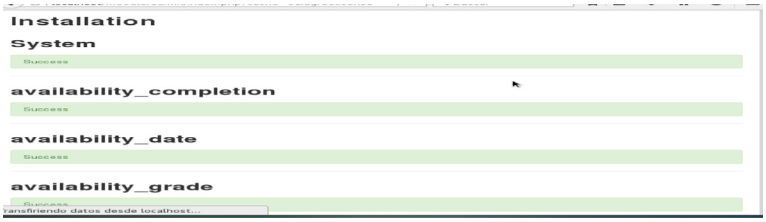


Figura 109: Instalación del sistema.

Paso 19: Llenar los campos, usuario, contraseña, nombre, apellido, correo electrónico, país, etc., y dar clic en continuar.



Figura 110: Llenado de datos.

Paso 20: Configuramos la página inicial de la plataforma. Pulsamos en "Guardar los cambios" para continuar.

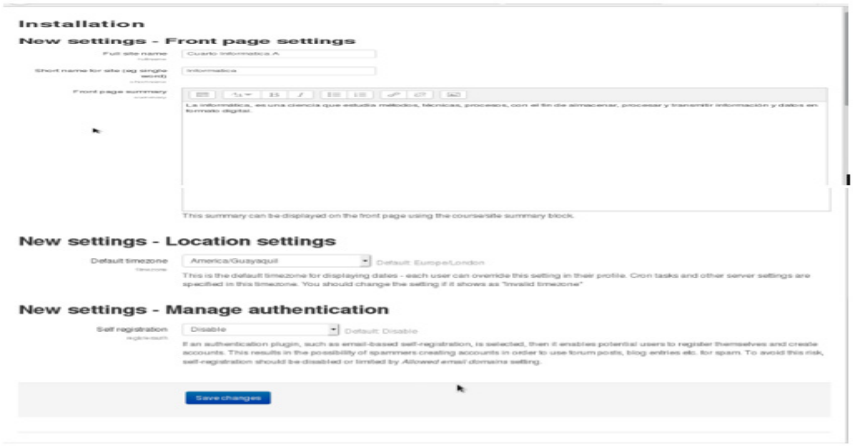


Figura 111: Configuración página inicial.

Paso 21: se culmina la instalación.

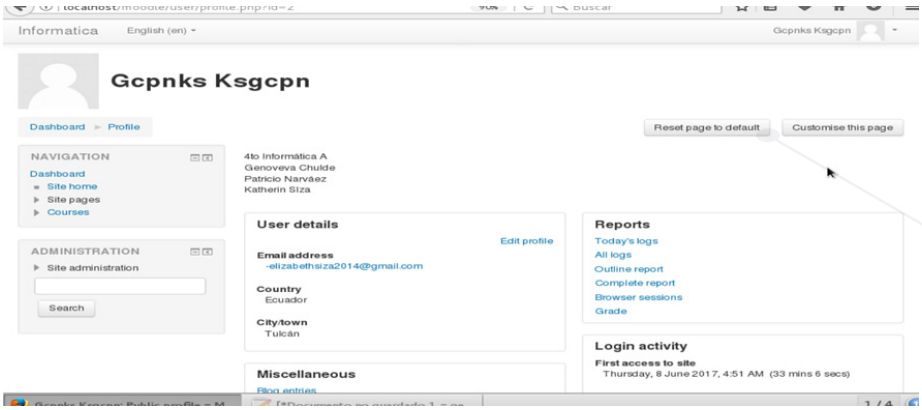


Figura 112: Interfaz principal del Software Moodle.

CAPÍTULO 4:
INTRODUCCIÓN DE SQUID 3.5



En este capítulo usted encontrará:

- *Introducción Squid 3.5.*
- *¿Qué es un Proxy?*
- *Proxy Nat.*
- *Proxy Transparente.*
- *Instalación de Squid 3.5.*

Introducción

Squid 3.5 es el software para servidor proxy más popular y extendido entre los Sistemas Operativos basados sobre Unix. Es muy confiable, robusto y versátil. Al ser software libre, además de estar disponible su **código fuente, está libre del pago de costosas licencias por** uso o con restricción a un uso con determinado número de usuarios. Entre otras cosas, squid puede hacer proxy y cache con los protocolos HTTP, FTP, GOPHER y WAIS, proxy de SSL, cache transparente, WWCP, aceleración HTTP y cache de consultas DNS.

¿Qué es un proxy?

Este puede ser un dispositivo hardware o software que se instala en una red como un mecanismo de control. Suele tener varias funciones, como filtrado de contenido web, optimización de ancho de banda y traducción de direcciones IP (NAT), entre otras.

Proxy cache: Su función es mejorar el rendimiento, ya que almacena las consultas web hechas por los usuarios en un espacio llamado memoria cache, esta es utilizada cuando la consulta hecha por el usuario se encuentra almacenada allí, y se le entrega al usuario sin

necesidad de descargarla nuevamente desde internet, optimizando el ancho de banda utilizado.

Proxy NAT o Enmascaramiento: Tiene como función hacer traducción de direcciones ip (NAT), como enmascarar una dirección IP de una red privada en una dirección IP pública para salir a internet. Esto contribuye a mantener oculto el direccionamiento interno y, por ende, mejorar la seguridad de los equipos que se encuentren en nuestra red.

Proxy Transparente: Es bastante importante, ya que trabaja en conjunto con el firewall y no requiere configuración en el navegador web, lo que supone una gran ventaja al no tener que configurarlo en cada equipo que tengamos en nuestra red; además, evita que los usuarios puedan deshabilitarlo en su navegador, también evita que sepan que sus conexiones a internet son filtradas por él.

Instalación de Squid 3.5

Paso 1: Como primer paso será instalar nuestro Squid con el comando **yum –y install squid.**



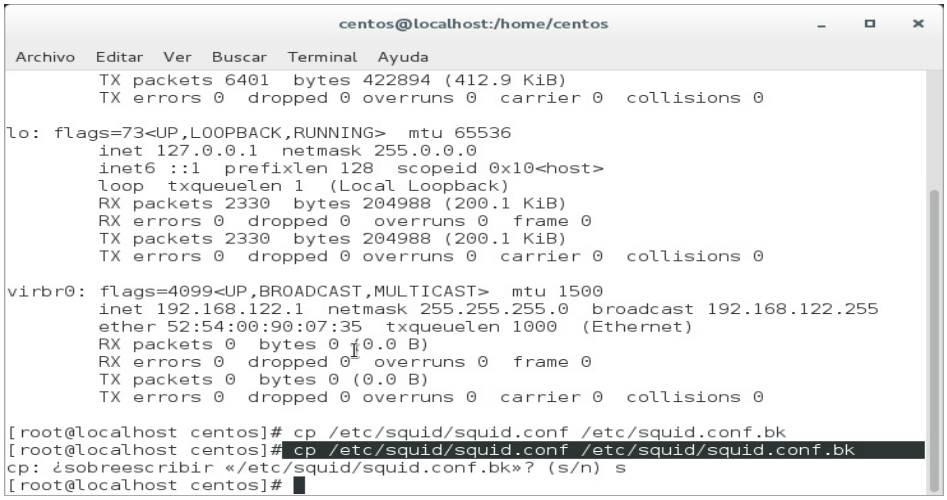
Figura 113: Instalación de Squid.

Paso 2: Para revisar las interfaces digitamos el comando ifconfig.



Figura 114: Comando ifconfig.

Paso 3: Creamos una copia de seguridad con el siguiente comando **cp /etc/squid/squid.conf /etc/squid/squid.conf.bk**



Creamos una carpeta llamada lista con el comando **mkdir /etc/squid/prueba** y creamos los respectivos archivos y agregaremos las **urls** que queremos restringir.

En esta pantalla mostramos las páginas que vamos a restringir.

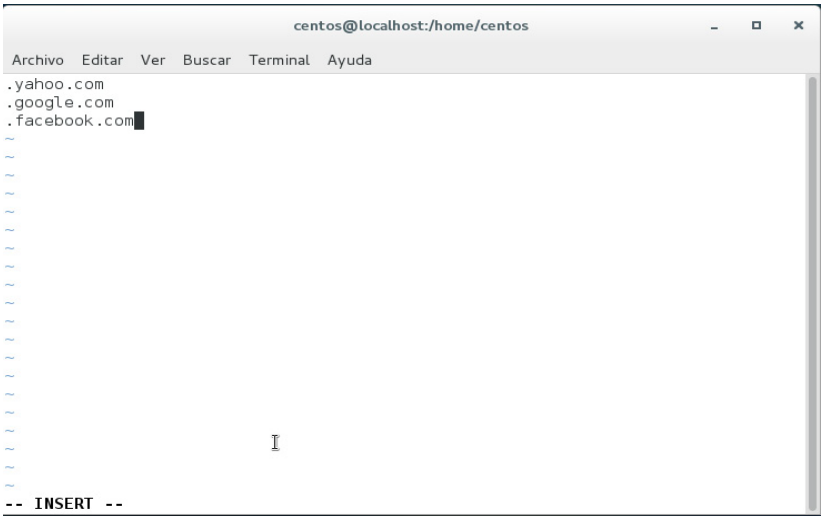


Figura 115: Pantalla de restricción.

Paso 4: Abrimos el archivo con el siguiente comando para editarlo vi **/etc/squid/squid.conf**

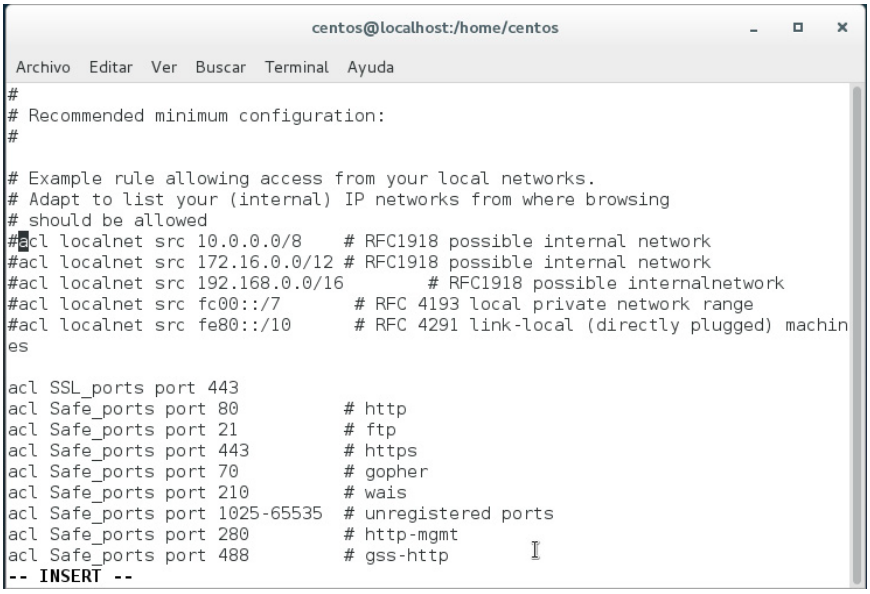


Figura 116: Edición archivo de configuración.

Paso 5: Iniciamos el servicio con el siguiente comando service **squid restart**

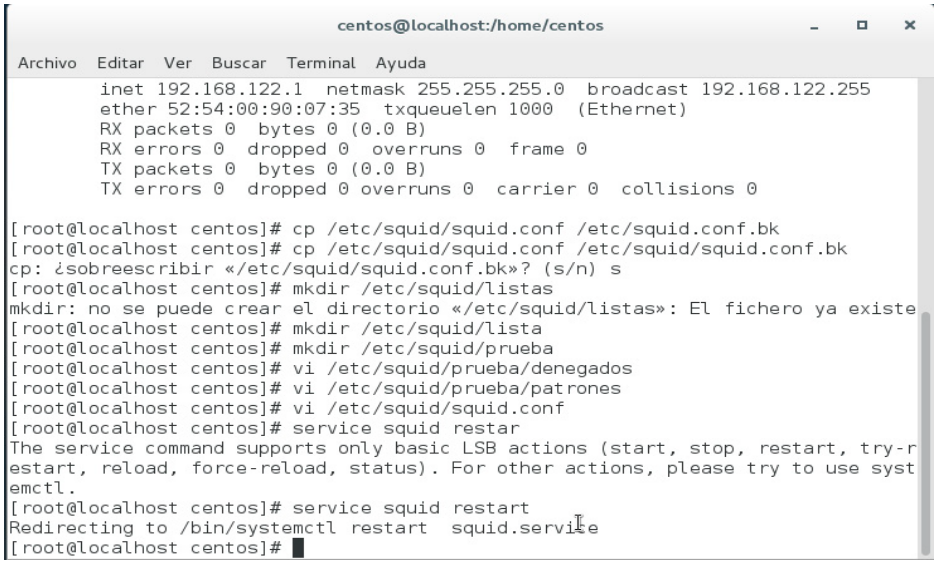


Figura 117: Comando service squid restart.

Paso 6: Configuramos el firewall con el comando **firewall-cmd – -zone=public - - add-port=3128/tcp - -permanent** y acabamos la configuración con el siguiente comando **firewall-cmd - -reload**

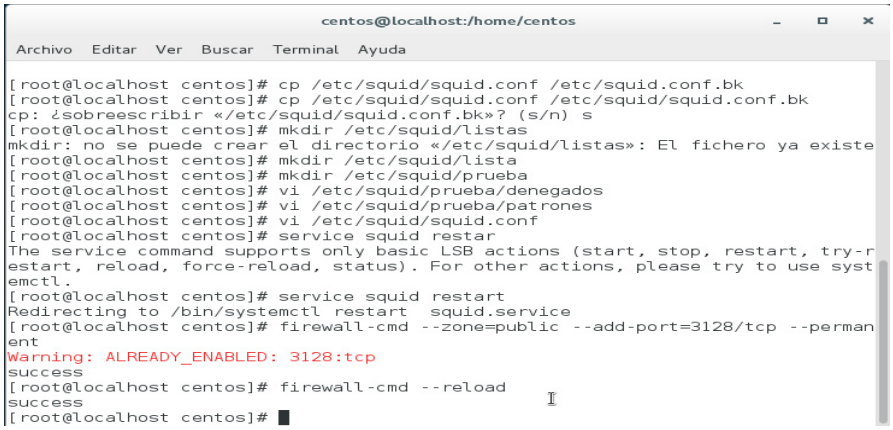


Figura 118: Configuración del firewall.

Paso 7: Ahora veremos la tarjeta de red del virtual box para colocar las direcciones ip.

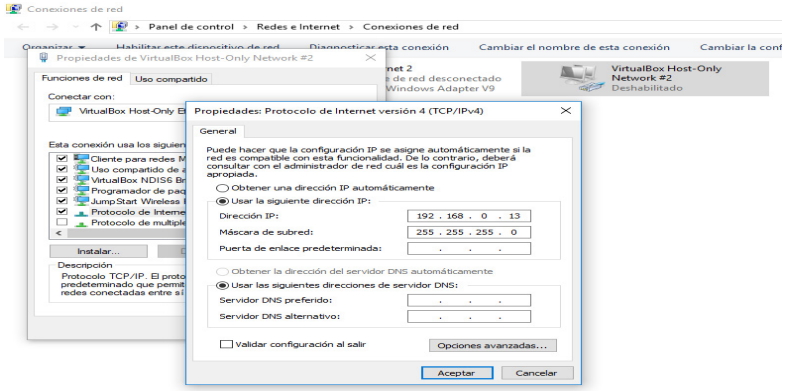


Figura 119: Direcciones IP.

Paso 8: Activaremos nuestro **proxy** en la máquina virtual para restringir las páginas señaladas.

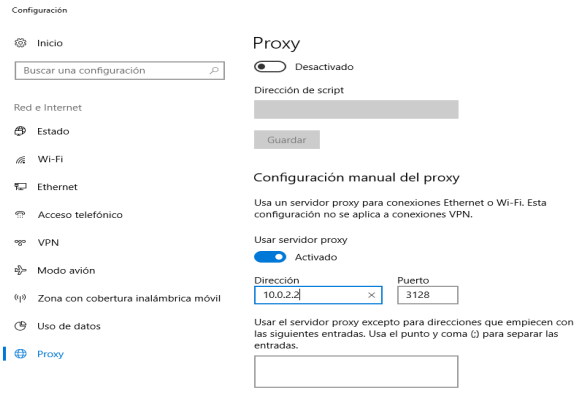


Figura 120: Activación de Proxy.

Paso 9: Abrimos el explorador web, luego vamos a configuraciones avanzadas y se observa el proxy

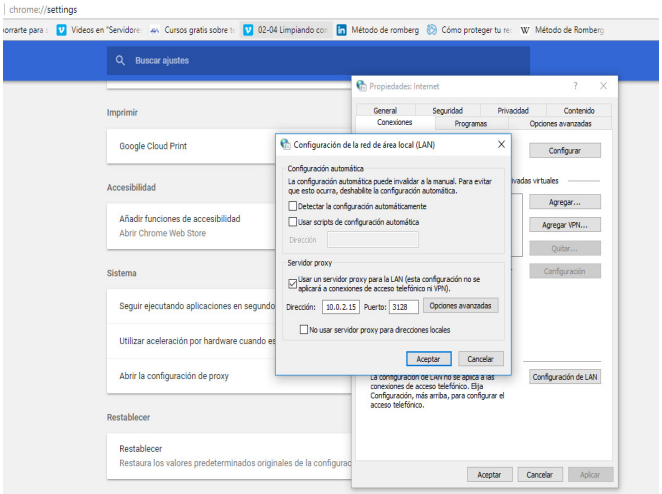


Figura 121: Configuración de la red de área local.

CAPÍTULO 5:
INTRODUCCIÓN DE SSH



En este capítulo usted encontrará:

- *Introducción a SSH.*
- *Instalación de SSH.*
- *Configuración de SSH.*
- *SSH desde un cliente Windows.*

Introducción

SSH es un paquete de software que permite una administración segura del sistema y transferencias de archivos a través de redes inseguras. Se usa en casi todos los centros de datos, en cada empresa más grande. SSH o Secure Shell es un protocolo de administración remota que permite a los usuarios controlar y modificar sus servidores remotos a través de internet.

Para conectar como un servidor remoto en el sistema operativo Windows, haremos uso del programa PuTTY, y así poder instalar el programa o configurar alguna parte del servidor. Por otra parte, en la conexión por SSH de CentOS a CentOS solo tendremos que configurar la red de nuestro cliente y hacer la conexión de SSH desde nuestro cliente, ejemplo ssh 10.0.0.2.

5.1 Instalación y configuración de SSH

Paso 1:

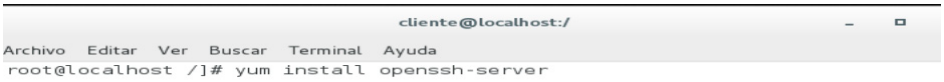


Figura 122: Instalar ssh-server en el servidor.

Paso 2:

```
[root@localhost /]# yum install ssh-clients
```

Figura 123: Instalar ssh en el equipo cliente

Paso 3: Configurar la red de VirtualBox, colocar en red interna y asignar una IP estática tanto en el servidor como en el cliente.

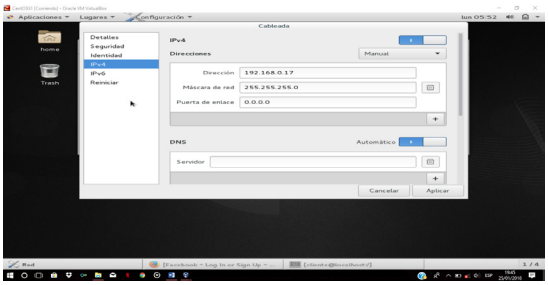


Figura 124: Servidor.

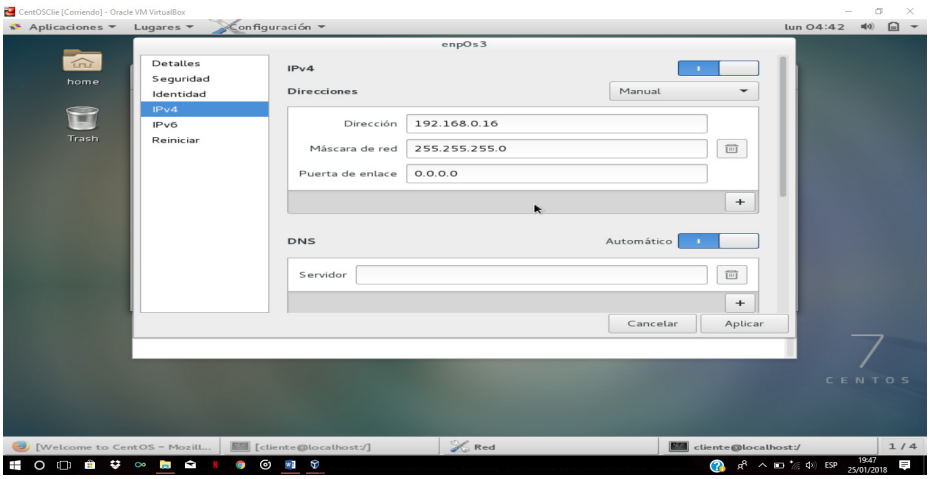


Figura 125: Cliente.

Paso 4: Comprobamos la conexión entre el servidor y el cliente usando el comando ping.

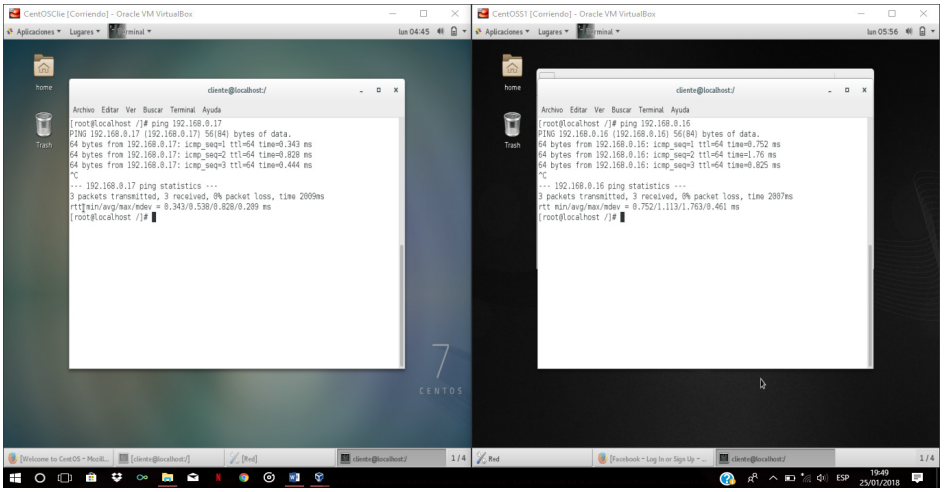


Figura 126: Venana Cliente – Servidor.

Paso 5: Usar el comando ssh seguido de la IP del servidor para ingresar mediante ssh a nuestro servidor.

1. Ingresar la contraseña del servidor y ya estaremos dentro del servidor.

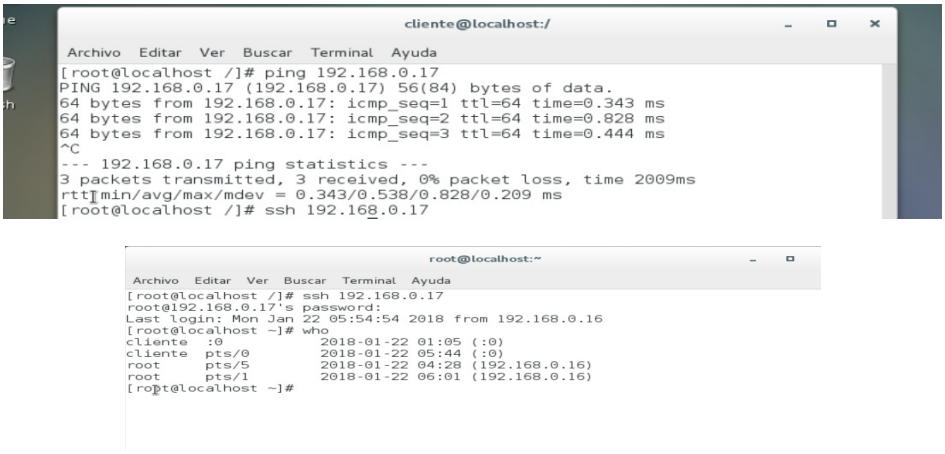


Figura 127: Ingreso al servidor

5.1.1 SSH desde un cliente Windows

Paso 1: Configurar una IP estática para que permita la conexión con el servidor.

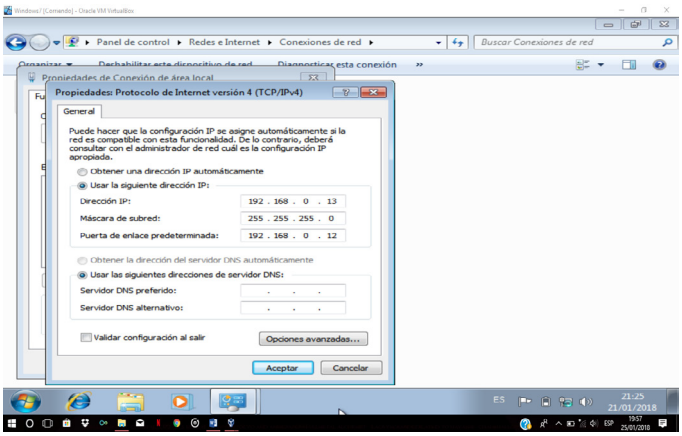


Figura 128: SSH desde un cliente Windows.

Paso 2: Probar la conexión hacia el servidor.

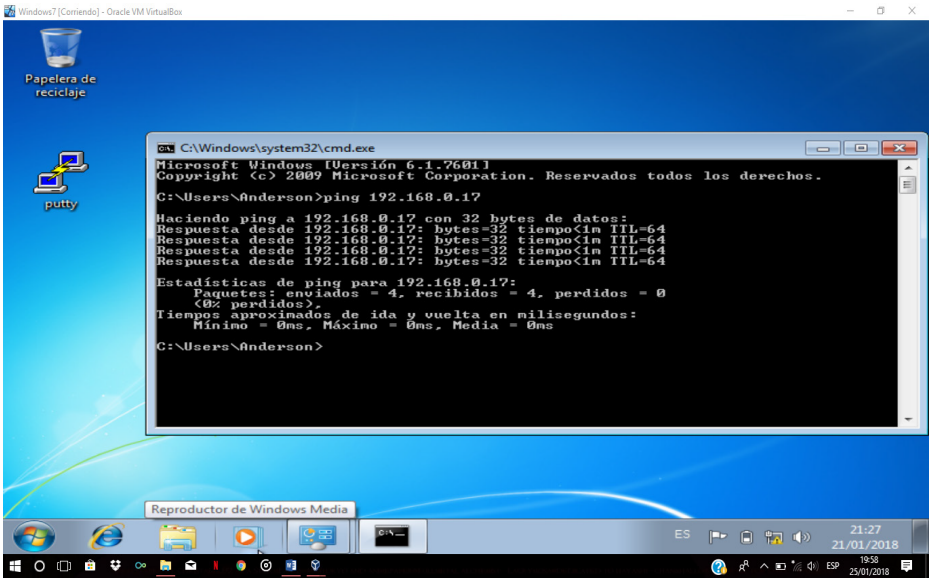


Figura 129: Comprobación conexión al servidor.

Paso 3: Descargar el programa Putty desde https://www.putty.org/ para ingresar mediante ssh usando el puerto por defecto.

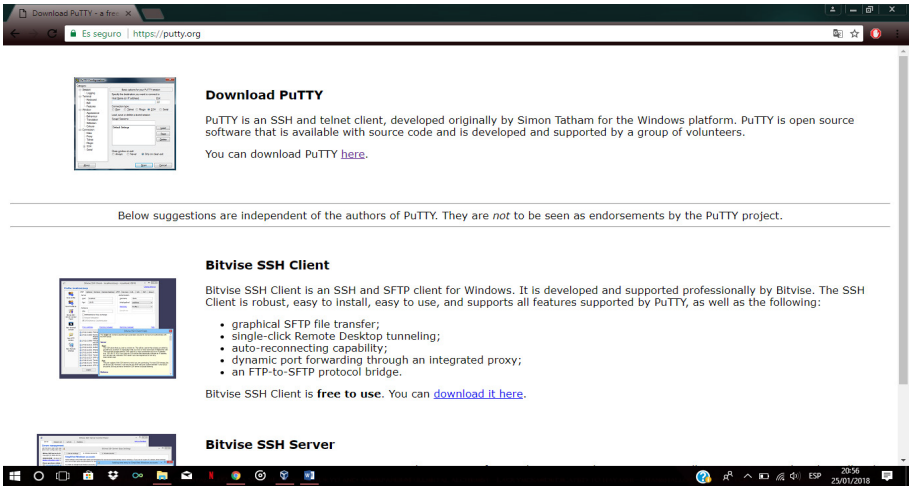


Figura 130: Acceso a programa Putty.

Paso 4:

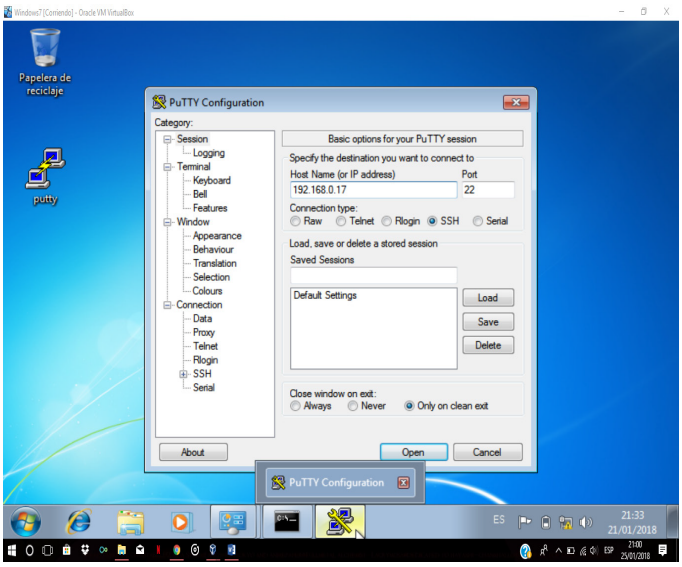


Figura 131:Abrir Putty e ingresar la IP del servidor y el puerto por defecto.

Paso 5:

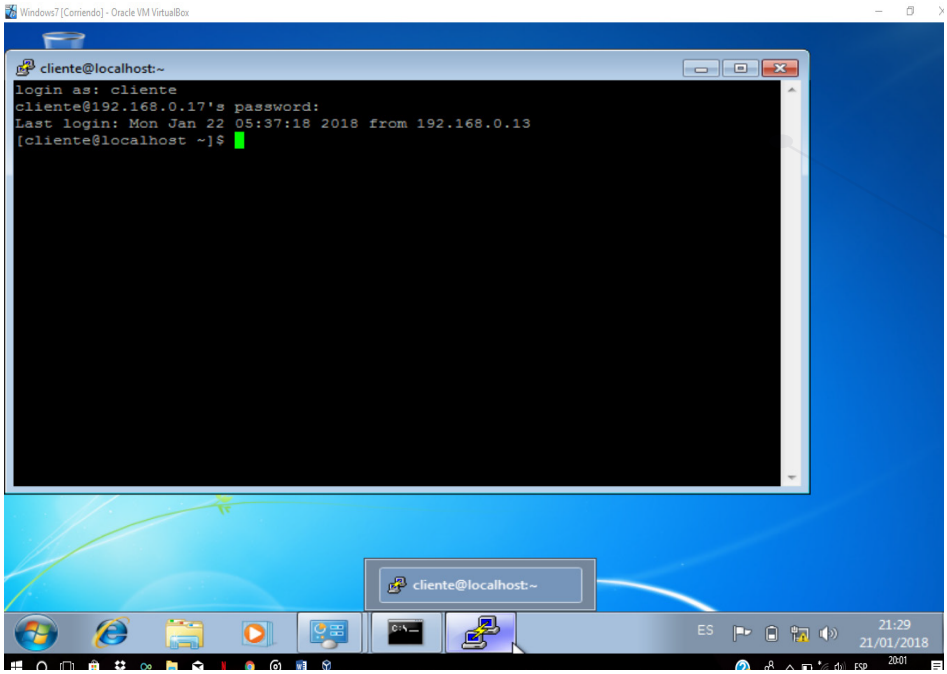


Figura 132: Ingresar el usuario y la contraseña del servidor.

Paso 6:

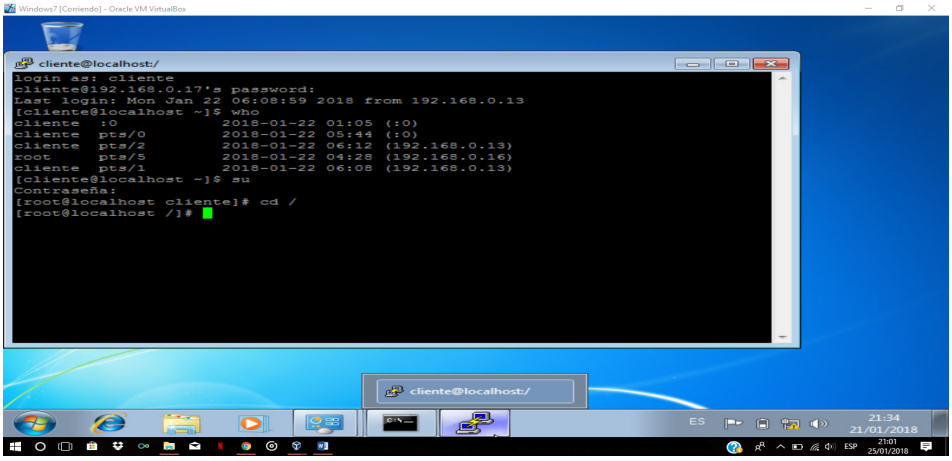


Figura 133: Ingresar como superusuario con el comando su, y ya estaremos dentro de nuestro servidor.

CAPÍTULO 6:
INTRODUCCIÓN DE NETDATA



En este capítulo usted encontrará:

- *Introducción a Netdata.*
- *Características del Netdata.*
- *Instalación Netdata.*
- *Configuración de Netdata.*

Introducción

Solvetic (2017) afirma que dentro de las tareas de control y supervisión que debemos realizar diariamente es necesario que contemos con herramientas prácticas que nos permitan llevar a cabo esta tarea de una forma sencilla, pero al mismo tiempo de forma integral en todos los componentes del sistema tanto a nivel de hardware como de software.

Netdata es una práctica herramienta que será de vital ayuda para todo el proceso de monitoreo en servidores, en este caso Centos 7.0, mediante la cual accederemos a múltiples parámetros del sistema, siempre en tiempo real y con datos reales, además es una aplicación que ha sido desarrollada con el objetivo de analizar en tiempo real el estado de rendimiento del sistema y sus respectivos componentes. Con Netdata podremos supervisar servidores físicos, virtuales o dispositivos IoT (Solvetic, 2017).

En este capítulo profundizaremos en esta herramienta y en su instalación y configuración bajo el sistema operativo Centos 7.0. Veremos cuáles son sus características, compatibilidad y componentes que permitirán realizar un correcto monitoreo hacia nuestros servidores.

Dentro de las principales características de Netdata encontramos.

- Velocidad: puede responder a las diferentes consultas en un lapso de tiempo de 0.5 ms por métrica.
- Alarmas configurables: es compatible con diferentes plantillas de alarmas y diversos métodos de notificación basados en roles.
- Extensible: puede ser añadido con APIs de BASH, Python, Perl, Node.js, Java, entre otras.
- Eficiente: consume únicamente consume el 1% de un núcleo de un procesador, pocos megas de RAM y casi nulo espacio en disco duro.
- Cero configuraciones: es capaz de recolectar alrededor de 5000 métricas de cada servidor.
- Personalizable: es compatible con plantillas HTML.
- Incrustable: puede ejecutarse de forma segura en cualquier sitio que ejecute un kernel de Linux.
- No requiere de mantenimiento: de forma automática se recupera y actualiza
- Cuenta con diferentes modos de operación como monitoreo multi-host, host autónomo, proxy de reenvío, etc.

Instalación y configuración de Netdata

Paso 1: Para instalar esta aplicación en Centos 7.0 ejecutaremos el siguiente comando: yum install zlib-devel gcc make git autoconf autogen automake pkgconfig

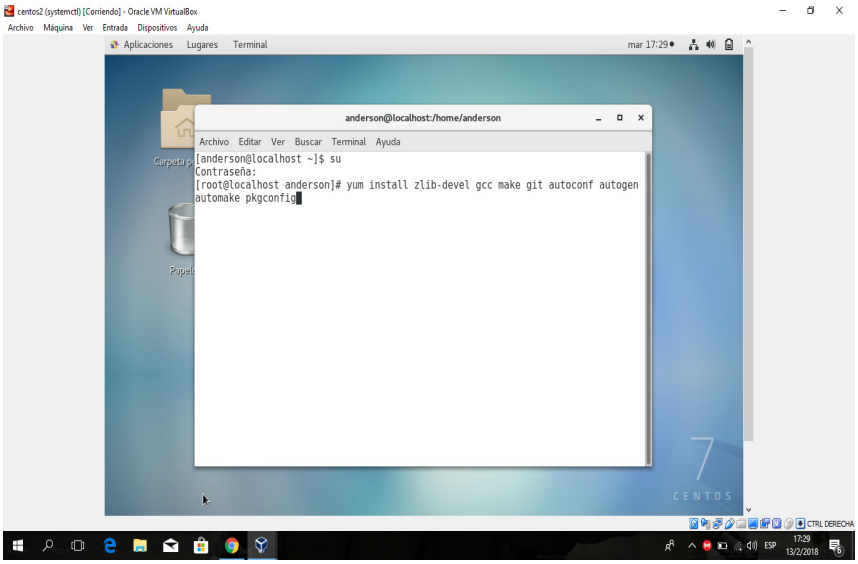


Figura 134: yum install zlib-devel gcc make git autoconf autogen automake pkgconfig.

Una vez finalice el proceso se observará lo siguiente:

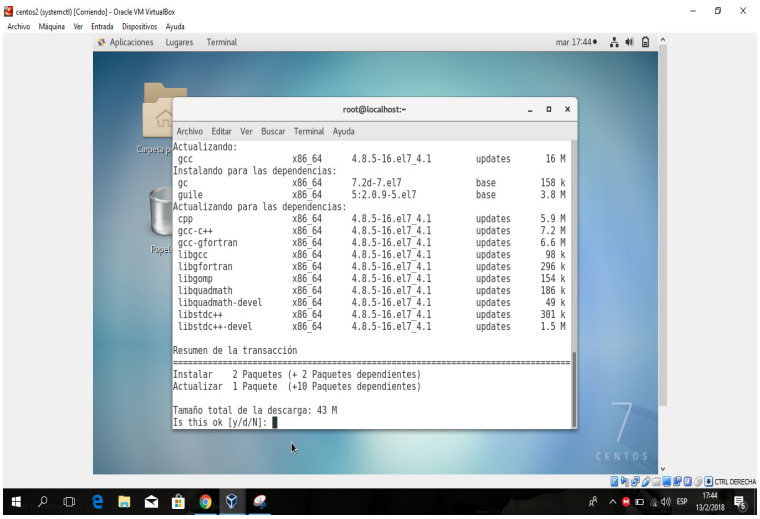


Figura 135: Escribimos la letra "y" para aceptar la descarga

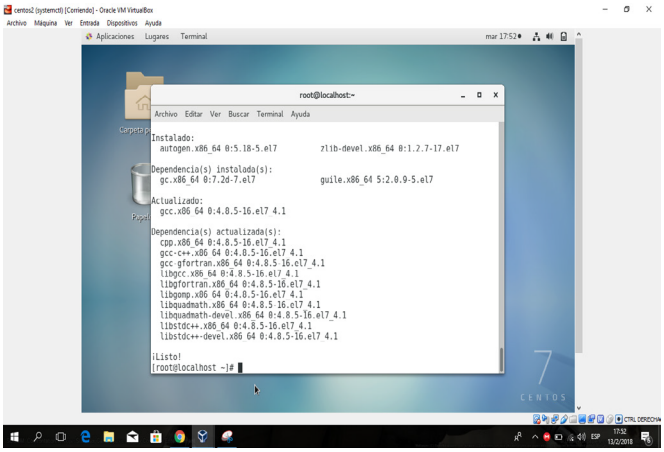


Figura 136: Instalación de Netdata.

Si la descarga se ha realizado correctamente, mostrará la palabra "correcto" al final de la instalación.

Paso 2: Una vez descargados e instalados los paquetes, vamos a clonar el repositorio de la aplicación usando git y ejecutaremos el script de instalación de Netdata: Para ello ejecutamos en primer lugar la siguiente línea:

Comando: git clone https://github.com/firehol/netdata.git --depth=1

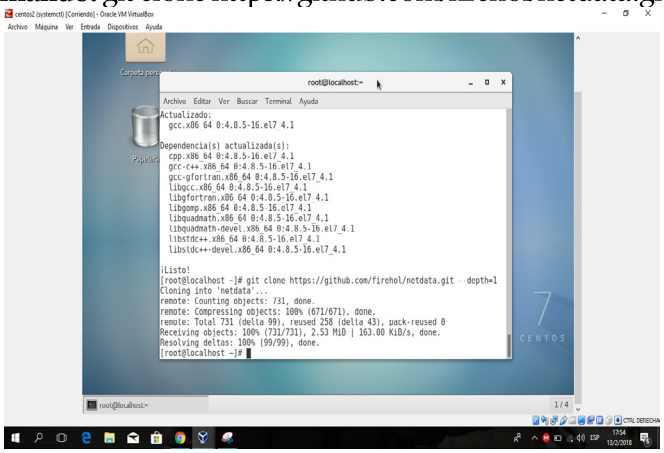


Figura 137: Se clono el repositorio.

Paso 3: Accedemos al respectivo directorio:

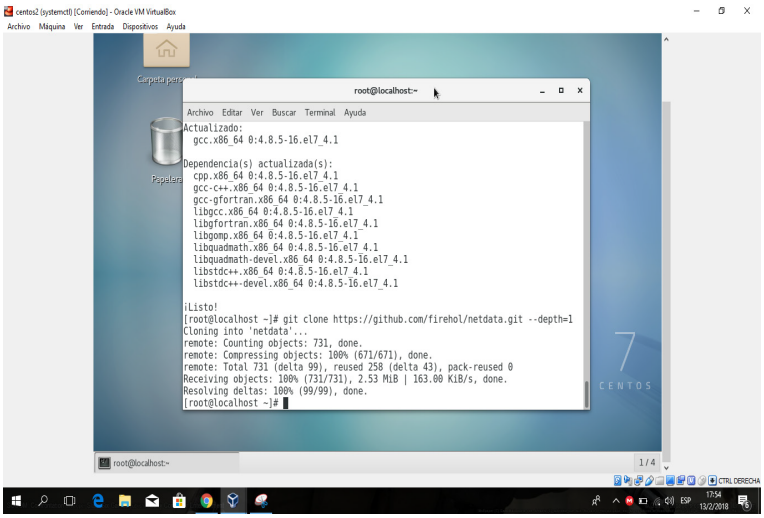


Figura 138: Comando: cd Netdata.

Paso 4: Ejecutamos el instalador del script usando la siguiente línea:

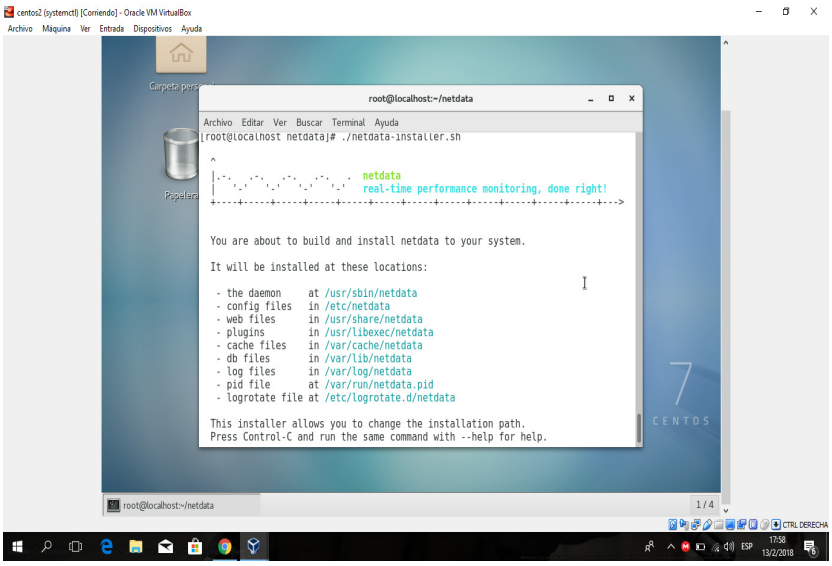


Figura 139:Comando: ./netdata-installer.sh.

Visualizaremos los paquetes que vamos a instalar para configurar Netdata en nuestro ordenador Linux.

Paso 5: Pulsamos "Enter" para iniciar el proceso de instalación. Esta instalación creará el archivo /etc/netdata/netdata.conf en Centos 7.0 desde donde podremos realizar el proceso de configuración. Obtendremos el siguiente resultado:

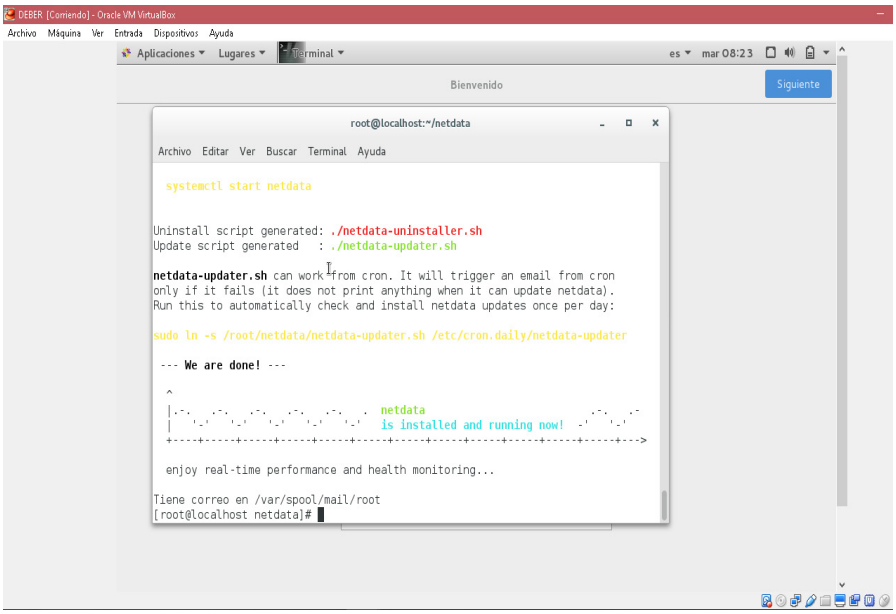


Figura 140: Inicio Proceso de instalación.

Paso 6: Ejecutar el servicio de Netdata procedemos a usar la siguiente línea:

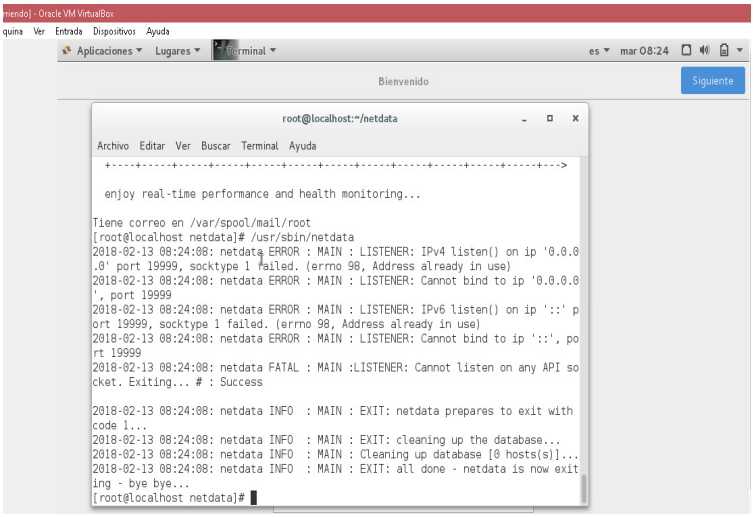


Figura 141: ***Comando:*** */usr/sbin/netdata.*

Ejecutamos Netdata, para utilizarlo en nuestro ordenador.

Paso 7: Para que la comunicación de Netdata con la red sea correcta, debemos habilitar el puerto 19999 en el firewall de Centos 7.0; para esto, ingresaremos lo siguiente: **comandos:** firewall-cmd --permanent --zone=public --add-port=19999/tcp firewall-cmd –reload

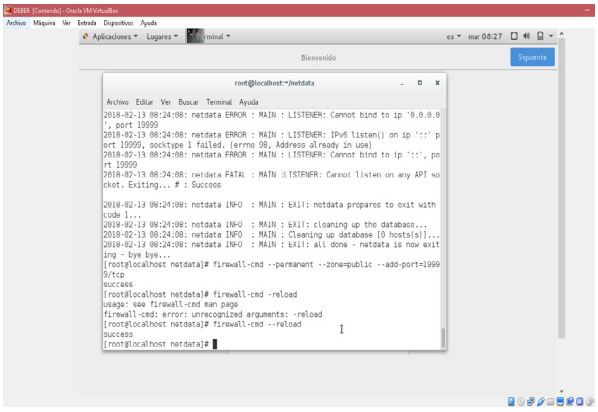


Figura 142: Ejecución del comando.

Habilitamos el puerto 19999, para acceder a nuestro ordenado desde el internet utilizando cualquier navegador.

Paso 8: Acceder a cualquier navegador, desde la barra de dirección ingresar la siguiente Sintaxis: http://IP:19999/. En nuestro caso, ingresaremos la ruta http://10.0.2.15:19999[/url] y el resultado será el siguiente:

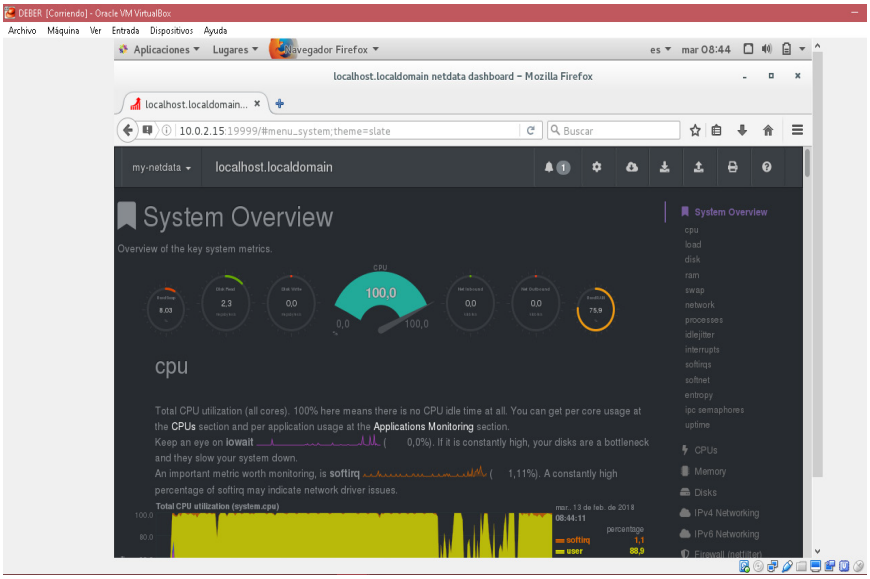


Figura 143: http://10.0.2.15:19999.

Resultados

Se ha accedido a la consola de Netdata donde se podrán ver todos los parámetros del sistema en tiempo real y con información detallada. En el costado derecho encontramos las diferentes opciones ya mencionadas como:

Memoria RAM:

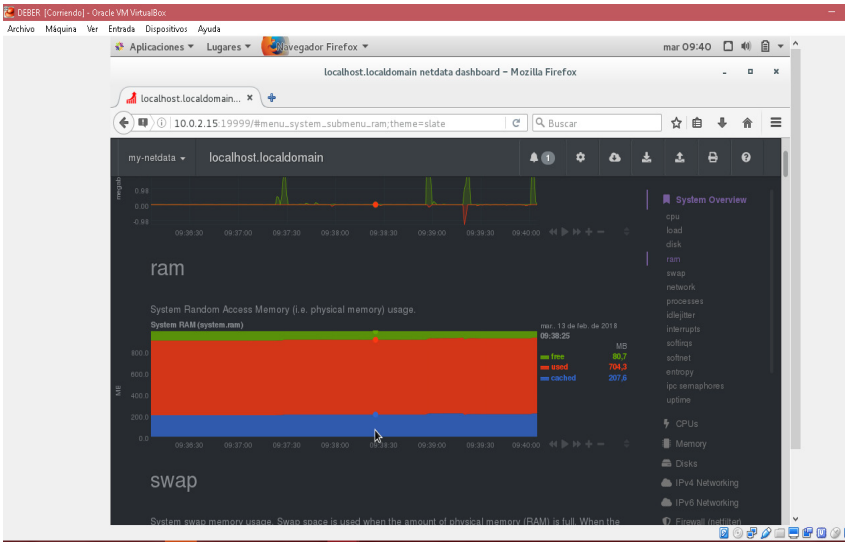


Figura 144: Analizador visual del rendimiento de la memoria RAM.

Swap:

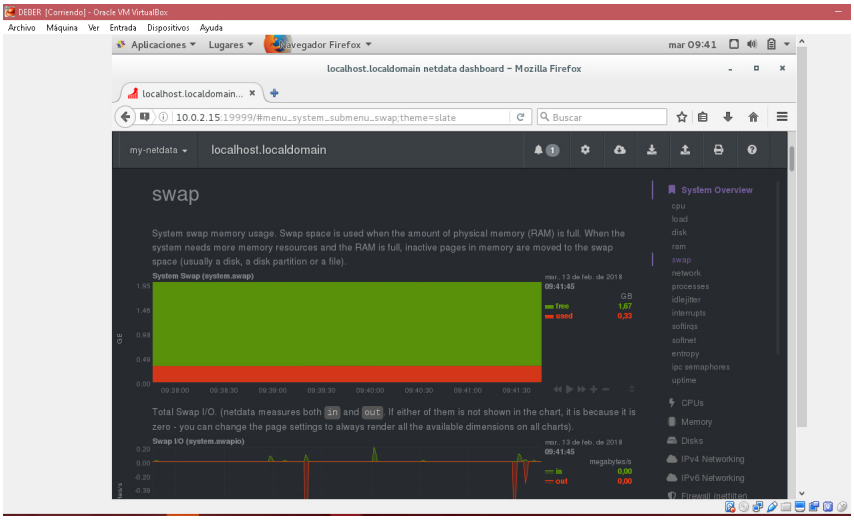


Figura 145: Espacio de Intercambio en disco.

Red:

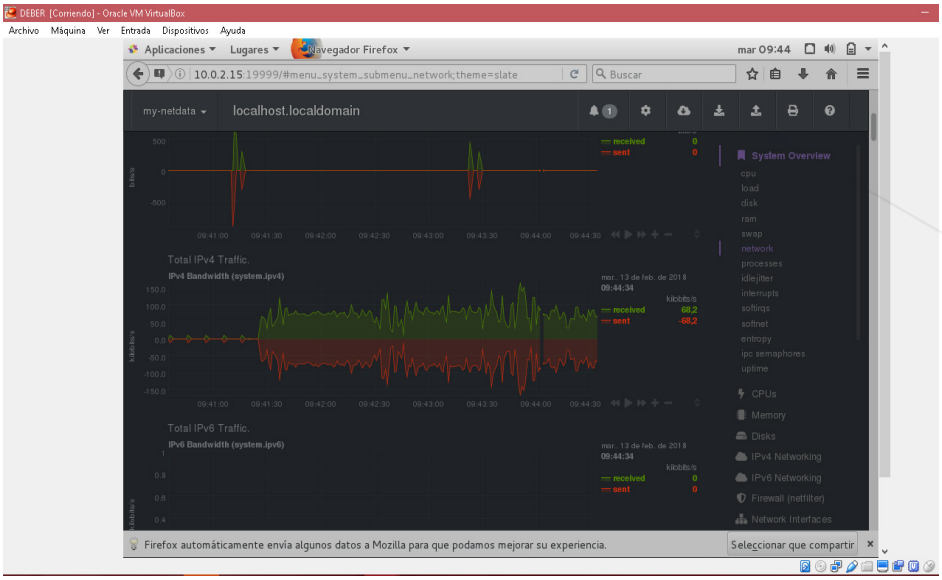


Figura 146:Ventana de monitoreo de la interfaz de Red.

Usuarios:

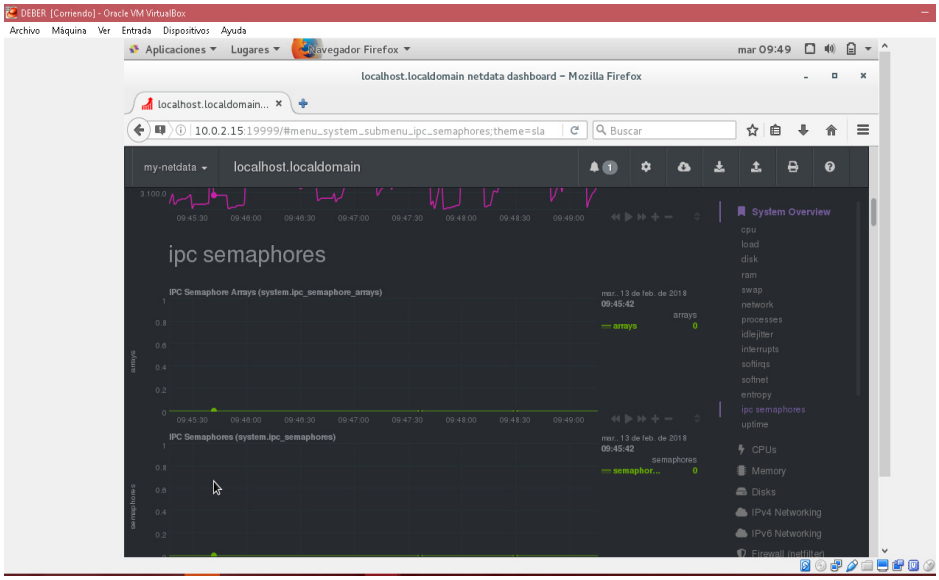


Figura 147:Ventana que visualiza a los usuarios del Sistema.

CAPÍTULO 7:
INTRODUCCIÓN DE VNC



En este capítulo usted encontrará:

- *Introducción a VNC.*
- *Instalación de VNC*
- *Configuración de VNC.*
- *Edición de archivos.*
- *Configuración de usuario-servidor.*

Introducción

VNC es un programa de software libre basado en una estructura cliente-servidor que permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente, también se denomina software de escritorio remoto. VNC no impone restricciones en el sistema operativo del ordenador servidor con respecto al del cliente: es posible compartir la pantalla de una máquina con cualquier sistema operativo que admita VNC conectándose desde otro ordenador o dispositivo que disponga de un cliente VNC portado.

Instalación configuración de VNC

Paso 1: Instalar el paquete tigervnc-server

```
Sudo yum install tigervnc-server
```

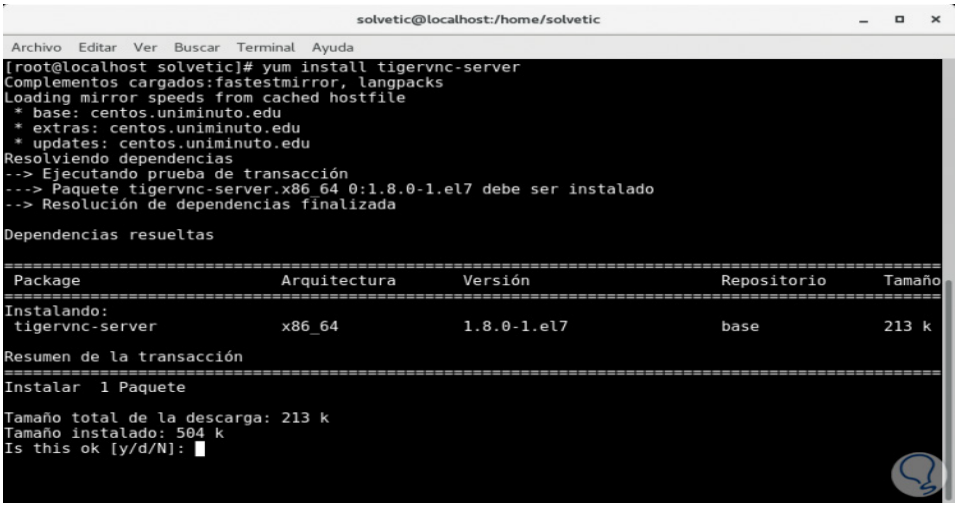


Figura 148: Instalación tigervnc-server.

Paso 2: Iniciar un usuario. Después de que la instalación ha sido correcta, vamos a iniciar sesión con el usuario que deseamos ejecutar en el programa VNC y ejecutaremos el siguiente comando en la terminal para configurar una contraseña para el servidor VNC: su – (Usuario) # (Si deseamos configurar el servidor VNC para que se ejecute bajo este usuario directamente desde la terminal CLI (interfaz de línea de comandos), sin cambiar usuarios de GUI).

vncpasswd

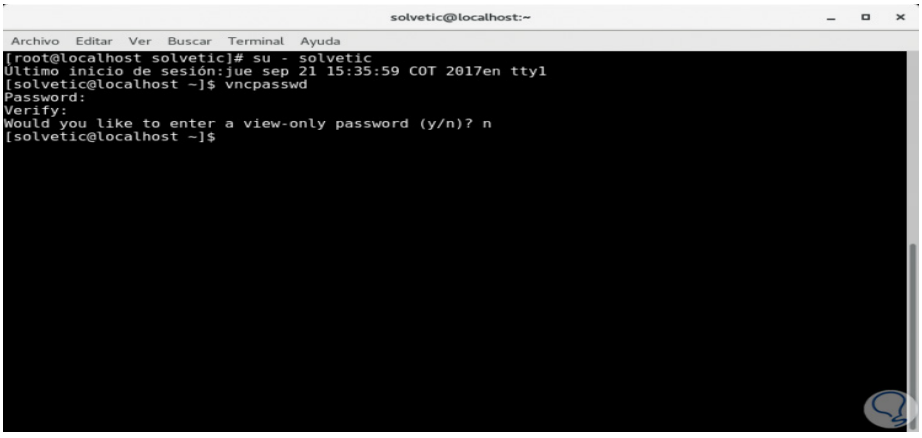


Figura 149: Iniciar un usuario.

Paso 3: Configurando VNC. Ahora será necesario agregar un archivo de configuración del servicio VNC para el usuario a través de un archivo de configuración del Daemon (Disco de ejecución de monitor) ubicado en el árbol de directorios system (sistemas de información empleados por las empresas operadoras de telecomunicaciones).

Para copiar el archivo de plantilla de VNC, será necesario el siguiente comando con privilegios de root:

Sudo cp /lib/systemd/system/vncserver@.service /etc/systemd/system/vncserver@:1.service

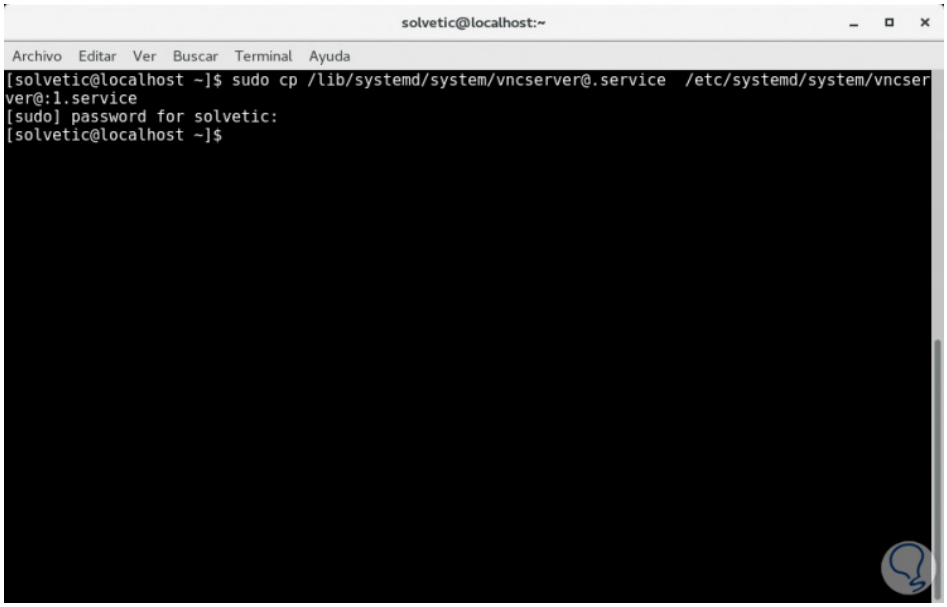


Figura 150: Archivos de configuración.

Paso 4: Editar archivos de configuración. El siguiente paso consiste en editar el archivo de configuración de plantilla de VNC el cual se encuentra en el directorio /etc/systemd/system/ y para ello usaremos el editor deseado: **nano /etc/systemd/system/vncserver@\:1.service**

Allí será necesario cambiar la línea USER por el nombre de nuestro usuario y estas serán las líneas:

[Unit]

Description=Remote desktop service (VNC)

After=syslog.target network.target

[Service]

Type=forking

ExecStartPre=/bin/sh -c '/usr/bin/vncserver -kill %i > /dev/null 2>&1 || :'

ExecStart=/sbin/runuser -l (Usuario) -c "/usr/bin/vncserver %i -geometry 1280x1024"

PIDFile=/home/(Usuario)/.vnc/%H%i.pid

ExecStop=/bin/sh -c '/usr/bin/vncserver -kill %i > /dev/null 2>&1 || :'

[Install]

WantedBy=multi-user.target

Ya reemplazado en la terminal queda de la siguiente manera.

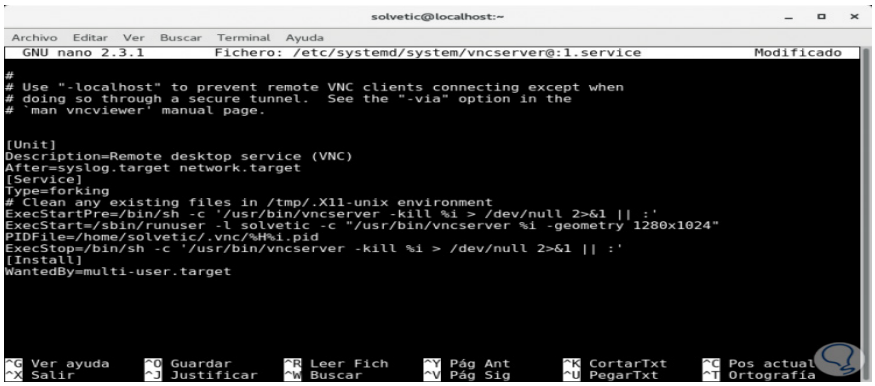


Figura 151: Clave servidor.

Paso 5: Reinicio del servidor**.** Guardaremos los cambios usando la combinación de teclas Crl + O y salimos del editor usando Crl + X. Ahora debemos reiniciar el servicio para aplicar los cambios que hemos ejecutado y para ello usaremos las siguientes líneas en su orden:

systemctl daemon-reload

systemctl start vncserver@:1

systemctl status vncserver@:1

systemctl enable vncserver@:1

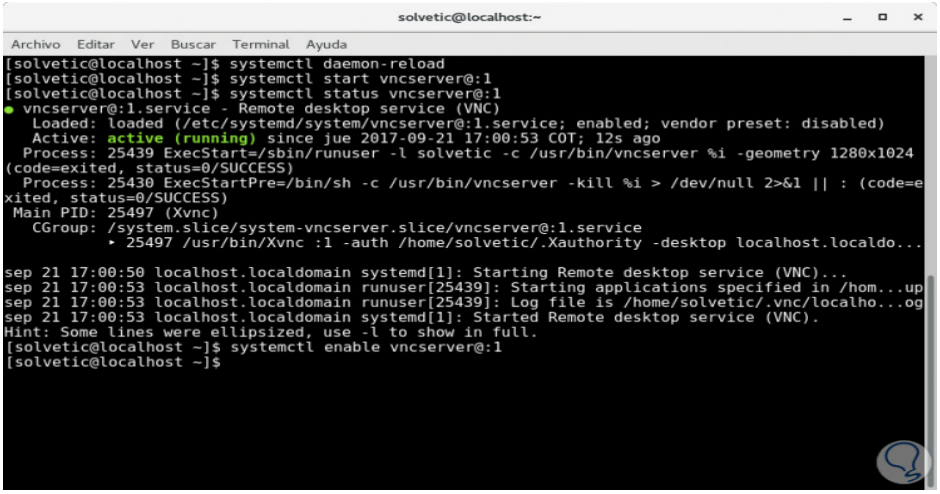


Figura 152: Reinicio del servidor.

Paso 6: Listado de puertos. Para listar los puertos abiertos en el estado de escucha del servidor VNC, ejecutaremos el comando ss (Comando, instrucción, sentencia) de la siguiente manera:

ss -tulpnl grep vnc

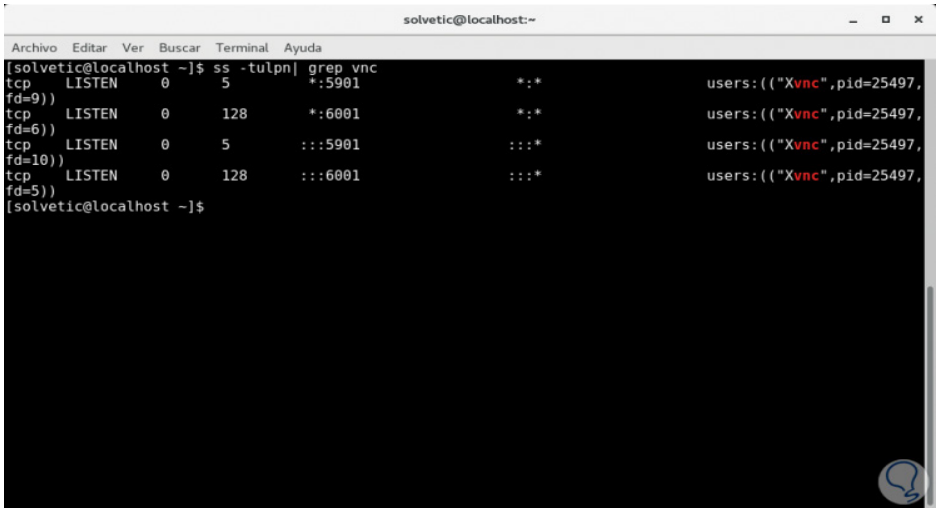


Figura 153: Listado de puertos.

Paso 7: Configuración del firewall. El siguiente paso consiste en permitir que los clientes VNC externos se conecten al servidor VNC en Centos 7.0 sin problemas, y para ello debemos asegurarnos de que los puertos abiertos VNC estén habilitados a través del cortafuegos.

En caso de que sólo se inicie una instancia del servidor VNC, sólo debe abrir el primer puerto VNC asignado: 5901/TCP (Protocolo de control de transmición), ejecutando los siguientes comandos en su orden:

firewall-cmd --add-port=5901/tcp

firewall-cmd --add-port=5901/tcp –permanent

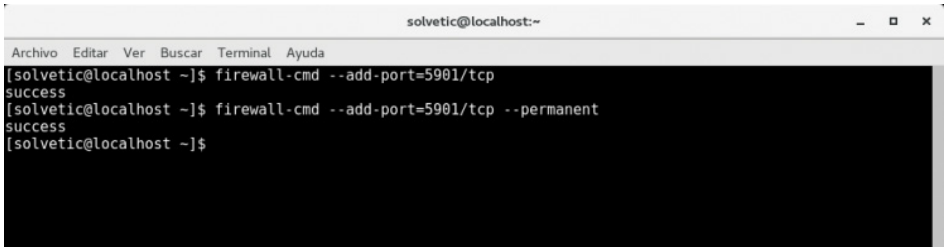


Figura 154: Configuración del firewall.

Paso 8: Conexión al equipo Centos 7.0 usando el cliente VNC. Al tratarse de un protocolo independiente de la plataforma, las conexiones VNC de interfaz gráfica de usuario remotas pueden ser usadas desde casi cualquier sistema operativo con una GUI (Interfaz grafica de usuario) y un cliente VNC especializado.

Para conectarnos de forma remota al escritorio de Centos 7.0 desde un sistema operativo de Microsoft, en este caso Windows 10, a través del protocolo VNC, ejecutaremos el programa VNC Viewer (solución de mantenimiento remoto excepcionalmente), ingresaremos la dirección IP y el número de puerto del servidor CentOS VNC de la siguiente forma:

Direccion_IP:5901

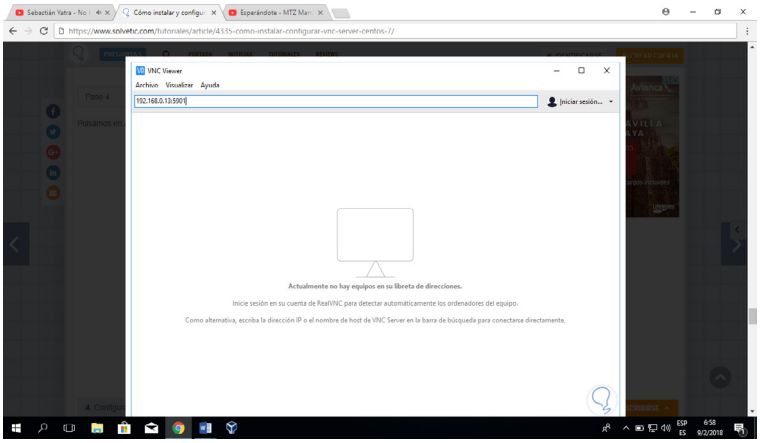


Figura 155: Conexión de forma remota desde cualquier SO.

Paso 9: Conexión al equipo Centos 7.0 usando el cliente VNC. Pulsamos "Enter" y será desplegado el siguiente mensaje de seguridad:

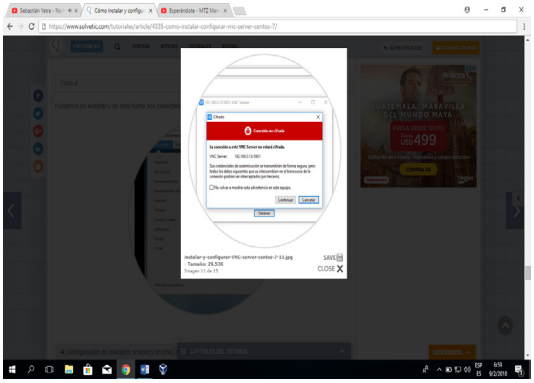


Figura 156: Conexión de forma remota desde cualquier SO.

Paso 10: Conexión al equipo Centos 7.0 usando el cliente VNC. Activamos la casilla "No volver a mostrar esta advertencia en este equipo" y pulsamos en "Continuar", luego será necesario agregar la respectiva contraseña de acceso que hemos configurado:

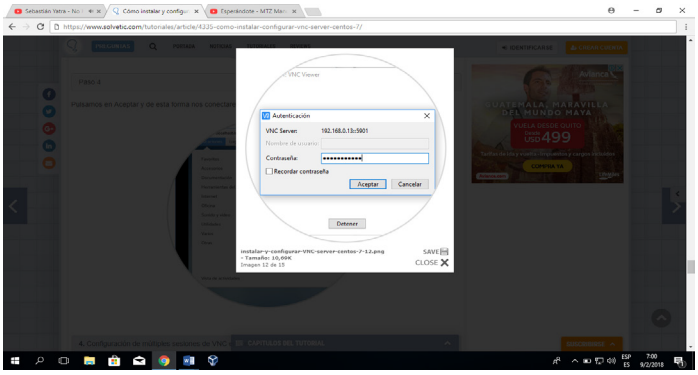


Figura 157: Conexión de forma remota desde cualquier SO.

Paso 11: Conexión al equipo Centos 7.0 usando el cliente VNC. Pulsamos en "Aceptar" y de esta forma nos conectaremos de forma remota al servidor Centos 7.0:

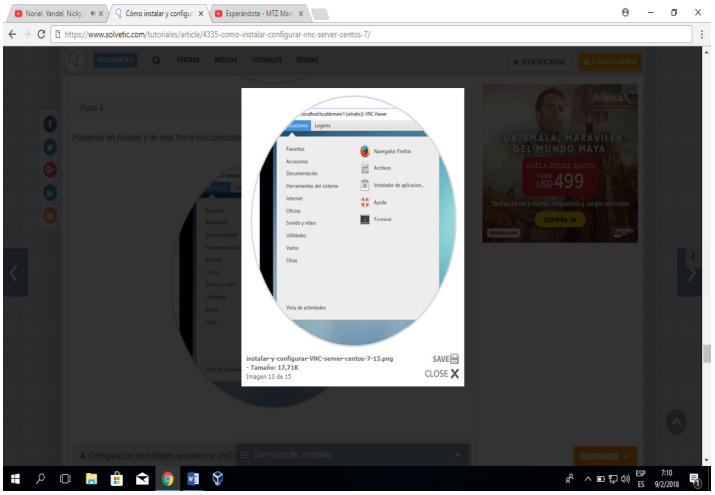


Figura 158: Conexión de forma remota desde cualquier SO.

CAPÍTULO 8:
INTRODUCCIÓN DE WEBMIN 1.7



En este capítulo usted encontrará:

- *Introducción a WebMin.*
- *Instalación de WEBMIN 1.7.*
- *Configuración de WEBMIN 1.7.*
- *Servidores.*
- *Trabajo en red.*
- *Hardware.*
- *Clúster.*

Introducción

Molina y Ortega (2014) expresan que Webmin se trata de un programa abierto escrito por Jaime Cameron que permite configurar la mayoría de las opciones de un sistema Linux. Es capaz de funcionar en más de 35 sistemas Unix/Linux diferentes, ofrece soporte a más de 20 lenguajes y en cada nueva versión da soporte a nuevas características del sistema operativo. La forma de acceder a Webmin una vez que está instalado en el sistema es a través de una ventana del navegador de Internet, especificando la dirección del propio equipo local. Este método permite también acceder a Webmin desde otro equipo distinto al que se encuentra instalado, lo que facilita las tareas de administración remota.

La herramienta Webmin está construida mediante módulos, lo que flexibiliza su configuración a la vez que facilita su actualización. Los módulos se dividen en categorías para que resulte más fácil su localización. Las categorías definidas por defecto en Webmin son las siguientes:

- **Webmin:** incluye los módulos de configuración propios de Webmin. Desde esta opción se puede configurar el propio programa Webmin (como el idioma, las cuentas de usuario que van a tener acceso a este programa, etc.).

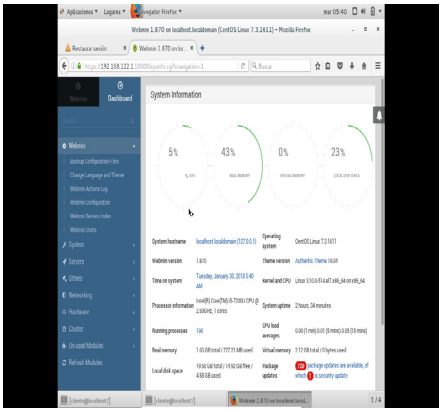


Figura 159: Configuración webmin.

- **Sistema:** aquí se encuentran los módulos relacionados con la configuración del sistema operativo. A este grupo pertenecen las opciones de configuración de los programas que se inician automáticamente en el arranque, instalar o desinstalar aplicaciones, gestionar cuentas de usuario y grupos, administrar sistemas de archivos locales y en red.

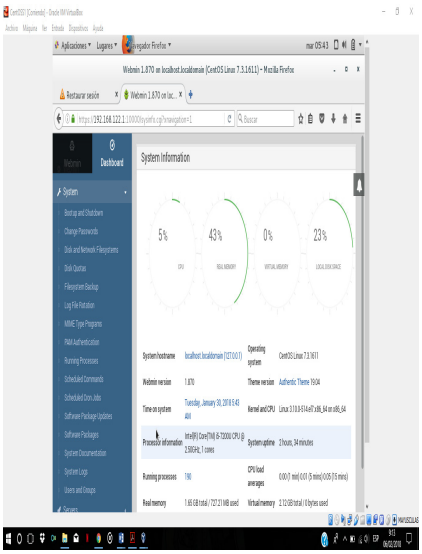


Figura 160: Opciones del sistema.

- **Servidores:** incluye los módulos de configuración de la mayoría de los programas servidores que se pueden instalar en el equipo. Aquí se incluyen opciones para compartir archivos con equipos Windows mediante Samba, configurar un servidor de correo electrónico, servidor de páginas Web, servidor de bases de datos, etc.

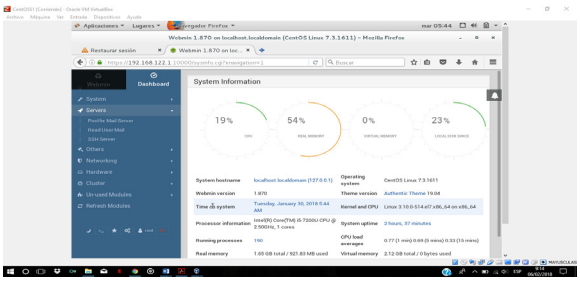


Figura 161: Opciones Servidores.

- **Trabajando en red:** aquí podemos encontrar los módulos de configuración de red del sistema, además de otros servicios como NFS, programa cortafuegos, etc.

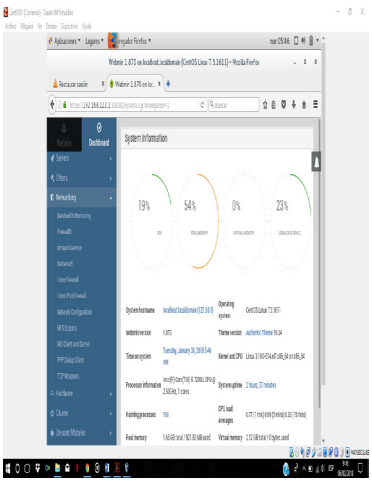


Figura 162: Opciones Networking.

- **Hardware:** esta opción incluye los módulos relacionados con la configuración de dispositivos hardware del sistema, como impresoras, discos duros, grabadoras de CD y DVD, sistemas RAID, etc.

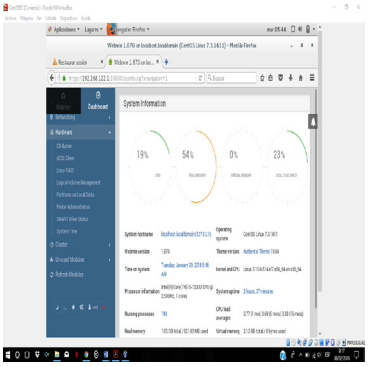


Figura 163: Opciones Hardware

- **Clúster:** incluye los módulos de configuración y administración de un sistema clúster (varios equipos conectados en red que funcionan como si fuera uno solo).

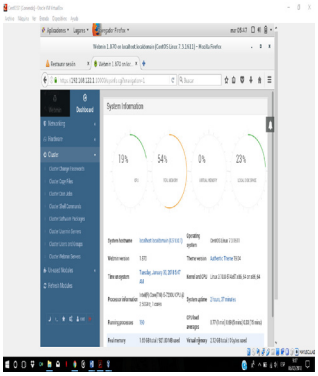


Figura 164: Opciones Cluster.

- **Otros:** esta categoría incluye otros módulos adicionales, entre los que podemos encontrar un administrador de archivos, línea de órdenes, órdenes ejecutadas habitualmente, entre otros.

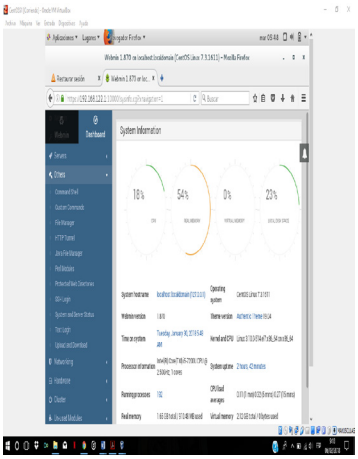


Figura 165: Otras opciones.

Microsoft (2009) manifiesta que la red compartida (NAT) está disponible para el primer adaptador de red en la máquina virtual. Permite a la máquina virtual compartir una conexión a una red física TCP/IP con el sistema operativo host. Esto resulta útil si se mueve el host a intervalos regulares entre distintas configuraciones de red, si se desea conectar la máquina virtual a Internet por medio de una conexión de marcación o de banda ancha usada por el host, incluida una conexión de red privada virtual (VPN), o si faltan direcciones IP. (p. 1)

Instalación y configuración de (“WEBMIN 1.7”)

Paso 1. Antes de iniciar con la instalación verificamos que la máquina virtual en la cual se instalará Webmin se encuentre en red NAT ingresando a la opción de configuración de la máquina virtual y luego a la opción red.

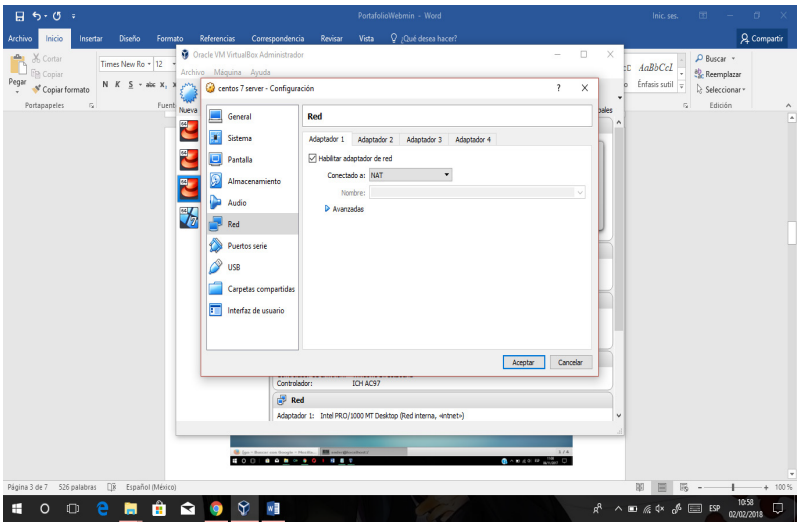


Figura 166: Verificación que esté conectado a NAT.

Paso 2. Descargamos e instalamos Webmin usando el comando:

wget http://prdownloads.sourceforge.net/webadmin/webmin-1.870-1.noarch.rpm

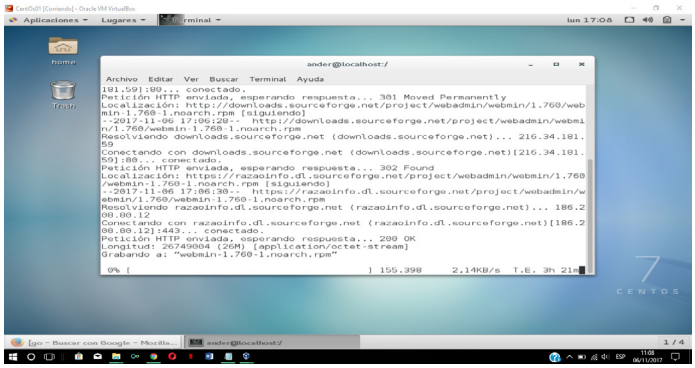


Figura 167: matamos el proceso con el comando kill -9 número pid.

Paso 3. Para la instalación solicitará las dependencias, para lo cual utilizamos el siguiente comando:

yum install perl

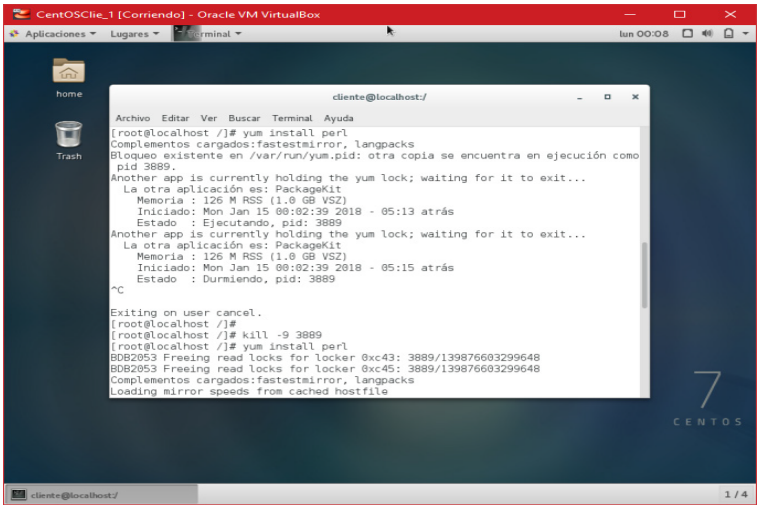


Figura 168: matamos el proceso con el comando kill -9 número pid:3889

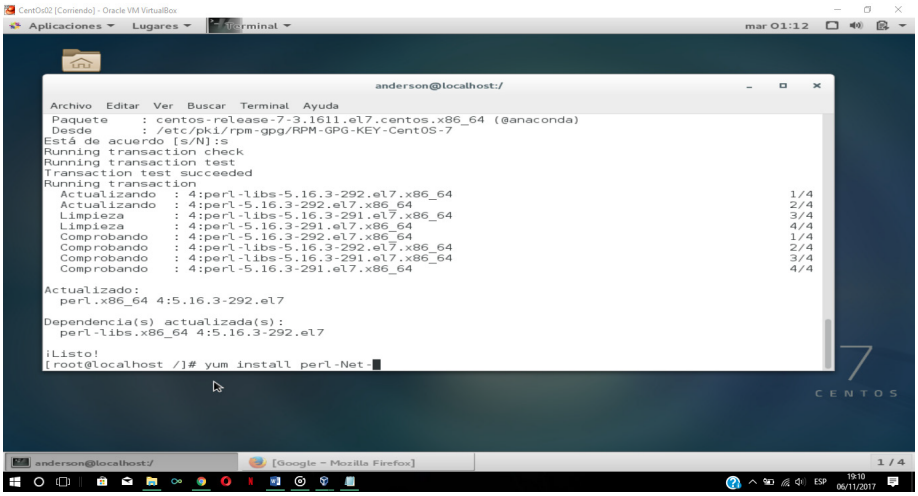


Figura 169: yum install perl- Net.

Paso 4. Una vez descargadas todas las dependencias procedemos a instalar Webmin usando el comando webmin.rpm-1.860-1.noarch.rpm

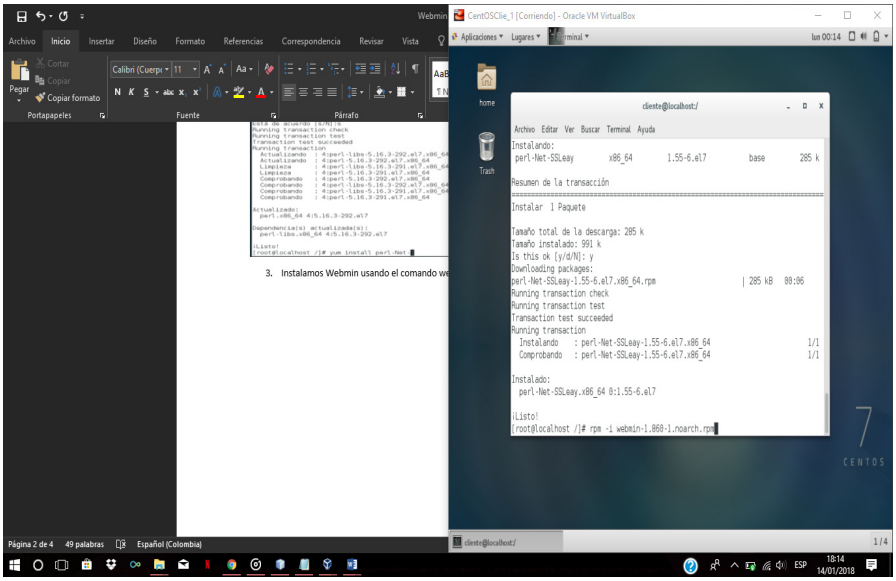


Figura 170: comando webmin.rpm-1.860-1.noarch.rpm.

Paso 5. Iniciamos el servicio Webmin usando el comando: service Webmin start y el comando chkconfig Webmin on.

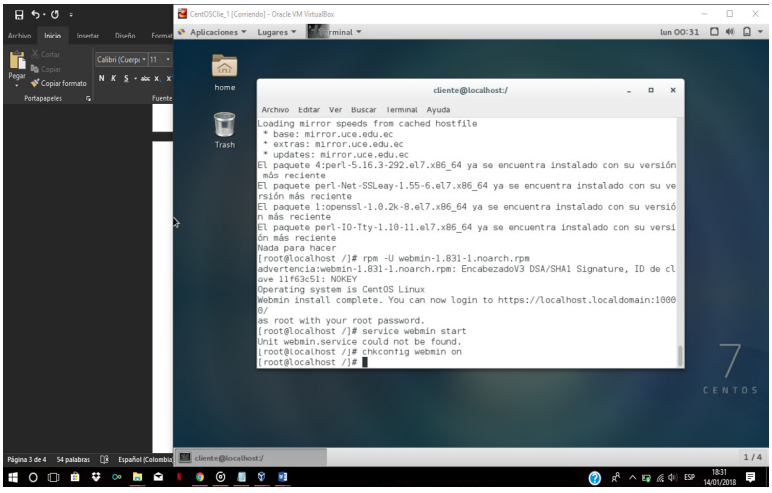


Figura 171: El comando chkconfig puede ser usado para activar y desactivar servicio.

Paso 6. Verificamos la dirección IP del servidor por el cual vamos a ingresar a Webmin mediante el comando ifconfig.

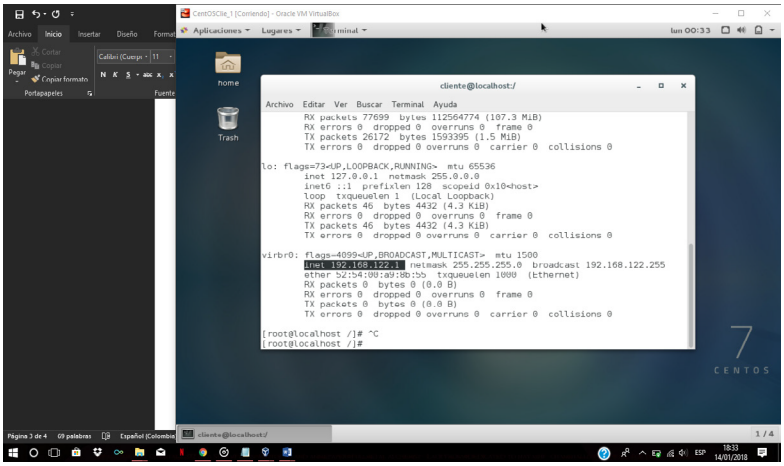


Figura 172: Aplicación Ifconfig.

Paso 7. Ingresamos como usuario root e ingresamos la respectiva contraseña root en este caso la contraseña es: root123

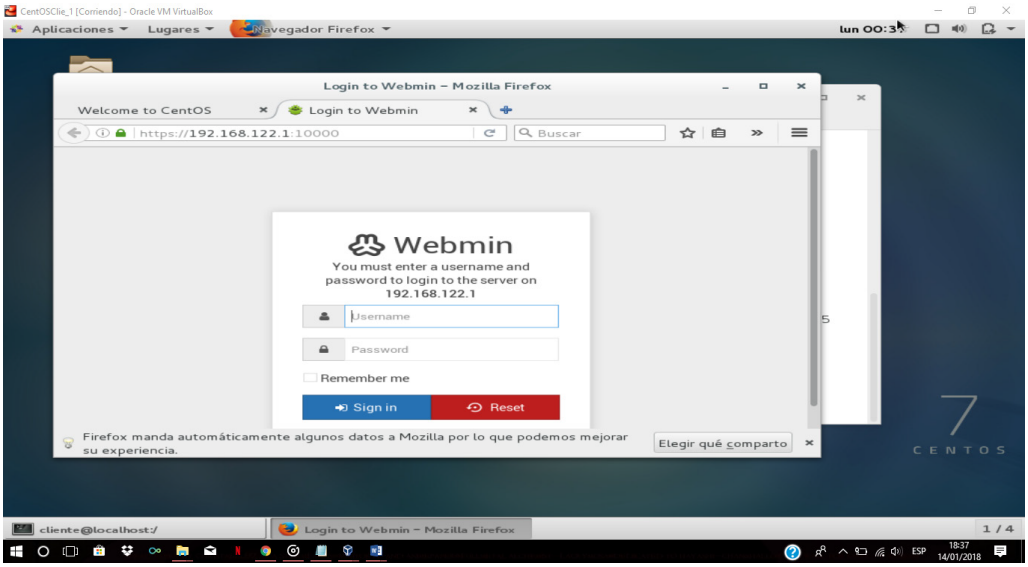


Figura 173: Ingresamos la dirección IP(192.168.122.1) seguido del puerto 10000.

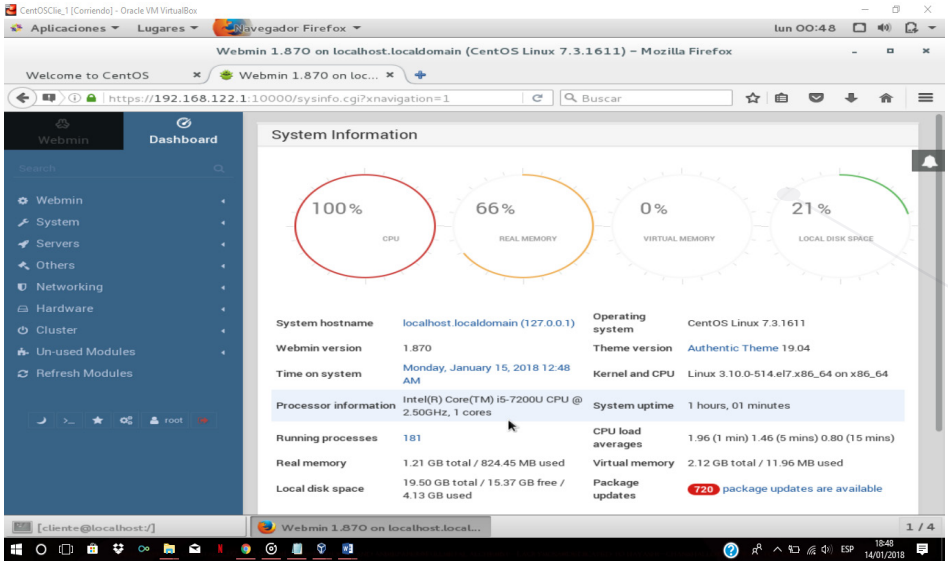


Figura 174: Ingreso como usuario root.

CAPÍTULO 9:
INTRODUCCIÓN DE JOOMLA 3.8



En este capítulo usted encontrará:

- *Introducción a Joomla 3.8.*
- *Instalación de Joomla 3.8.*
- *Configuración de Joomla 3.8.*
- *Habilitación de la base de datos.*

Introducción

Joomla es un sistema de gestión de contenidos que permite desarrollar sitios web dinámicos e interactivos. Permite crear, modificar o eliminar contenido de un sitio web de manera sencilla a través de un «panel de administración». Es un software de código abierto, programado o desarrollado en PHP y liberado bajo Licencia pública general GNU (GPL).

Este administrador de contenidos puede utilizarse en una computadora personal local (localhost), en una intranet o a través de Internet, y requiere para su funcionamiento una base de datos creada con un motor de bases de datos (MySQL es lo más habitual), así como de un servidor HTTP Apache y Php.

Instalación y configuración de Joomla 3.8

Paso 1: Abrimos una ventana e iniciamos como administrador con el siguiente comando: SU

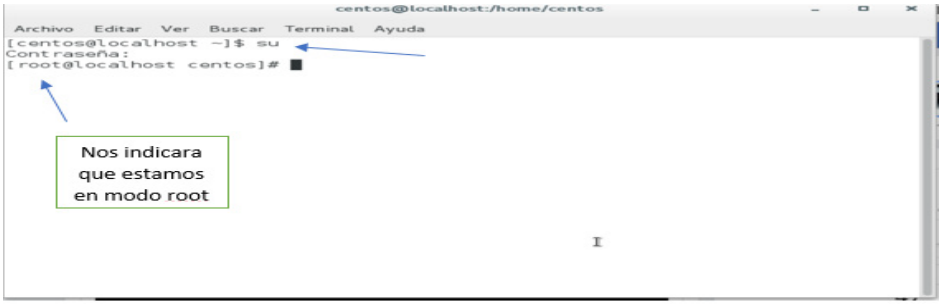


Figura 175:Comando SU.

Paso 2: Ahora tendremos que instalar mariadb: yum –y install mariadb-server mariadb.



Figura 176:Instalar la base de datos.

Paso 3: Luego nos indicará que ya está instalado:

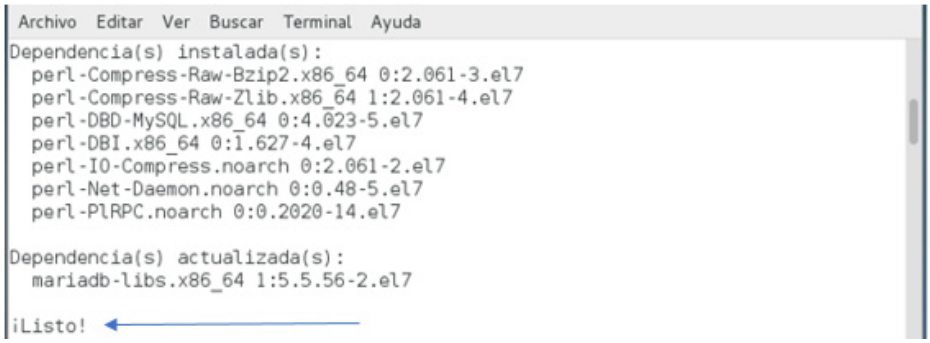


Figura 177:Confirmación de instalación.

Paso 4: Ahora iniciamos y habilitamos la mariadb:

- Systemctl start mariadb. service
- Systemctl enable mariadb. Service

```
[root@localhost mjaramillo]# systemctl start mariadb.service
[root@localhost mjaramillo]# systemctl enable mariadb.service
Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service
 to /usr/lib/systemd/system/mariadb.service.
```

Figura 178:Iniciar la base de datos.

Paso 5: Ahora instalaremos la base de datos mysql, nos pedirá una contraseña la creamos: mysql_secure_installation

```
[root@localhost mjaramillo]# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
```

Figura 179: Instalar la base de datos.

Paso 6: Se debe seleccionar los paquetes que se desea que se instalen colocando lo siguiente: y: y: n: y: y.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] n
 ... skipping.

By default, MariaDB comes with a database named 'test' that anyone can
```

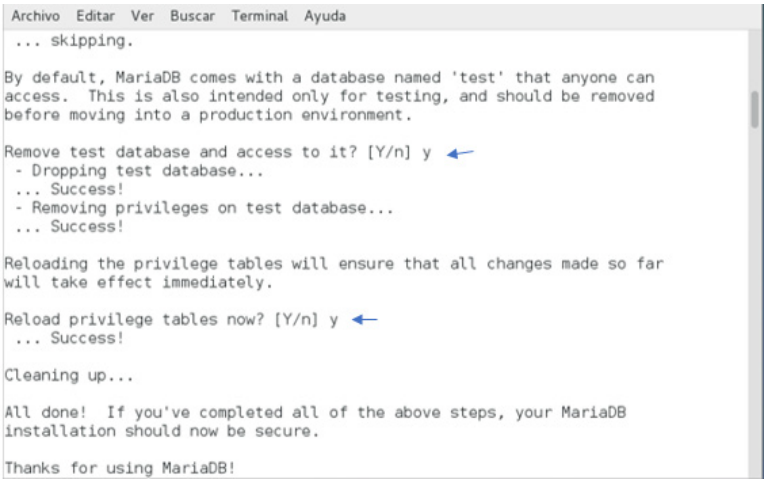


Figura 180: Selección de paquetes.

Paso 7: Ahora instale el servidor web Apache con el siguiente comando: yum –y install httpd

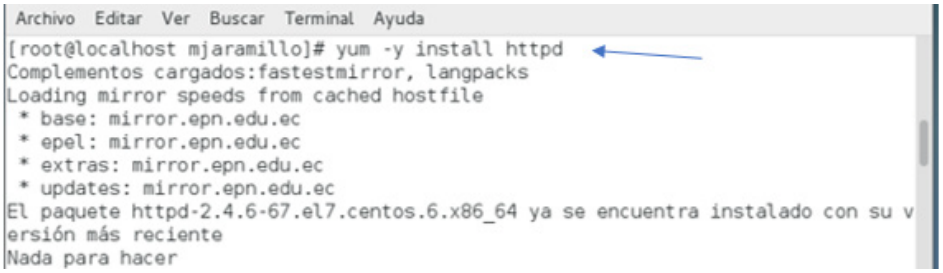


Figura 181: Instalación del web apache.

Paso 8: Habilitamos el servicio: Systemctl enable httpd.service

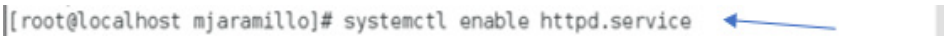


Figura 182:Habilitación del servicio.

Paso 9: Habilitaremos los servicios y haremos permanentes los archivos.

Firewall -cmd --permanet --zone=public --add-service=https

```
[root@localhost mjaramillo]# firewall-cmd --permanent --zone=public --add-servic
e=https
success
```

Figura 183: Archivos permanentes.

Paso 10:

```
[root@localhost mjaramillo]# firewall-cmd --permanent --zone=public --add-servic
e=https
Warning: ALREADY_ENABLED: https
success
```

Figura 184: Firewall -cmd --permanet --zone=public --add-service=https

Paso 11:

```
[root@localhost mjaramillo]# firewall-cmd --permanent --zone=public --add-servic
e=http
success
```

Figura 185: Firewall -cmd --permanet --zone=public --add-service=https

Paso 12:

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@localhost mjaramillo]# firewall-cmd --permanent --zone=public --add-servic
e=https
Warning: ALREADY_ENABLED: https
success
```

Figura 186: Firewall -cmd --permanet --zone=public --add-service=https

Paso 13: Una vez habilitados los servicios procedemos a instalar php: yum –y install php

```
[root@localhost mjaramillo]# yum -y install php
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.epn.edu.ec
 * epel: mirror.epn.edu.ec
 * extras: mirror.epn.edu.ec
 * updates: mirror.epn.edu.ec
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete php.x86_64 0:5.4.16-43.el7_4 debe ser instalado
--> Procesando dependencias: php-common(x86-64) = 5.4.16-43.el7_4 para el paquet
e: php-5.4.16-43.el7_4.x86_64
--> Procesando dependencias: php-cli(x86-64) = 5.4.16-43.el7_4 para el paquete:
php-5.4.16-43.el7_4.x86_64
--> Procesando dependencias: libcrypto.so.10(OPENSSL_1.0.2)(64bit) para el paque
te: php-5.4.16-43.el7_4.x86_64
--> Ejecutando prueba de transacción
---> Paquete openssl-libs.x86_64 1:1.0.1e-60.el7 debe ser actualizado
--> Procesando dependencias: openssl-libs(x86-64) = 1:1.0.1e-60.el7 para el paqu
ete: 1:openssl-1.0.1e-60.el7.x86_64
```

Figura 187:Instalar el php.

Paso 14: Una vez instalado el paquete php instalaremos los paquetes nano con el siguiente comando: Yum –y install nano.

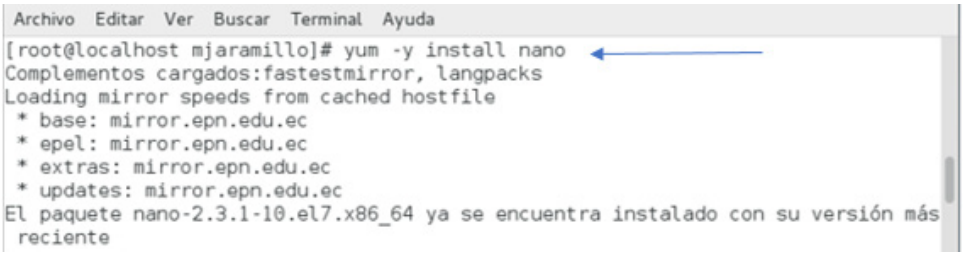


Figura 188:Paquetes nano.

Paso 15: Ingresamos al directorio y cargaremos los archivos en el servidor:

nano /var/www/html/info.php

yum search php

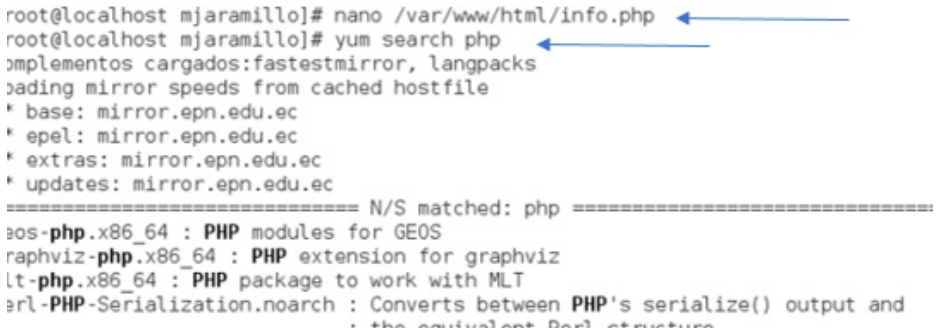


Figura 189: Activación de directorios.

Paso 16: Instalaremos mysql junto con php: yum –y install php-mysql



```
Dependencia(s) instalada(s):
  php-pdo.x86_64 0:5.4.16-43.el7_4

¡Listo!
```

Figura 190:Instalación del mysql y php.

Paso 17: Cargaremos los archivos a mysql: Yum –y install php-gb php-ldap php-odbc php-pear php-xml php-xmlrpc php-mbstring php-snmp php-soap curl-devel.

```
[root@localhost mjaramillo]# yum -y install php-gd php-ldap php-odbc php-pear ph
p-xml php-xmlrpc php-mbstring php-snmp php-soap curl curl-devel
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.epn.edu.ec
 * epel: mirror.epn.edu.ec
 * extras: mirror.epn.edu.ec
 * updates: mirror.epn.edu.ec
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete curl.x86_64 0:7.29.0-35.el7.centos debe ser actualizado
---> Paquete curl.x86_64 0:7.29.0-42.el7_4.1 debe ser una actualización
--> Procesando dependencias: libcurl = 7.29.0-42.el7_4.1 para el paquete: curl-7
.29.0-42.el7_4.1.x86_64
---> Paquete libcurl-devel.x86_64 0:7.29.0-42.el7_4.1 debe ser instalado
updates/7/x86_64/filelists_db                              | 2.1 MB     00:28
---> Paquete php-gd.x86_64 0:5.4.16-43.el7_4 debe ser instalado
--> Procesando dependencias: libt1.so.5()(64bit) para el paquete: php-gd-5.4.16-
43.el7_4.x86_64
```

Figura 191:Cargar archivos.

Paso 18: Una vez acabado de instalar nos dirigiremos a nuestro navegador y colocamos la siguiente ruta nos direccionará al servidor de php:

localhost/info.php

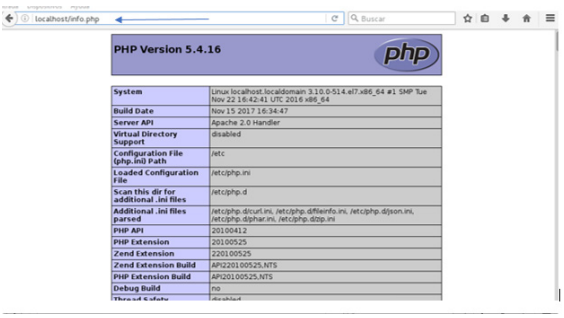


Figura 192:ventana del navegador

Paso 19: Se deberá ingresar el usuario root y contraseña creada en la base de datos, buscaremos nuestro paquete que instalamos y nos re direccionará nueva a Joomla.

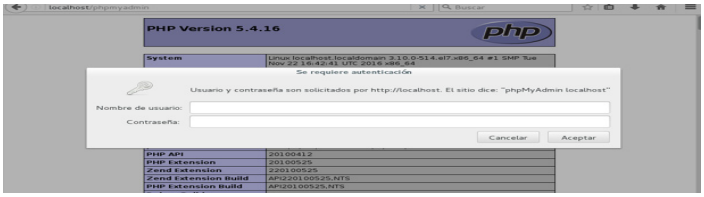


Figura 193:Inicio de sesión.

Paso 20: Nos visualiza una pantalla como la que se muestra a continuación, buscaremos nuestro paquete instalado.

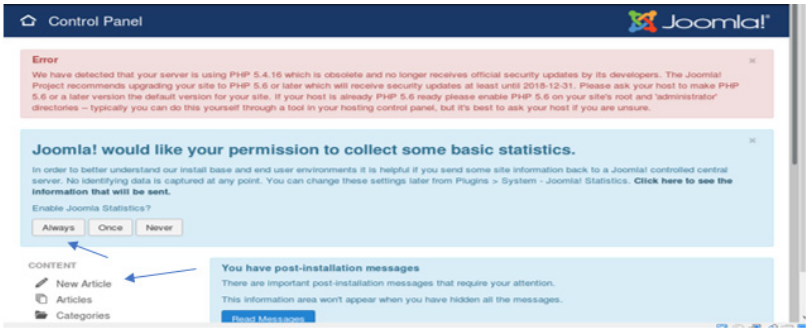


Figura 194: Paquetes instalados.

Paso 21: Nos mostrará la siguiente ventana. Aquí podremos verificar si están instalados y dados los privilegios de usuario.



Figura 195:Privilegios de usuario.

Paso 22: Configuramos Joomla en Linux CentOS vía web. Abrimos un navegador en otro pc y nos vamos a la ip del servidor http://ip-servidor-joomla/joomla

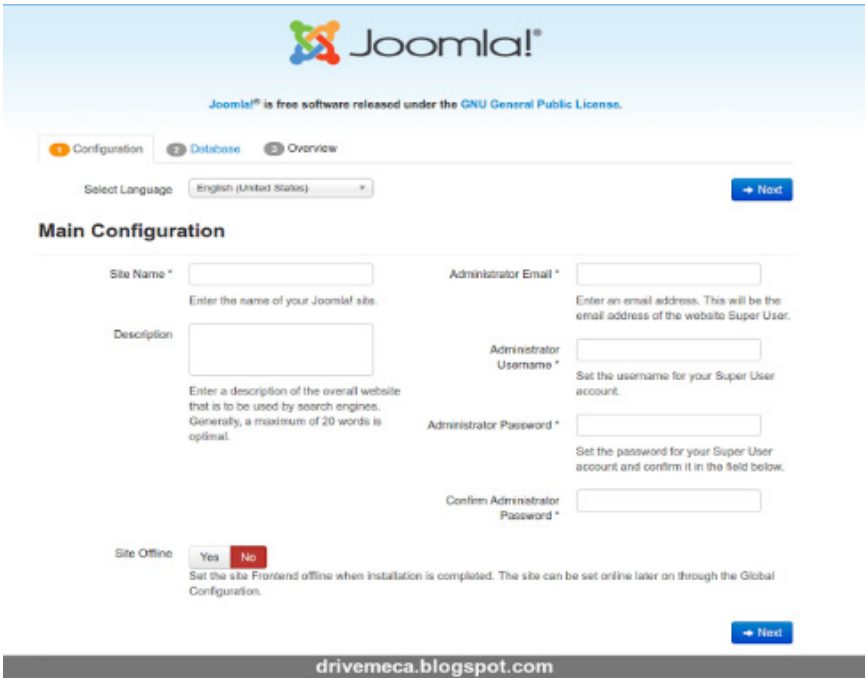


Figura 196:Configuración de Joomla

Paso 23: Seleccionamos el idioma a español por medio de la caja "Seleccionar el idioma". Automáticamente refrescará la página y ya se verá en español. Llenamos los demás campos teniendo cuidado de colocar un email valido en **El correo electrónico del administrador,** ya que este será usado como destino para resetear la contraseña si acaso de olvido.



Figura 197:Configuración pantalla principal.

Paso 24: Una vez lleno los campos. Hacemos clic al botón "Siguiente".

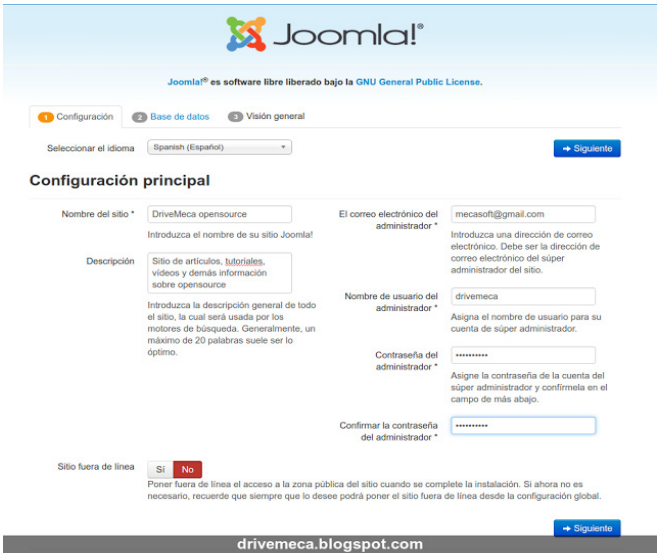


Figura 198:Confirmamos los datos

Paso 25: Seguimos los siguientes pasos para continuar con la instalación, en este ejemplo es joomlausr

- configuración de la conexión a la base de datos
- colocando en Tipo de base de datos MySQLi,
- **Hospedaje localhost,**
- Usuario el que creamos
- Contraseña (la que le creamos al usuario de la base de datos) y Base de datos joomladb.
- Hacemos clic al botón Continuar



Figura 199: Instalación joomlausr.

Paso 26: Se da la opción de instalar datos de ejemplo para generar páginas. Hacemos un rápido vistazo a que todo esté correcto.



Figura 200: Instalación datos de ejemplo.

Paso 27: Verificamos estén todas las extensiones php habilitadas y hacemos clic al botón "Siguiente".



Figura 201: Verificación de extensiones php.

Paso 28: Joomla está instalado en el servidor Linux Centos. Ahora hacemos clic al botón Eliminar carpeta de instalación.

Ya eliminada podemos entrar dando clic al botón Administración



Figura 202: logeo con usuario administrador.

Paso 29:



Figura 203: Inicio de sesión en Joomla

Se muestra la ventana el dashboard de Joomla preguntándonos si se desea permitir el envío de estadísticas a los desarrolladores, recomendable, en este caso hacemos clic **a Always.**

CAPÍTULO 10:
INTRODUCCIÓN DE WINE 1.7



En este capítulo usted encontrará:

- *Introducción a Wine.*
- *Instalación y Configuración de Wine 1.7.*
- *Explicación de comandos para Wine.*

Introducción

Wine es una plataforma que permite instalar software nativo para Windows en cualquier distribución Linux, FreeBSD, Solaris, Mac OS X y otros sistemas operativos.

Instalación y configuración de Wine 1.7

Paso 1: Ingresemos como super usuario. Luego ejecutamos los siguientes comandos .

```
[root@localhost diegofig]# ls
Descargas   jcameron-key.asc    Público                    wine-1.7.9.tar.bz2
Documentos  jcameron-key.asc.1  Vídeos
Escritorio  Música              webmin-1.870-1.noarch.rpm
Imágenes    Plantillas          wine-1.7.9
[root@localhost diegofig]# yum -y install libX11-devel freetype-devel
Complementos cargados:fastestmirror, langpacks
Webmin                                                   | 1.0 kB     00:00
base                                                     | 3.6 kB     00:00
extras                                                   | 3.4 kB     00:00
updates                                                  | 3.4 kB     00:00
(1/2): extras/7/x86_64/primary_db                          | 166 kB   00:02
(2/2): updates/7/x86_64/primary_db                         | 6.0 MB   00:39
Loading mirror speeds from cached hostfile
 * base: centos.uniminuto.edu
 * epel: mirror.globo.com
 * extras: centos.uniminuto.edu
 * updates: centos.ufes.br
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete freetype-devel.x86_64 0:2.4.11-15.el7 debe ser instalado
--> Procesando dependencias: zlib-devel para el paquete: freetype-devel-2.4.11-1
5.el7.x86_64
```

Figura 204: yum -y install libx11 -devel freetype-devel para instalar los paquetes de wine.

Paso 2: Debemos esperar los todos procesos de instalación, ya que son muchos paquetes.

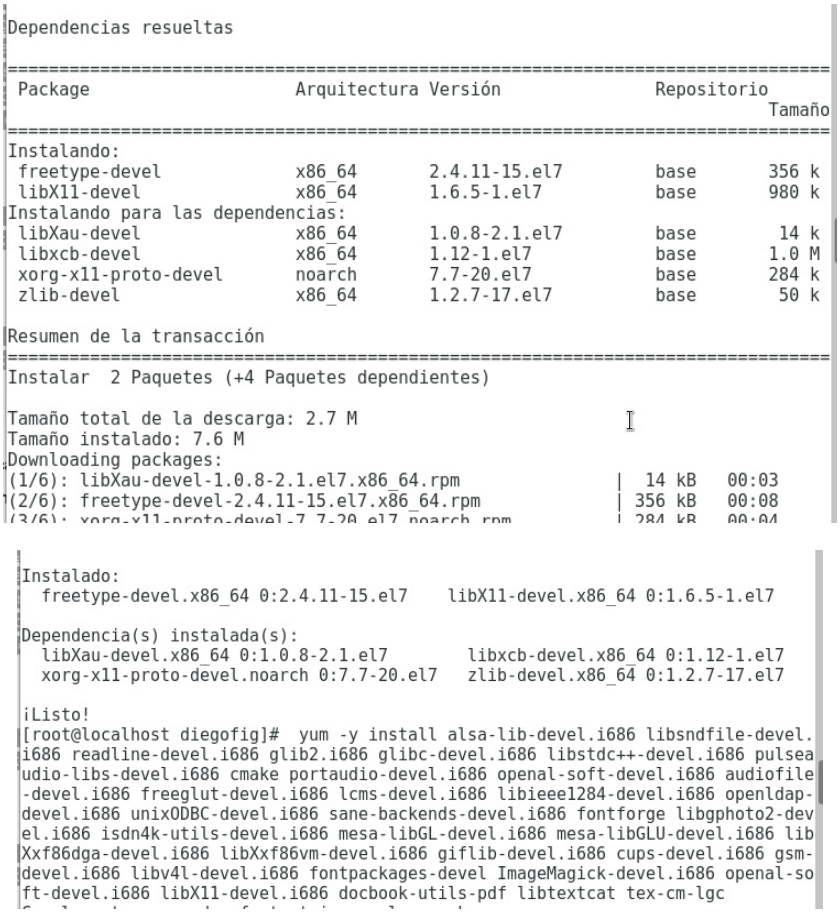


Figura 205: Proceso de instalación.

Paso 3: pwd : Sirve para mostrar nuestra ubicación en el terminal

Paso 4: mkdir wine64: permite ejecutar wine pero depende de nuestro bits del sistema.

Paso 5: ls : Para mostrar si efectivamente esta instalado wine

Paso 6: cd wine64: sirve para ir a la carpeta de wine64 y trabajar dentro de este directorio

Paso 7: ../wine-1.7.9/configure –enable-win64: Este comando sirve para habilitar los servicios de wine

Los pasos del 3 al 7 se muestran en la siguiente imagen, de la manera en que deben ser ejecutados.

```
¡Listo!
[root@localhost diegofig]# pwd
/home/diegofig
[root@localhost diegofig]# mkdir wine64
[root@localhost diegofig]# ls
Descargas   jcameron-key.asc    Público                    wine-1.7.9.tar.bz2
Documentos  jcameron-key.asc.1  Vídeos                     wine64
Escritorio  Música              webmin-1.870-1.noarch.rpm
Imágenes    Plantillas          wine-1.7.9
[root@localhost diegofig]# cd wine64
[root@localhost wine64]# ls
[root@localhost wine64]# ../wine-1.7.9/configure --enable-win64
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking whether make sets $(MAKE)... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
```

Figura 206: Orden de ejecución de comandos.

Paso 8: make > make.log 2>&1 sirve para hacer la instalación desde el repositorio que instalamos anteriormente

```
configure: libcapi20 development files not found, ISDN won't be supported.
configure: libgsm development files not found, gsm 06.10 codec won't be supporte
d.
configure: libmpg123 development files not found (or too old), mp3 codec won't b
e supported.

configure: Finished.  Do 'make' to compile Wine.

[root@localhost wine64]# make > make.log 2>&1
```

Figura 207: make > make.log 2>&1

Paso 9: Para este paso abrimos otra ventana en el terminal y tecleamos el comando cd wine64 al repositorio de wine64 y luego ls para mostar los config log.

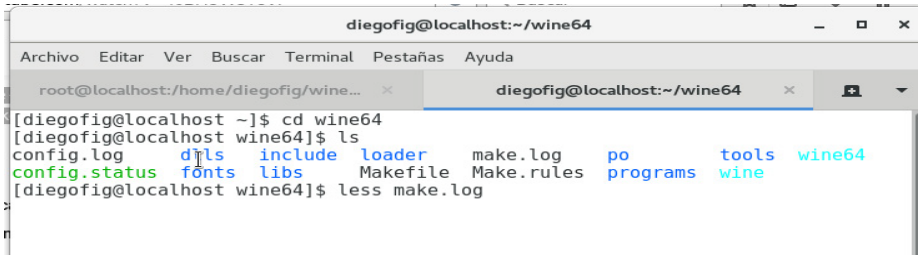


Figura 208: ls para mostar los config log.

Paso 10: Finalmente este comando sirve para hacer la instalacion de Wine.

```
[root@localhost wine64]# cd ..
[root@localhost diegofig]# mkdir wine32
mkdir: no se puede crear el directorio «wine32»: El fichero ya existe
[root@localhost diegofig]# cd wine32
[root@localhost wine32]# ../wine-1.7.9/configure --with-wine64=../wine64
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking whether make sets $(MAKE)... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
```

Figura 209: comando make install

Paso 11: Finalmente, luego de terminar la instalación de los diferentes paquetes, obtenemos las siguientes carpetas creadas en nuestro directorio, todo eso conseguido mediante conmandos.

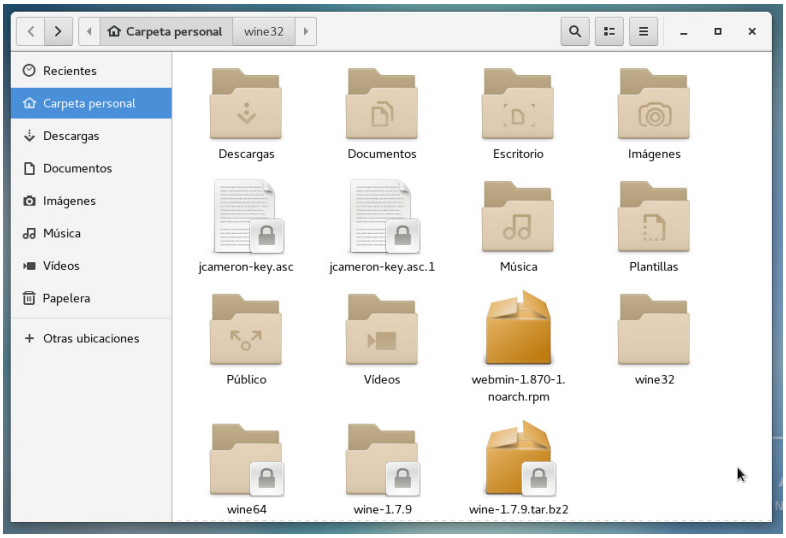


Figura 210: carpetas creadas mediante comandos.

Paso 12: Se puede visualizar las carpetas donde está alojado el emulador Wine, por ejemplo, dentro de la versión 1.7.9 se alojaron muchos contenidos que sirven para levantar o ejecutar la aplicación propia para el sistema operativo Windows en Centos de Linux.

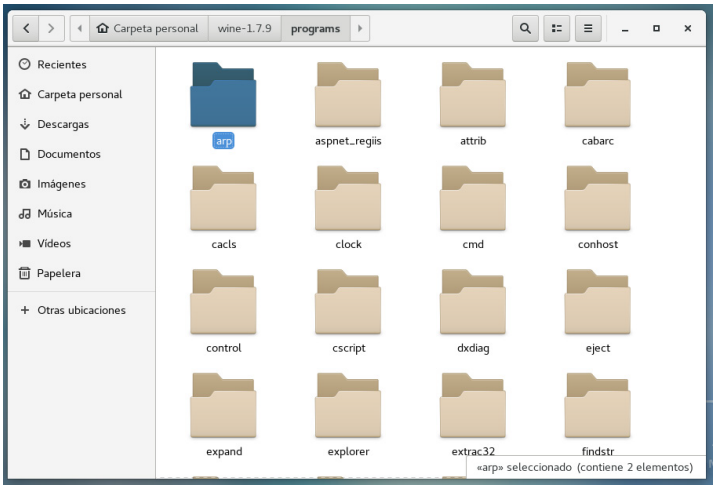


Figura 211: emulador Wine.

Paso 13: Wine en nuestro sistema aparecerá como un icono en el que podremos ingresar como cualquier aplicación.

Configuración de Wine 1.7

Desde el menú “Applications > Wine”, abrir “Wine Configuration”:

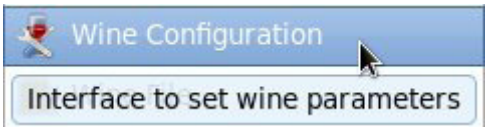


Figura 212: Abrir Wine configuración.

Paso 14: Dentro de wine se podrá observar todas sus configuraciones.

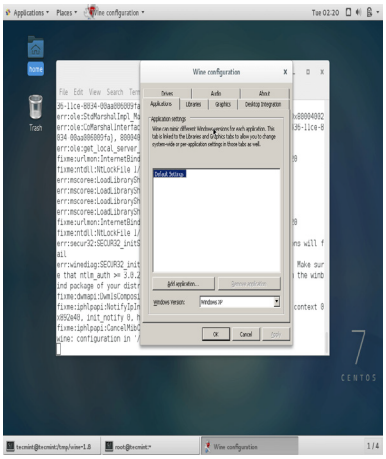


Figura 213: Configuración de Wine.

Paso 15: Luego de configurar Wine podemos instalar cualquier aplicación de Windows en Centos, para hacer esto primero debemos descargar una aplicacion desde torret, luego hacer click derecho sobre el archivo ejecutable para proceder a instalar la aplicación, abrir con Wine, de esta manera se se abrirá la ventana de instalación del programa y se procede a instalar como lo haríamos en Windows.

Se debe descargar aplicaciones que sean compatibles con Wine, debido a que Wine es limitado.

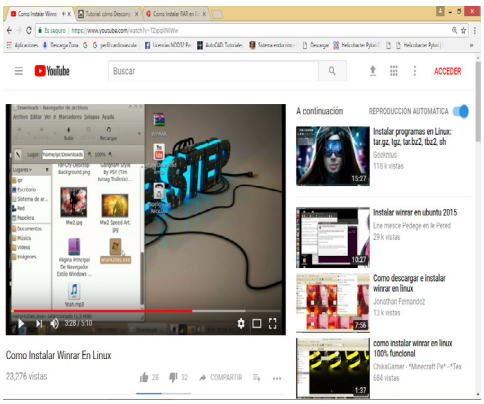


Figura 214: Aplicaciones compatibles con Wine.

Paso 16: Después de descargar cualquier juego o aplicación debebemos hacer clic derecho sobre el archivo ejecutable y lo abrimos con Wine, y procederá la instalación como cualquier programa a lo que estamos acostumbrados con Windows.

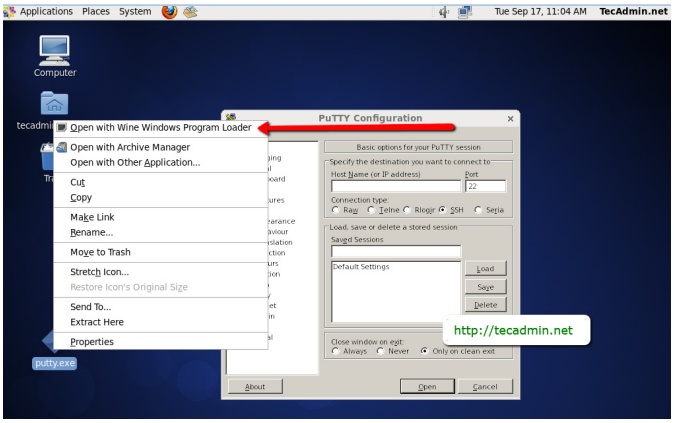


Figura 215: Instalación de aplicativos

De esta forma ya podemos utilizar esta aplicación en Centos.

CAPÍTULO 11:
INTRODUCCIÓN DE IPSEC



En este capítulo usted encontrará:

- *Instalación de IPSEC.*
- *Configuración de IPSEC.*
- *Reconociendo strongswan haveged.*

Introducción

Ipsec es un conjunto de protocolos de red seguro que autentica y cifra los paquetes de datos enviados a través de una red IPv4. IPv4, en su desarrollo inicial, aplicó pocas disposiciones de seguridad, lo que originó que esta versión de IP resulte incompleta, dejando cualquier mejora para futuras investigaciones. IPsec incluye protocolos para establecer la autenticación mutua entre agentes al inicio de una sesión y la negociación de claves criptográficas para usar durante la sesión. IPsec puede proteger los flujos de datos entre un par de hosts (host a host), entre un par de pasarelas de seguridad (red a red) o entre una pasarela de seguridad y un host (red a host).

Ipsec utiliza servicios de seguridad criptográfica para la protección de las comunicaciones que viajan a través de las redes del protocolo de Internet (IP). De igual forma se admite la autenticación entre iguales a nivel de red, la autenticación de origen de datos, la integridad de datos, la confidencialidad de datos (cifrado) y la protección de repetición.

IPsec definitivamente no es una VPN, algunos lo tratan como tal, pero no lo es, no tiene el mismo comportamiento, aunque en la práctica puede funcionar haciendo túneles asegurando dos puntos remotos, aun así, no es igual a una VPN.

¿Por qué existe IPsec si hay soluciones VPN? IPsec actualmente funciona en el internet actual IPV4 porque fue portado de su

protocolo nativo el IPV6, en IPV6 tiene todo el sentido del mundo y las VPN no tienen ningún sentido en IPV6, en IPV4 IPsec no tiene tanto sentido, su funcionamiento está pensado para pares iguales. Aunque puede manejar NAT transversal, eso ya no es natural en un protocolo como IPSec.

Para hacerlo más simple de entender vamos a hacerlo en equivalencia de analogía de algo que en teoría todos conocen hoy.

Si conocemos la diferencia entre HTTP y HTTPS, entonces TCP/IP sería equivalente a HTTP e IPsec sería equivalente a HTTPS, seguridad en la capa 3.

En IPsec.conf se describen dos cosas: ¿Cuál es su ip a la que se aplicará la seguridad? ¿Qué redes se pueden encontrar de su lado? ¿A qué IP remota quiere llegar con seguridad y qué redes espera encontrar del lado remoto?

El segundo archivo es el de secretos (archivo. secrets). Este archivo es el que describe la llave que se usará para cifrar la conexión entre ambas IPs, asumiendo que ya se tiene compilado el OpensWan o LibreSwam o instalado con su paquete de distribución.

Instalación y configuración de IPESEC

Paso 1: Como primer paso, vamos a instalar el strongswan haveged, ya que es una herramienta que va a servir para generar números aleatorios al momento de generar certificados.

```
[root@localhost ~]# yum install strongswan haveged
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.cedia.org.ec
 * epel: mirror.cedia.org.ec
 * extras: mirror.cedia.org.ec
 * updates: mirror.cedia.org.ec
El paquete strongswan-5.4.0-2.el7.x86_64 ya se encuentra instalado con su versió
n más reciente
El paquete haveged-1.9.1-1.el7.x86_64 ya se encuentra instalado con su versión m
ás reciente
Nada para hacer
```

Figura 216: Instalar el strongwan.

Una vez instalado strongswan haveged lo iniciaremos.

```
[root@localhost ~]# systemctl start havged
Failed to start havged.service: Unit havged.service failed to load: No such file
 or directory.
[root@localhost ~]# systemctl start haveged
[root@localhost ~]#
```

Figura 217:Iniciar el strongwan.

Paso 2: Luego de correr el strongswan haveged vamos a generar los certificados en el lado del servidor, para lo cual haremos uso de la siguiente sentencia.

```
[root@localhost strongswan]# strongswan pki --gen --type rsa --size 4096 --outfo
rm der > ipsec.d/private/strongswankey.der
```

Figura 218:Correr el strongwan.

Paso 3: A continuación, se cambiarán los permisos del archivo que generamos en el paso anterior con el siguiente comando.

```
[root@localhost strongswan]# chmod 600 ipsec.d/private/strongswankey.der
[root@localhost strongswan]#
```

Figura 219: Cambio de permisos.

Paso 4: Después procederemos a crear el archivo ca autoafirmado con el siguiente comando.

```
[root@localhost strongswan]# strongswan pki --self --ca --lifetime 3650 --in ips
ec.d/private/strongswankey.der --type rsa --dn "C=EC, ST=MA, L=Portoviejo, O=SOL
INF, OU=TI, CN=localhost/name=localhost/emailAddress=gabriel@localhost" --outfor
m der > ipsec.d/cacerts/strongswancert.der
```

Figura 220:Crear el archivo ca.

Paso 5: Luego se verá el contenido del archivo que generamos con el siguiente comando.

```
[root@localhost strongswan]# strongswan pki --print --in ipsec.d/cacerts/strongs
wancert.der
  subject:  "C=EC, ST=MA, L=Portoviejo, O=SOLINF, OU=TI, CN=localhost/name=local
host/emailAddress=gabriel@localhost"
  issuer:   "C=EC, ST=MA, L=Portoviejo, O=SOLINF, OU=TI, CN=localhost/name=local
host/emailAddress=gabriel@localhost"
  validity:  not before Sep 07 00:24:28 2016, ok
             not after  Sep 05 00:24:28 2026, ok (expires in 3649 days)
  serial:    13:c9:d7:27:17:a9:4c:ef
  flags:     CA CRLSign self-signed
  subjkeyId: 9e:33:7d:b2:5a:d1:d9:4b:bf:b1:00:72:08:a1:ed:13:ae:b3:45:ca
  pubkey:    RSA 4096 bits
  keyid:     ab:08:96:a2:b2:02:2a:b5:ea:7f:ad:4a:68:e5:2c:6e:de:ee:01:03
  subjkey:   9e:33:7d:b2:5a:d1:d9:4b:bf:b1:00:72:08:a1:ed:13:ae:b3:45:ca
[root@localhost strongswan]#
```

Figura 221:Contenido de archivos.

Paso 6: Se procederá a generar el archivo. DER de la VPN o también llamada clave con el siguiente comando.

```
[root@localhost strongswan]# strongswan pki --gen --type rsa --size 2048 --outfo
rm der > ipsec.d/private/vpnhostkey.der
```

Figura 222:Archivo DER.

Procedemos a cambiar los permisos del archivo generado.

```
[root@localhost strongswan]# chmod 600 ipsec.d/private/vpnhostke
```

Figura 223:Cambio de permisos.

Paso 7: Luego se generará el archivo de la clave pública el cual va a ser el que se entregará al usuario.

```
ot@localhost strongswan]# strongswan pki --pub --in ipsec.d/private/vpnhos
er --type rsa | strongswan pki --issue --lifetime 730 --cacert ipsec.d/cac
trongswancert.der --cakey ipsec.d/private/strongswankey.der --dn "C=EC, ST
=Portoviejo, O=SOLINF, OU=TI, CN=localhost/name=localhost/emailAddress=gab
ocalhost" --san localhost --san localhost --san 192.168.1.15 --san 127.0.0
an @192.168.1.15 --san @127.0.0.1 --flag serverAuth --flag ikeIntermediate
form der > ipsec.d/certs/vpnhostcert.der
```

Figura 224:Clave del usuario.

Paso 8: Mostramos el contenido de nuestra clave y nos quedará algo como esto:

```
[root@localhost strongswan]# strongswan pki --print --in ipsec.d/certs/vpnhostce
rt.der
  subject:  "C=EC, ST=MA, L=Portoviejo, O=SOLINF, OU=TI, CN=localhost/name=local
host/emailAddress=gabriel@localhost"
  issuer:   "C=EC, ST=MA, L=Portoviejo, O=SOLINF, OU=TI, CN=localhost/name=local
host/emailAddress=gabriel@localhost"
  validity:  not before Sep 07 00:25:16 2016, ok
             not after  Sep 07 00:25:16 2018, ok (expires in 729 days)
  serial:    2f:64:fc:bf:ca:05:9b:bc
  altNames:  localhost, localhost, 192.168.1.15, 127.0.0.1, 192.168.1.15, 127.0.
0.1
  flags:     serverAuth ikeIntermediate
  authkeyId: 9e:33:7d:b2:5a:d1:d9:4b:bf:b1:00:72:08:a1:ed:13:ae:b3:45:ca
  subjkeyId: 51:83:9e:1a:df:55:53:86:cf:65:63:b2:69:8a:64:30:e7:ef:8a:3a
  pubkey:    RSA 2048 bits
  keyid:     ac:3d:88:c3:6b:fa:39:bc:96:eb:9b:cb:0f:fa:66:16:1d:6c:44:34
  subjkey:   51:83:9e:1a:df:55:53:86:cf:65:63:b2:69:8a:64:30:e7:ef:8a:3a
[root@localhost strongswan]#
```

Figura 225:Contenido de la clave.

Luego vamos a generar la clave privada, que será para el lado del cliente y cambiamos los permisos:

```
[root@localhost strongswan]# strongswan pki --gen --type rsa --size 2048 --outfo
rm der > ipsec.d/private/clientekey.der

[root@localhost strongswan]# chmod 600 ipsec.d/private/clientekey.der
```

Figura 226:Generar clave privada.

Paso 9: Después generamos el certificado de la clave pública.

```
[root@localhost strongswan]# strongswan pki --pub --in ipsec.d/private/clienteke
y.der --type rsa | strongswan pki --issue --lifetime 730 --cacert ipsec.d/cacert
s/strongswancert.der --cakey ipsec.d/private/strongswankey.der --dn "C=EC, ST=MA
, L=Portoviejo, O=SOLINF, OU=TI, CN=localhost/name=localhost/emailAddress=gabrie
l@localhost" --san "cliente@localhost" --san "cliente@192.168.1.15" --outform de
r > ipsec.d/certs/clientecert.der
[root@localhost strongswan]#
```

Figura 227:Certificados de la clave pública.

Luego escribimos el archivo pem de la clave pública con los siguientes comandos.

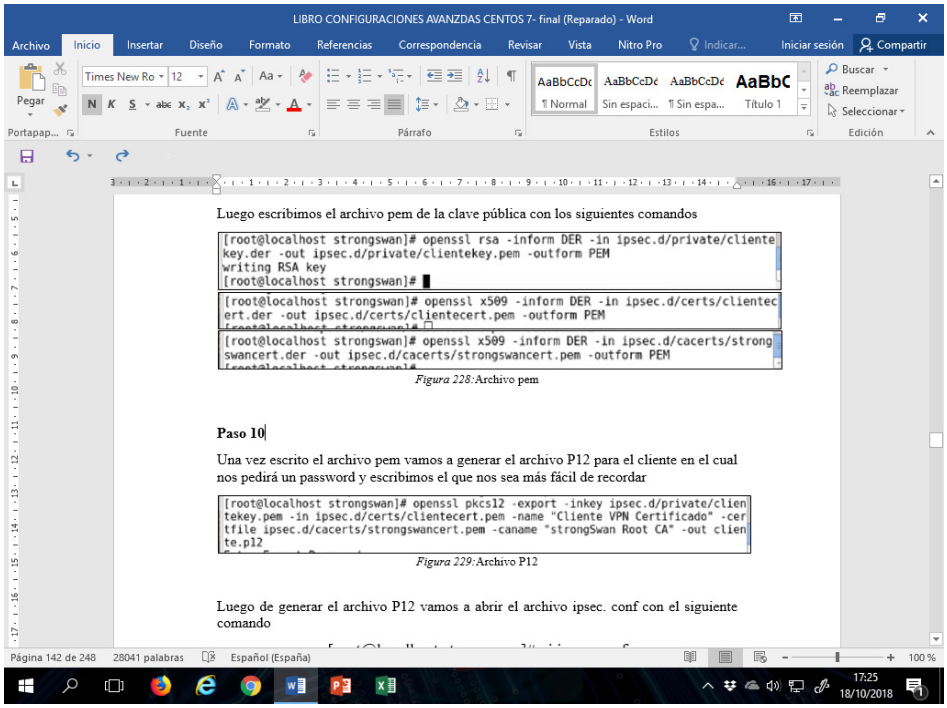


Figura 228:Archivo pem.

Paso 10: Una vez escrito el archivo pem vamos a generar el archivo P12 para el cliente, ahí pedirá un password y escribimos el que nos sea más fácil de recordar.

```
[root@localhost strongswan]# openssl pkcs12 -export -inkey ipsec.d/private/clien
tekey.pem -in ipsec.d/certs/clientecert.pem -name "Cliente VPN Certificado" -cer
tfile ipsec.d/cacerts/strongswancert.pem -caname "strongSwan Root CA" -out clien
te.p12
```

Figura 229:Archivo P12.

Luego de generar el archivo P12 vamos a abrir el archivo ipsec. conf con el siguiente comando.

[root@localhost strongswan]# vi ipsec.conf

Paso 11: Una vez dentro del archivo ipsec. conf vamos a copiar lo siguiente donde ike serán nuestros protocolos de inscripción, ponemos nuestro certificado, que en este caso es vpnhostcert.der, también especificaremos los dns que usaremos para nuestra vpn y el rango de las direcciones ip.

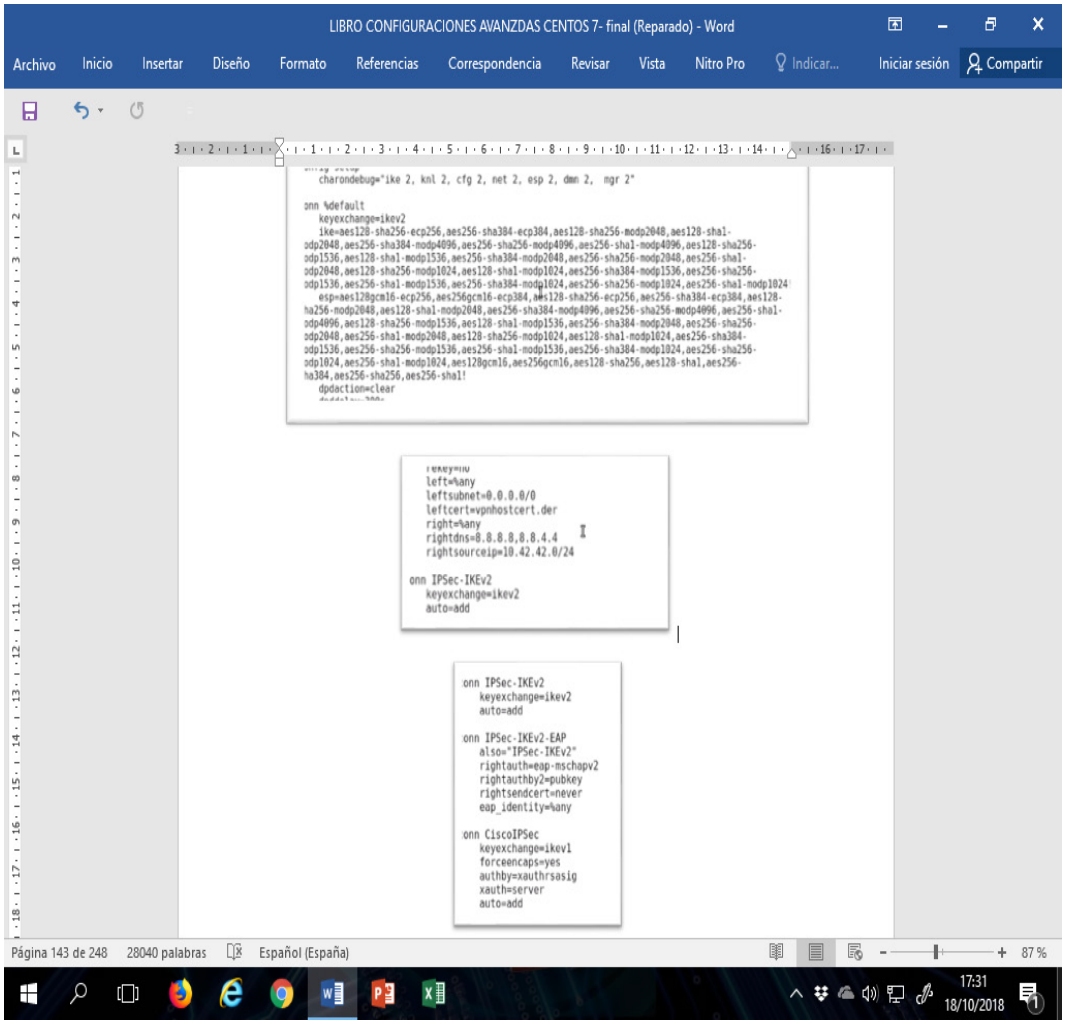


Figura 230: Protocolos de inscripción.

Paso 12: Una vez editado el archivo, lo guardaremos y pasamos al siguiente paso, que es añadir los usuarios con sus respectivas claves y reiniciamos el servicio del strongswan, ya con esto tendremos configurado nuestro servidor

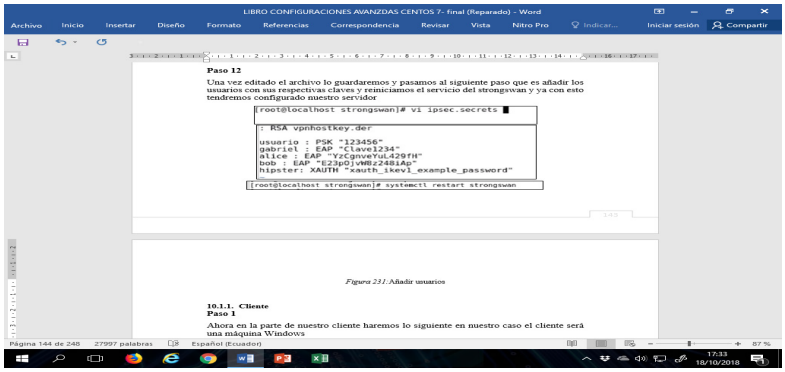


Figura 231:Añadir usuarios.

Cliente

Paso 1: Ahora en la parte de nuestro cliente haremos lo siguiente: (en nuestro caso el cliente será una máquina Windows)

Ir al centro de redes y recursos compartidos.

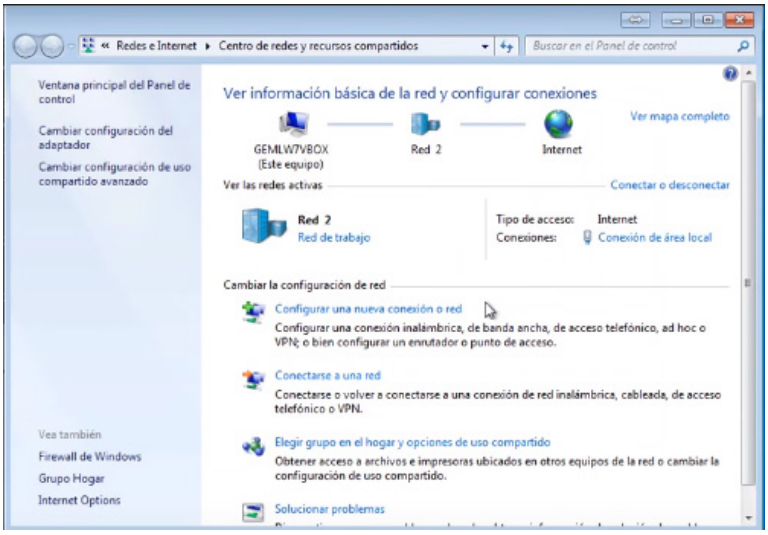


Figura 232: Centro de redes y recursos compartidos.

Paso 2: Y luego configurar nueva conexión de red

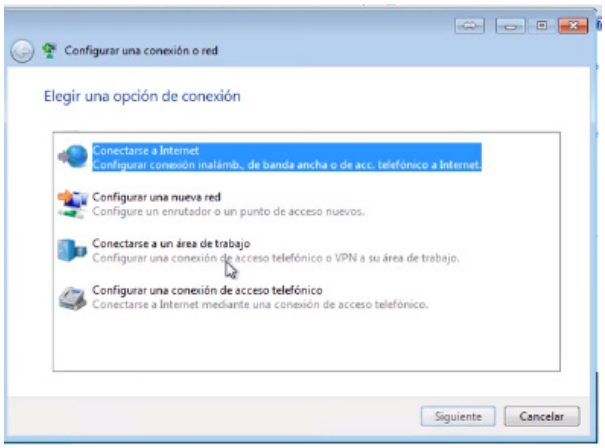


Figura 233:Conexión de red.

Y seleccionamos conectarse a un área de trabajo.

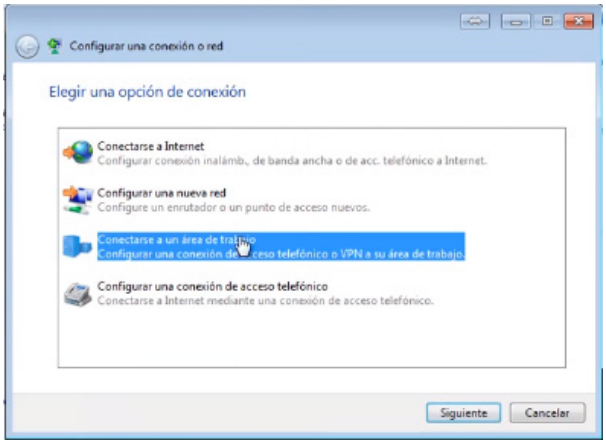


Figura 234: Selección de área de trabajo.

Paso 3: Y vamos a crear una conexión nueva.

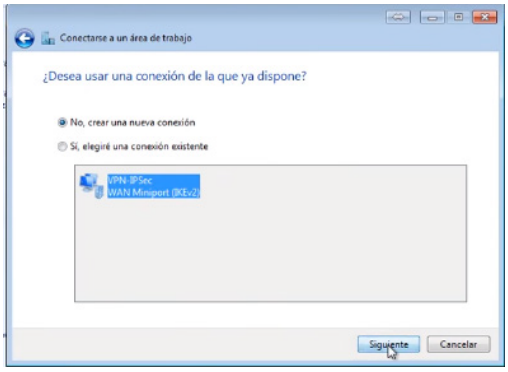


Figura 235: Nueva conexión.

Seleccionamos usar mi conexión a internet.



Figura 236: Selección de conexión a internet.

Paso 4: Colocamos la ip y el nombre, y comprobamos que no se conecte todavía y hacemos click en siguiente.

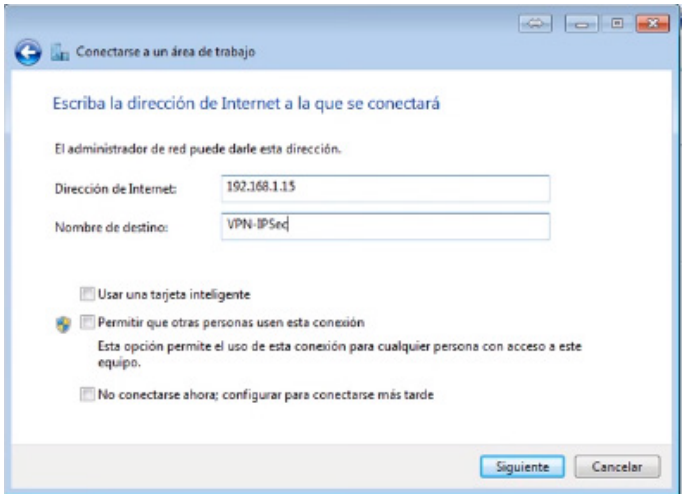


Figura 237:Ip y nombre

Luego ingresaremos el usuario y la contraseña.

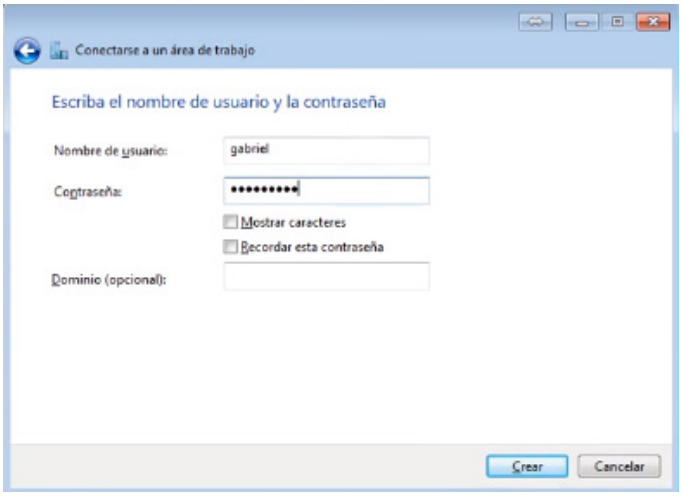


Figura 238: Login.

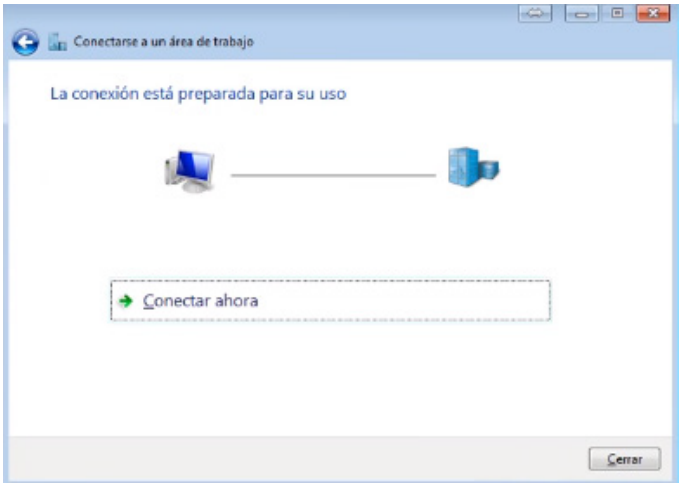


Figura 239: Conexión a una área de trabajo.

Paso 5: Y listo, pero aún no seleccionamos conectar, ya que nos hace falta añadir el certificado que generamos anteriormente, para lo cual vamos a la máquina CentOS y haremos lo siguiente:

```
[root@localhost strongswan]# cp cliente.p12 /home/gabriel/
cp: ¿sobreescribir «/home/gabriel/cliente.p12»? (s/n) s
[root@localhost strongswan]#
```

Y copiaremos el archivo a nuestra máquina.

```
[gabriel@galeon Escritorio]$ scp gabriel@192.168.1.15:/home/gabriel/cliente.p12
.
gabriel@192.168.1.15's password:
cliente.p12                                   100% 4620     4.5KB/s   00:00
[gabriel@galeon Escritorio]$
```

Paso 6: Luego en el cmd de Windows digitaremos y nos abrirá la siguiente ruta:

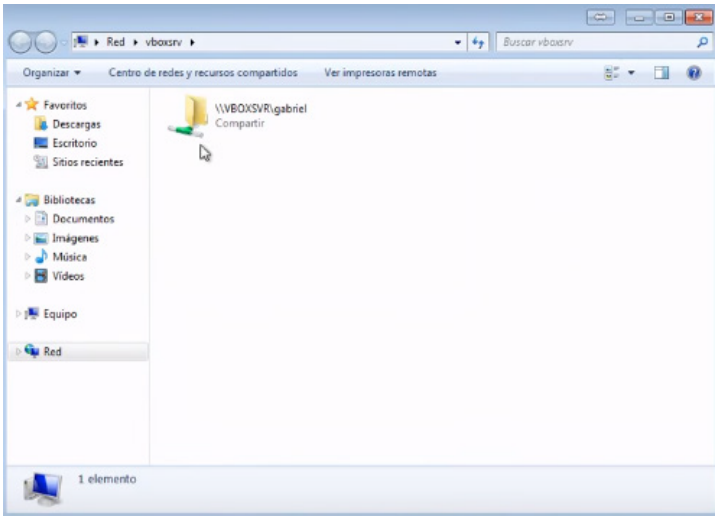
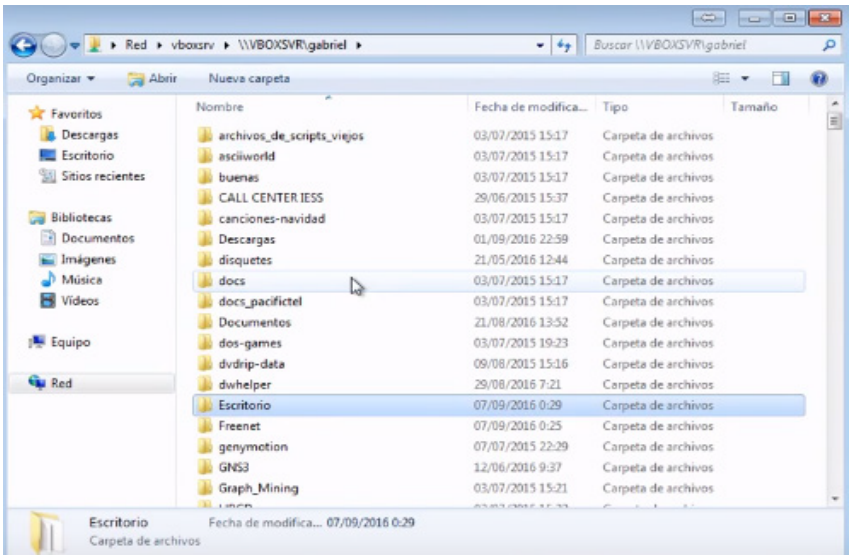


Figura 240: C:\Users\Administrador>start \\vboxsrv

Abrimos la carpeta y nos dirigimos al escritorio y copiamos el archivo a la carpeta de openvpn.



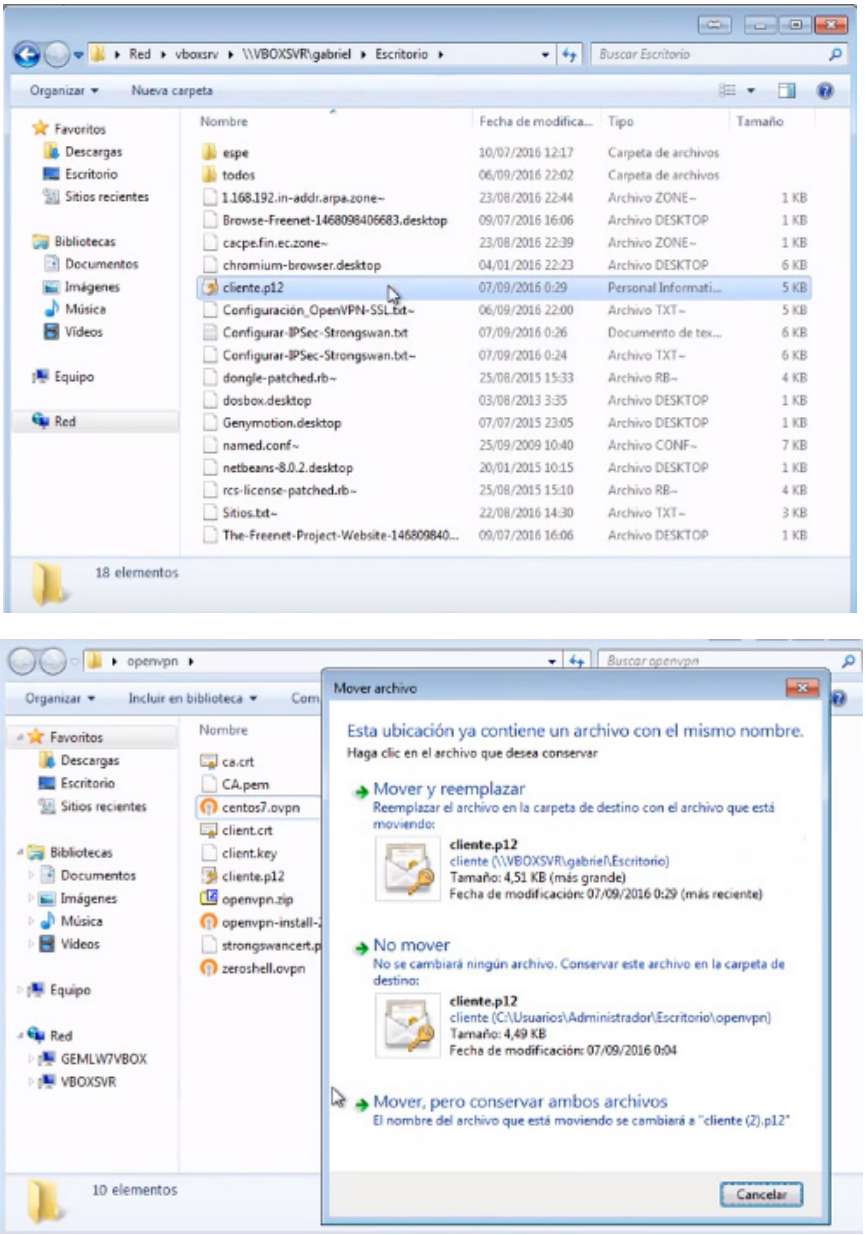
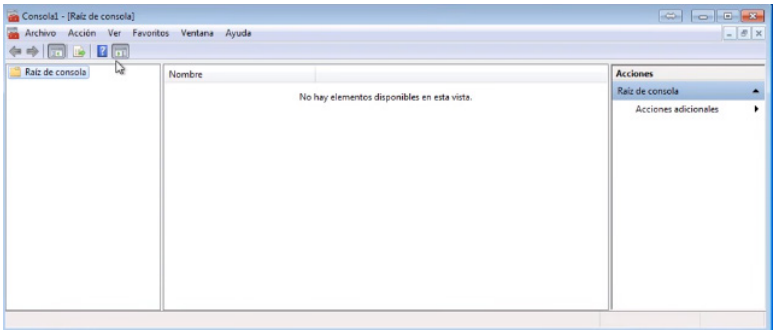
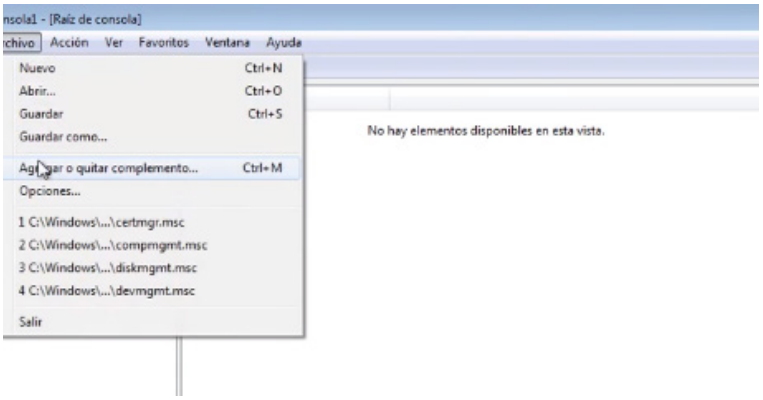
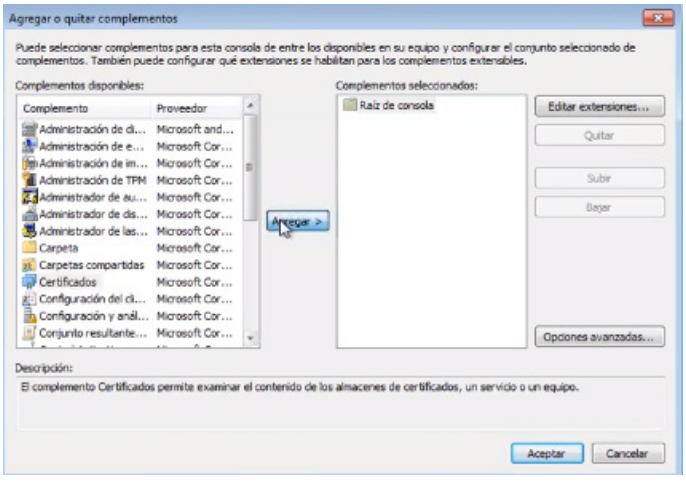


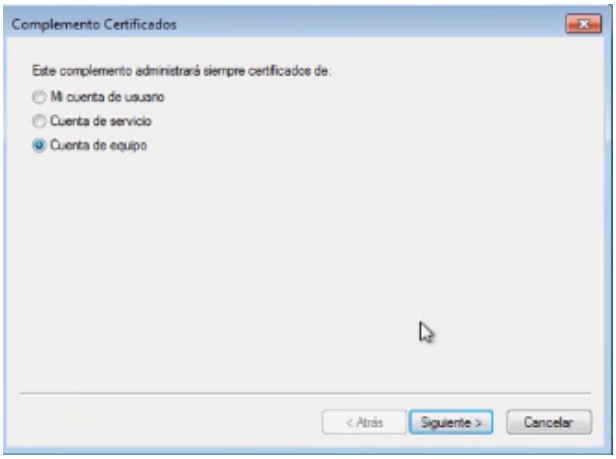
Figura 241: Copia del archivo.

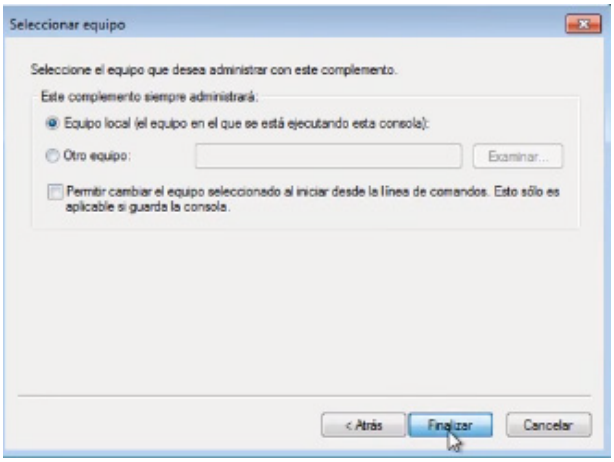
Paso 7: Luego en el cmd de Windows tecleamos mmc para abrir la consola de administración de Windows y añadiremos el siguiente complemento.

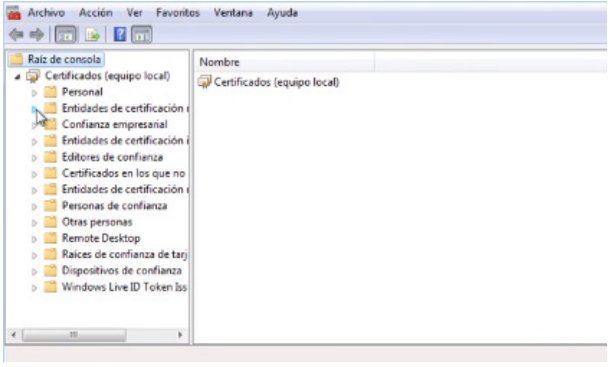


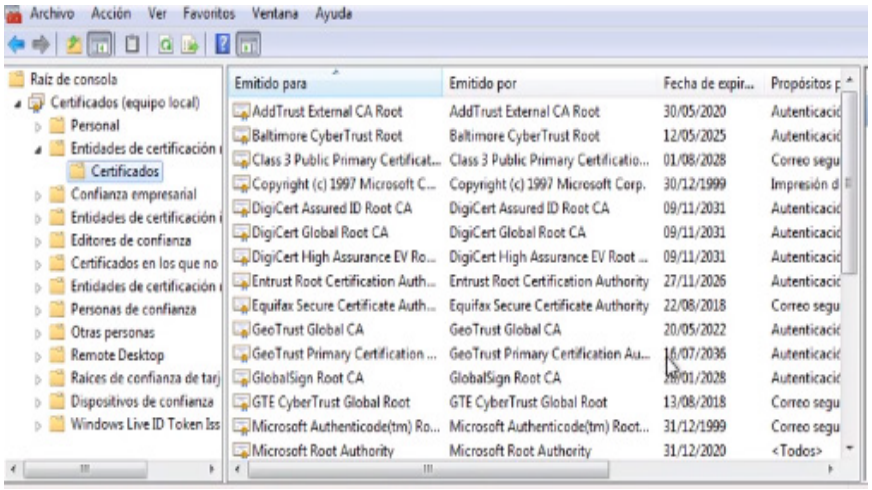


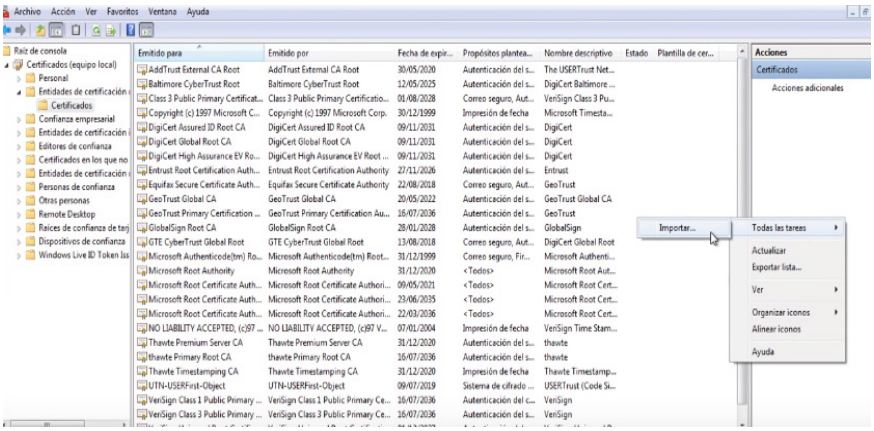


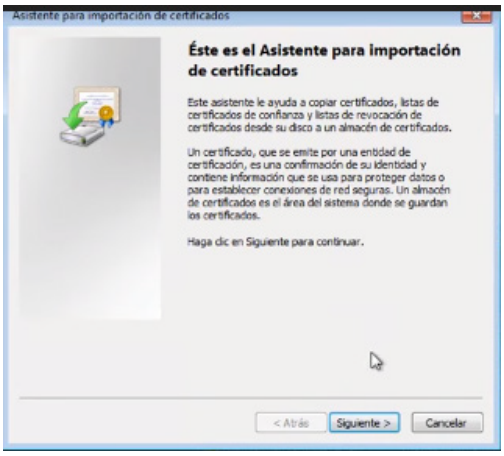

Complemento Certificados
Este complemento administrará siempre certificados de:
Mi cuenta de usuario
Cuenta de servicio
Cuenta de equipo
< Atrás
Siguiente >
Cancelar


Seleccionar equipo
Seleccione el equipo que desea administrar con este complemento.
Este complemento siempre administrará:
Equipo local (el equipo en el que se está ejecutando esta consola):
Otro equipo:
Examinar...
Permitir cambiar el equipo seleccionado al iniciar desde la línea de comandos. Esto sólo es aplicable si guarda la consola.
< Atrás
Finalizar
Cancelar


Archivo Acción Ver Favoritos Ventana Ayuda
Raíz de consola
Certificados (equipo local)
Personal
Entidades de certificación
Confianza empresarial
Editores de confianza
Certificados en los que no
Personas de confianza
Otras personas
Remote Desktop
Dispositivos de confianza
Nombre
Certificados (equipo local)


Archivo Acción Ver Favoritos Ventana Ayuda
Raíz de consola
Certificados (equipo local)
Personal
Entidades de certificación
Certificados
Confianza empresarial
Editores de confianza
Certificados en los que no
Personas de confianza
Otras personas
Remote Desktop
Dispositivos de confianza
Windows Live ID Token Iss
Emitido para
Emitido por
Fecha de expir...
Propósitos p
AddTrust External CA Root
Baltimore CyberTrust Root
Class 3 Public Primary Certificat...
Copyright (c) 1997 Microsoft C...
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert High Assurance EV Ro...
Entrust Root Certification Auth...
Equifax Secure Certificate Auth...
GeoTrust Global CA
GeoTrust Primary Certification ...
GlobalSign Root CA
GTE CyberTrust Global Root
Microsoft Authenticode(tm) Ro...
Microsoft Root Authority
Microsoft Root Authority
31/12/2020
<Todos>


Importar...
Todas las tareas
Actualizar
Exportar lista...
Ver
Organizar iconos
Alinear iconos
Ayuda
Acciones
Certificados
Acciones adicionales


Asistente para importación de certificados
Éste es el Asistente para importación de certificados
Este asistente le ayuda a copiar certificados, listas de certificados de confianza y listas de revocación de certificados desde su disco a un almacén de certificados.
Un certificado, que se emite por una entidad de certificación, es una confirmación de su identidad y contiene información que se usa para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados es el área del sistema donde se guardan los certificados.
Haga clic en Siguiente para continuar.
< Atrás
Siguiente >
Cancelar

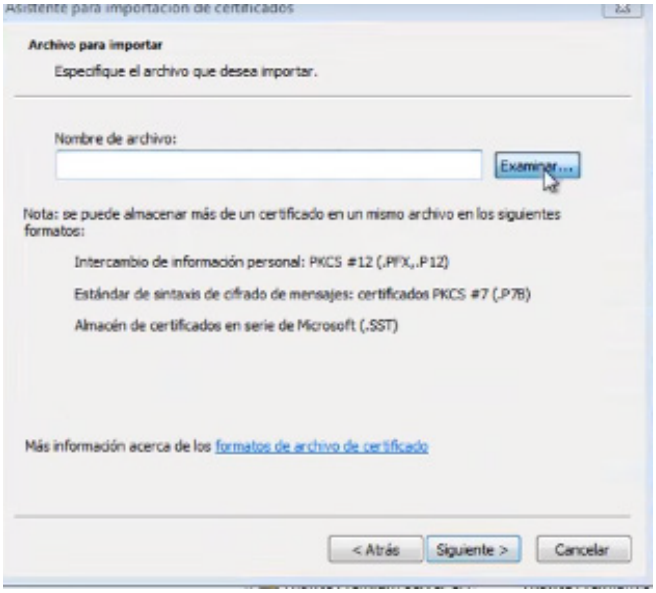
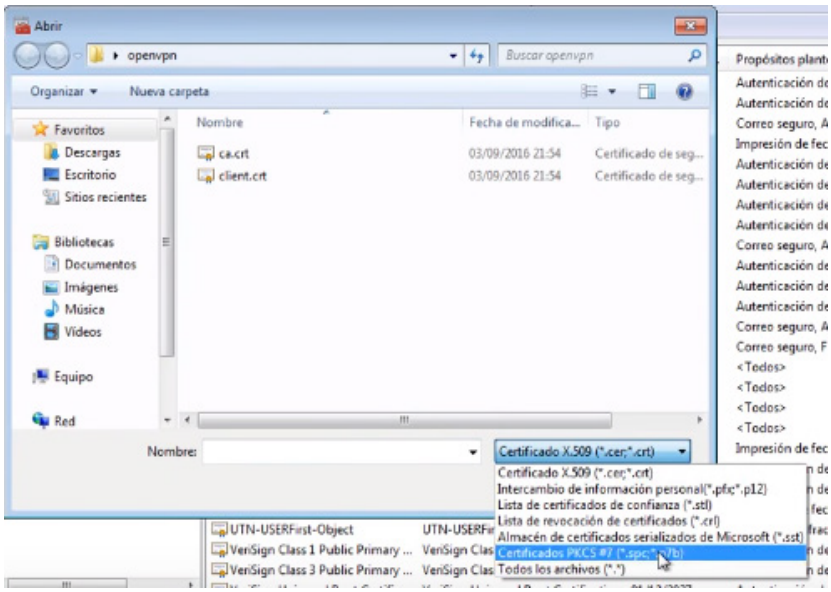
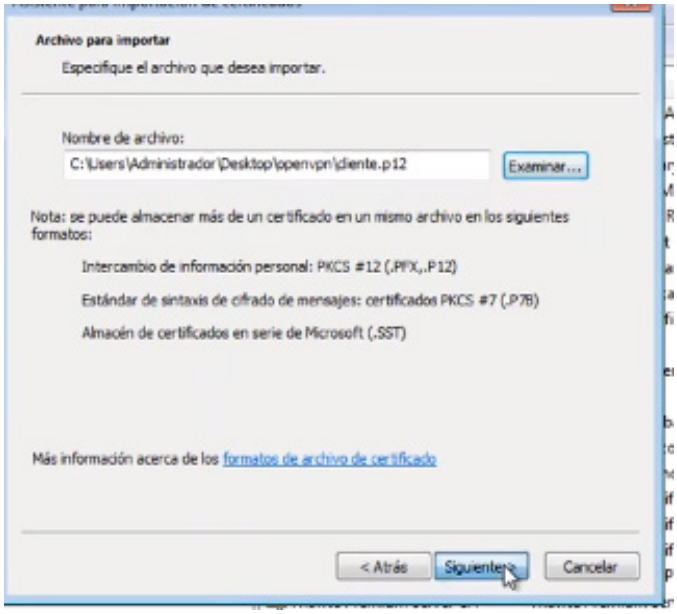


Figura 242: Secuencia de ventanas para inserción de archivo p12.

Buscamos nuestro archivo p12.



Lo seleccionamos y le hacemos a siguiente:



Paso 8: Colocamos la contraseña que creamos al momento de crearlo.

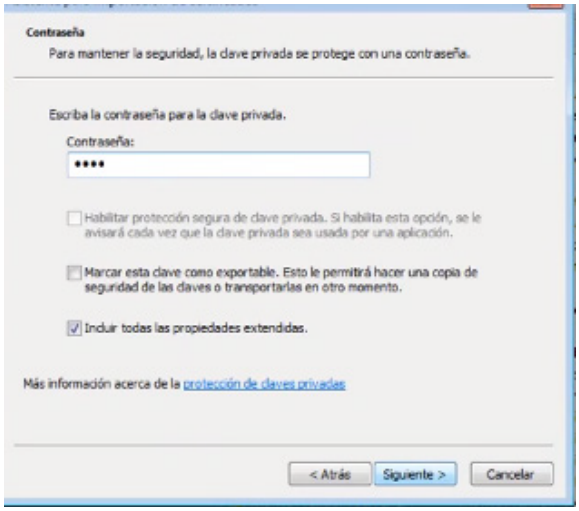


Figura 243: Ingreso de contraseña.

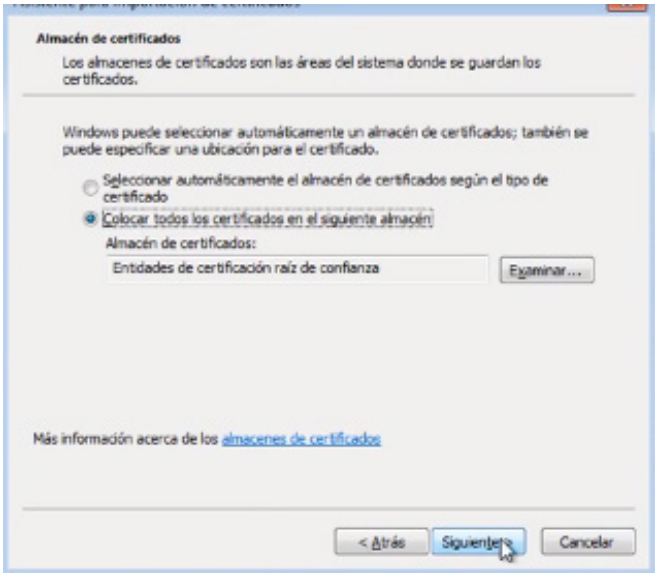


Figura 244: Almacén de certificados.

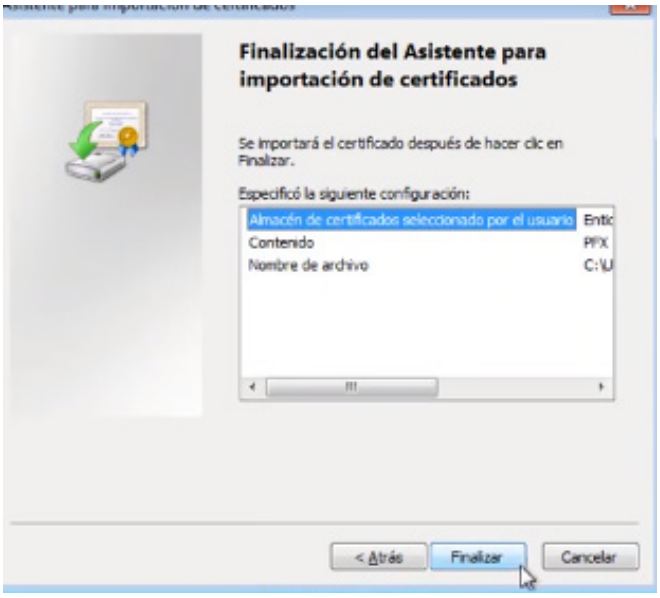


Figura 245: Finalización de importación de certificados.

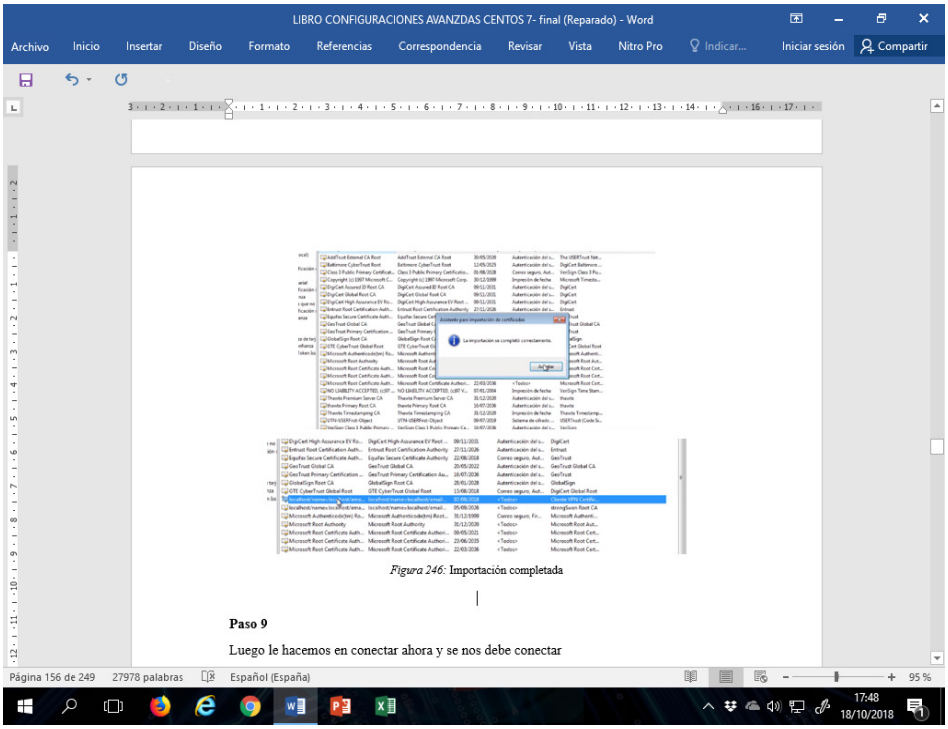
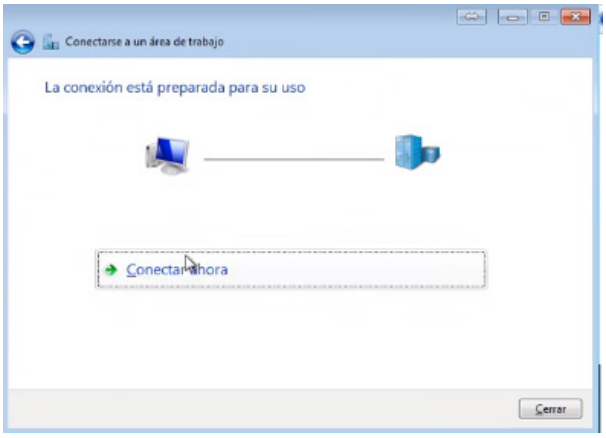


Figura 246: Importación completada.

Paso 9: Procedemos a conectar.



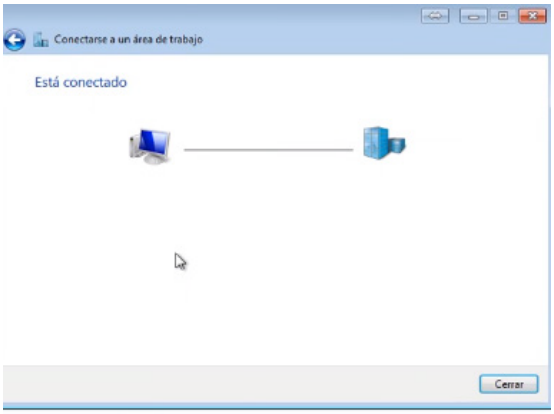


Figura 247: Conexión a red de trabajo.

Y lo podemos observar en cmd de Windows con el comando ip config que se nos agregó correctamente:

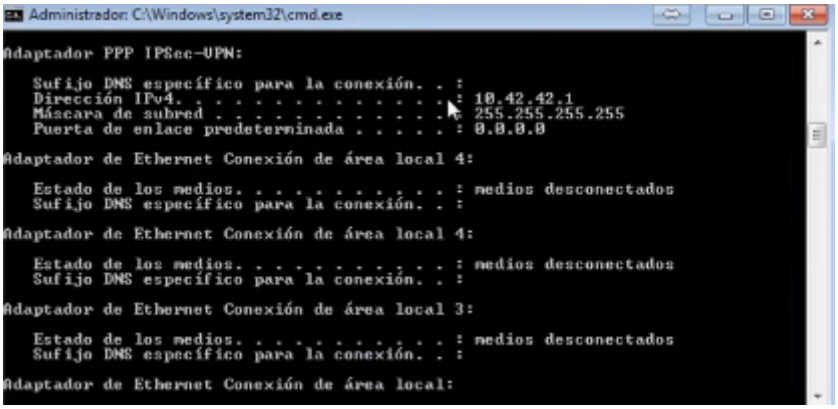


Figura 248: Ejecución comando cmd.

CAPÍTULO 12:
INTRODUCCIÓN DE NFS



En este capítulo usted encontrará:

- *Instalación Y Configuración de NFS.*
- *NFSv2.*
- *NFSv3.*
- *Servidor NFS.*

Introducción

NFS (**N**etwork **F**ile **S**ystem) es un popular protocolo utilizado para compartir sistemas de archivos de manera transparente entre anfitriones dentro de una red de área local. Es utilizado para sistemas de archivos distribuido.

Fue desarrollado en 1984 por Sun Microsystems, teniendo en mente la independencia del anfitrión, sistema operativo, protocolo de transporte. Funciona a través de los protocolos **XDR** (nivel de presentación del modelo OSI de TCP/IP) y **ONC RPC** (nivel de sesión del modelo OSI de TCP/IP).

Existen tres versiones de NFS que se utilizan hoy en día:

- **NFSv2**: Es la versión más antigua y mejor soportada.
- **NFSv3**: Tiene más características que NFSv2, como el manejo de archivos de tamaño variable y mejores informes de errores. Sólo es parcialmente compatible con los clientes para NFSv2.
- **NFSv4**: Es la versión más moderna, y, entre otras cosas, incluye soporte para seguridad a través de Kerberos, soporte para ACL y utiliza operaciones con descripción del estado.

Salvo que se trate de directorios de acceso público, se recomienda utilizar **NFS** sólo dentro de una red de área local detrás de un muro contrafuegos y que sólo se permita el acceso a los anfitriones que integren la red de área local y evitar compartir sistemas de archivos con información sensible a través de Internet.

Las versiones antiguas del protocolo requerían otros servicios RPC que utilizaban puertos asignados dinámicamente. Afortunadamente, con la versión 4 de NFS solo son necesarios los puertos 2049 (para el NFS propiamente) y el 111 (para el *portmapper*), por lo que son fáciles de filtrar mediante cortafuegos.

Servidor NFS: Es parte del núcleo Linux; en los núcleos que Debian provee está compilado como un módulo de núcleo. Si necesita ejecutar el servidor NFS automáticamente al iniciar, debe instalar el paquete nfs-kernel-server; contiene los scripts de inicio relevantes.

Instalación y configuración de NFS

Paso 1: Lo primero que vamos a necesitar es instalar los paquetes de NFS, para lo cual utilizaremos el comando "yum –y install nfs-utils" y esperaremos que se descarguen para posteriormente utilizarlos.

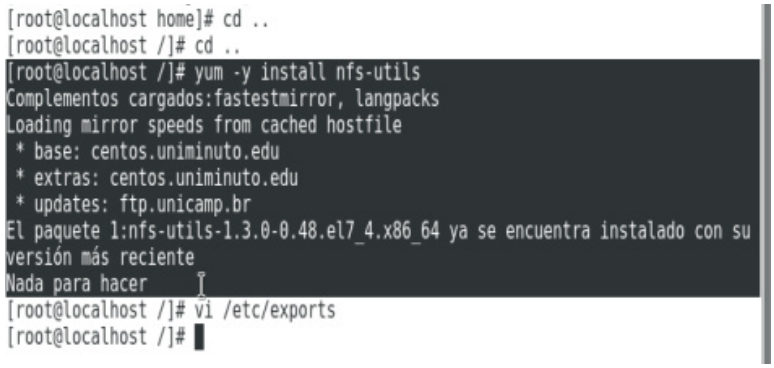


Figura 249: comando "yum –y install nfs-utils"

Paso 2: Luego de haber instalado los paquetes de NFS ingresaremos el comando "vi /etc/exports" y haremos lo siguiente:



Figura 250: comando "vi /etc/exports".

Paso 3: Una vez digitado el comando anterior se abrirá un archivo para modificar, presionando "i", una vez procedemos a editarlo ingresaremos la dirección de la carpeta que vamos a compartir con el cliente, luego la ip del cliente y le asignamos los permisos respectivos.

/home/final 192.168.0.102(rw,no root_squash,async)

Paso 4: Una vez editado el archivo presionamos "esc", luego "shif+:" y "wq", posteriormente, tenemos que exportar el archivo que editamos con el comando "exportfs -ra".

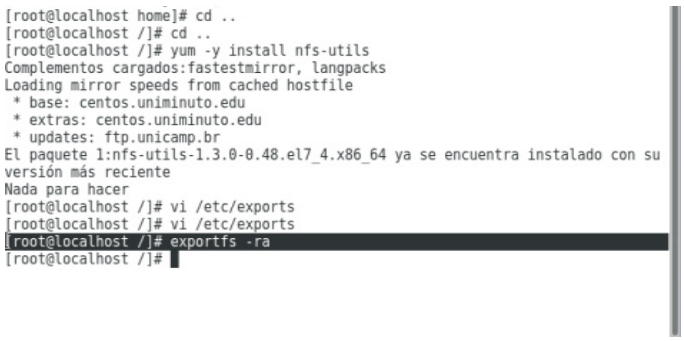


Figura 251: comando "exportfs -ra".

Paso 5: Una vez exportado el archivo, a continuación correremos los servicios de rpcbind y nfs, para lo cual utilizaremos el siguiente comando "systemctl start rpcbind nfs-server".



Figura 252: comando "systemctl start rpcbind nfs-server".

Paso 6: Una vez que los servicios están corriendo, los vamos a habilitar con el comando "systemctl enable rpcbind nfs-server".



Figura 253:comando "systemctl enable rpcbind nfs-server".

Paso 7: Una vez hecho esto, tenemos casi listo nuestro servidor, lo único que faltaría por hacer es activar el firewall para los servicios de nfs, esto lo vamos a hacer con el comando "firewall-cmd –add-service=nfs --permanent".

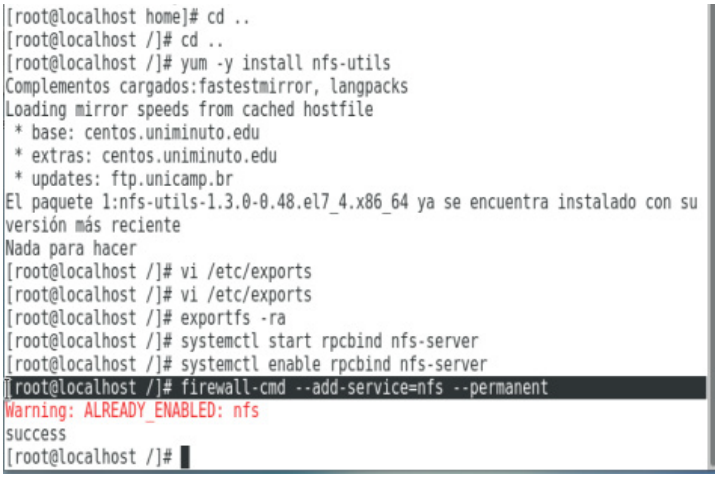


Figura 254:comando "firewall-cmd –add-service=nfs --permanent"

Paso 8: Finalmente, volveremos a recargar el firewall con el comando "firewall-cmd --reload" y listo, el servidor estará configurado.



Figura 255: comando "firewall-cmd --reload".

Paso 9: Una vez configurado el servidor, pasaremos al lado del servidor e instalaremos el paquete de nfs con el comando "yum –y install nfs-utils".

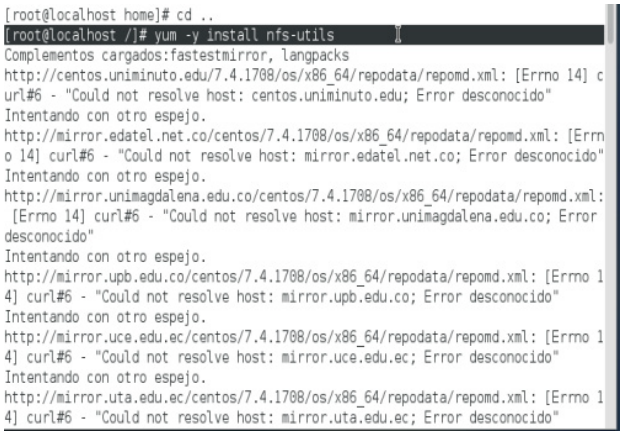


Figura 256: comando "yum –y install nfs-utils".

Paso 10: Después de haber instalado el paquete de nfs en el lado del servidor, vamos a correr los servicios de rpcbind con el comando "systemctl start rpcbind".

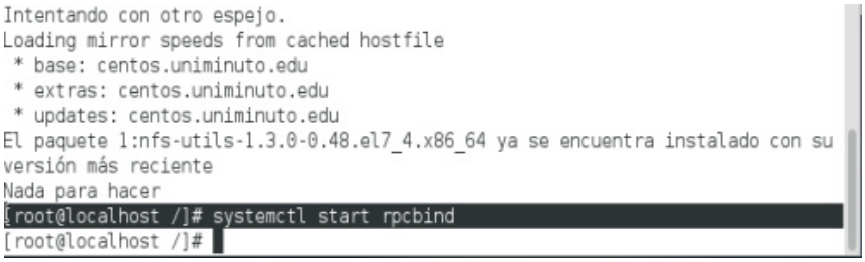


Figura 257: comando "systemctl start rpcbind".

Y luego lo habilitaremos con el comando "systemctl enable rpcbind".

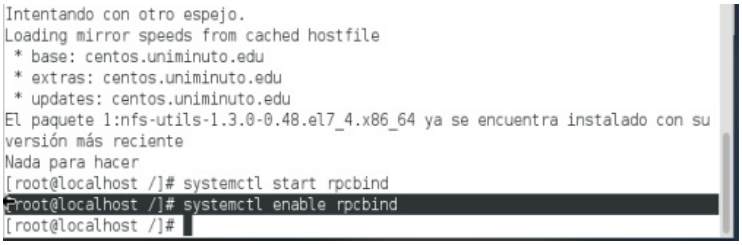


Figura 258: comando "systemctl enable rpcbind".

Paso 11: Una vez realizado esto, vamos a montar nuestro cliente con nuestro servidor con el comando "mount –t nfs <ip-servidor>: carpetadelservidor carpetadelcliente". Una vez hecho este paso, habremos finalizado con la configuración de nuestro cliente y nuestro servidor.

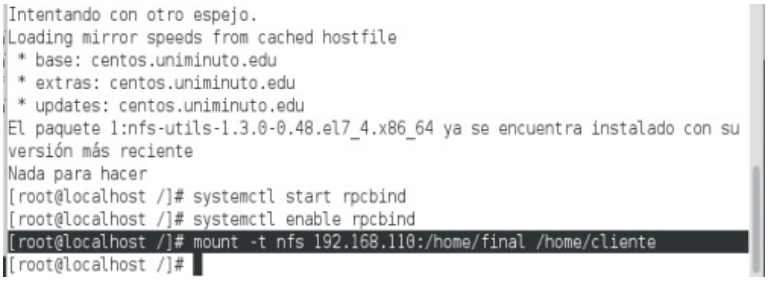


Figura 259: comando "mount –t nfs <ip-servidor>:carpetadelservidor

Paso 12: Como paso final veremos si se montó nuestro cliente con nuestro servidor. Para esto, haremos uso del comando "df hT" y, como podemos ver en la siguiente imagen, sí se montó el cliente con el servidor:

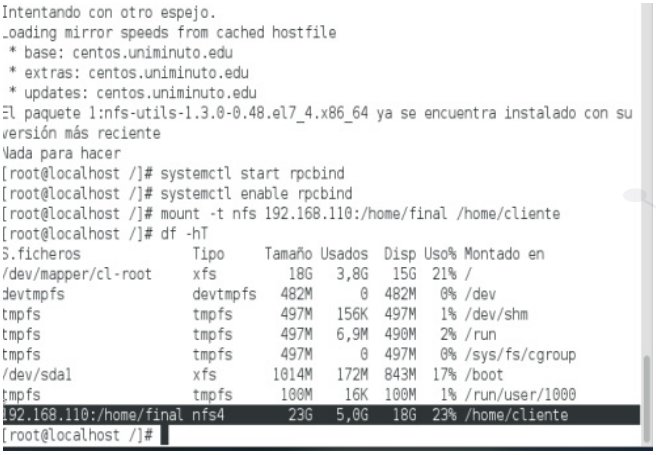


Figura 260: comando "df hT".

CAPÍTULO 13:
INTRODUCCIÓN DE OpenVPN



En este capítulo usted encontrará:

- *Instalación de OpenVPN.*
- *Configuración de OpenVPN*
- *Host*

Introducción

¿Qué es vpn? Las redes privadas virtuales (VPN) permiten utilizar los medios de comunicación públicos como internet para establecer comunicaciones entre redes locales ubicadas en lugares distintos, haciendo que se comporten como si fuera la misma red local. Para ello se precisan técnicas de cifrado de la información y establecimiento de túneles sobre las redes públicas, con objeto de mantener la seguridad de las comunicaciones.

¿Qué es host? Es un ordenador que funciona como el punto de inicio y final de las transferencias de datos, comúnmente descrito como el lugar donde reside un sitio web. Un anfitrión de internet tiene una dirección de internet única (dirección ip) y un nombre de dominio único o nombre de anfitrión (host name).

Instalación y configuración de host a host

Paso 1: Instalar el paquete epel-release

Yum install epel-release

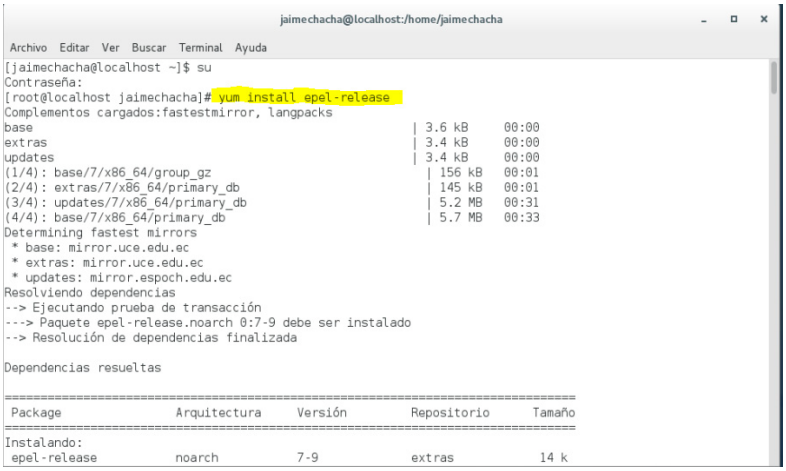


Figura 261: Instalación epel-release.

Paso 2: Instalar OpenVPN. Tenemos que instalar OpenVPN. También instalaremos Easy RSA (Paquete de creación de certificados), para generar nuestros pares de claves SSL (Protocolo de transmisión de información de ida, de manera segura), que protegerán nuestras conexiones VPN.

Yum install openvpn easy-rsa

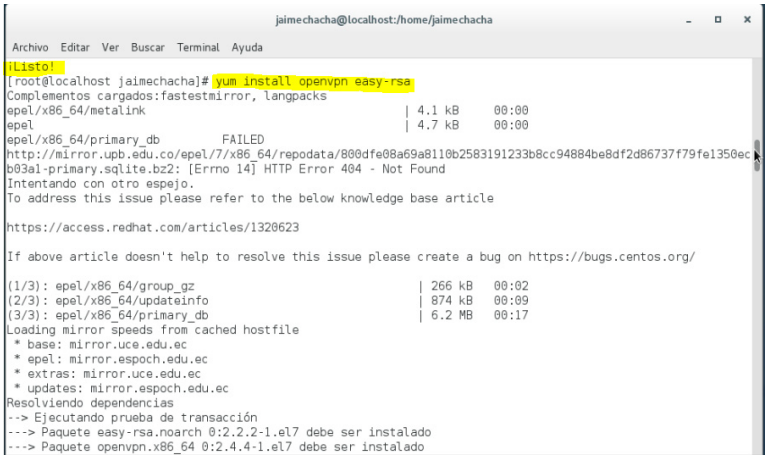


Figura 262: Instalación easy-rease.

Paso 3: Configurando OpenVPN. OpenVPN tiene archivos de configuración de ejemplo en su directorio de documentación. Vamos a copiar el server. Con archivo de muestra como punto de partida para nuestro propio archivo de configuración.

Cp -r /usr/share/easy-rsa /etc/openvpn

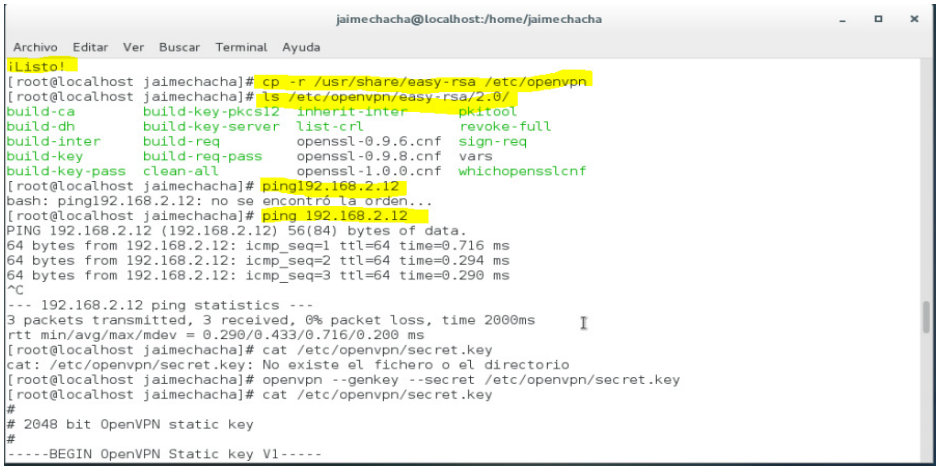


Figura 263:Archivos de configuración.

Paso 4: Generando llaves y certificados. Ahora que el servidor está configurado, tendremos que generar nuestras claves y certificados. Easy RSA instala algunos scripts para generarlas.

Vamos a crear un directorio para las teclas para entrar.

Cat /etc/openvpn/secret.key

También debemos copiar los scripts de generación de claves y certificados en el directorio.

Openvpn --genkey – secret /etc/openvpn/secret.key

Para hacernos la vida más fácil, vamos a editar los valores predeterminados que usa el script (Instrucciones), para no tener que escribir nuestra información en cada momento. Esta información se almacena en el varsarchivo, así que vamos a abrir esto para su edición.

Cat /etc/opnvpn/secret.key

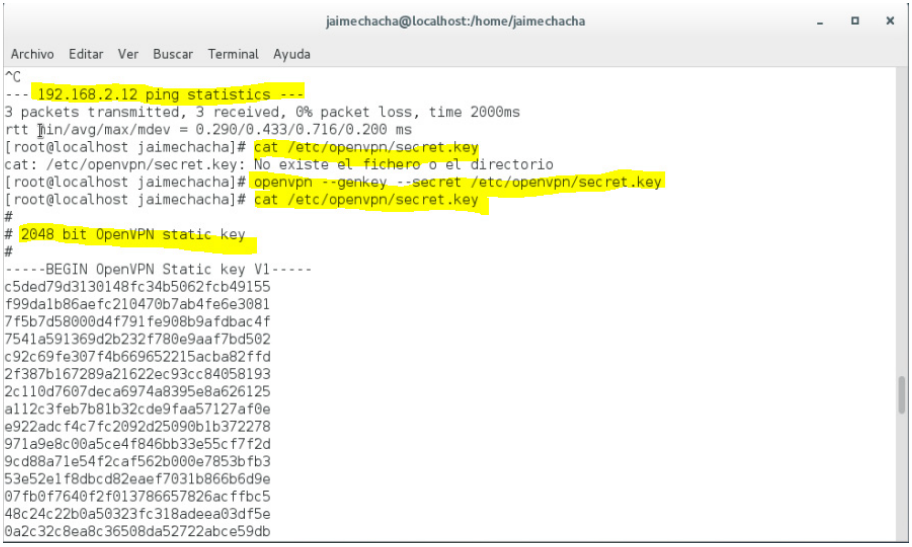


Figura 264: Clave servidor.

Paso 5: Enrutamiento. El enrutamiento es el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta (la más corta).

Scp/etc/openvpn/secret.key root@192.168.2.12:/etc/openvpn/

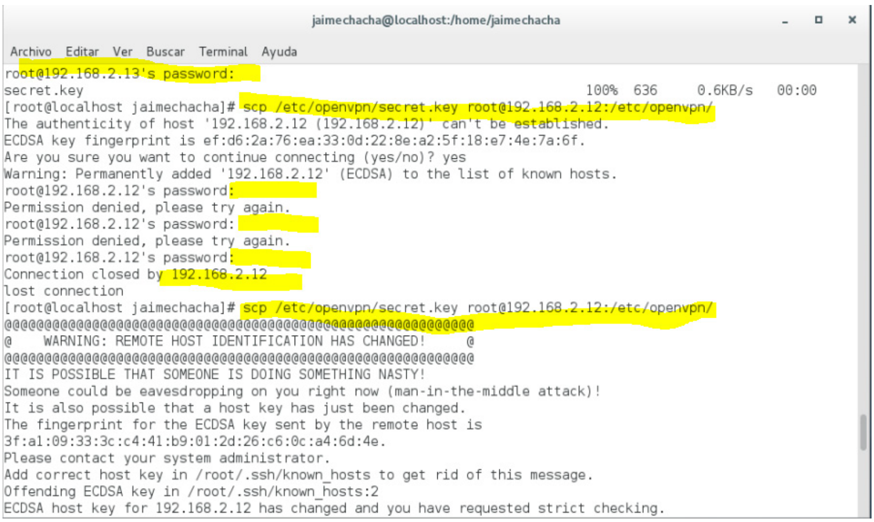


Figura 265: Enrutamiento.

Paso 6: Archivo de configuracion en el cliente. En esta parte modificamos la dirección ip, primero la del cliente, luego la del servidor.



Figura 266: Archivos de configuración cliente.

Paso 7: Archivo de modificacion de cliente. En este archivo lo que cambiamos es el orden en que van las direciones ip del cliente y servidor.



Figura 267: Archivos de configuración cliente.

Paso 8: Copiamos la clave del servidor en el cliente. Ejecutamos de nuevo la combinación de código y mostrará la conectividad que debe ser igual al que nos aparece en la máquina cliente.

Cat /etc/openvpn/secret.key

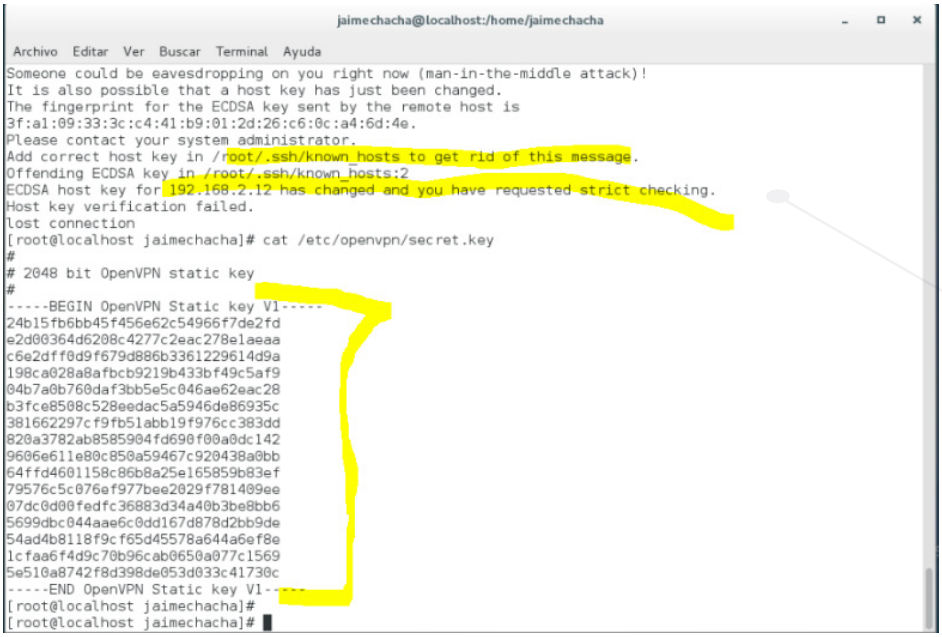


Figura 268: Copia de clave en el cliente.

CAPÍTULO 14:
INTRODUCCIÓN A CONFIGURACION DE SERVIDORES



En este capítulo usted encontrará:

- *Servidor en Linux Ubuntu server 8.04.*
- *Servidor FTP.*
- *Configuración Linux Ubuntu.*

Introducción a servidores

Servidor en Linux Ubuntu server 8.04

Paso 1: Con el archivo de imagen ISO (International Standarization Organization) grabado, lo insertamos en la unidad lectora y arrancamos el ordenador. La primera pantalla que aparece nada más arrancar nos pregunta el lenguaje que queremos para la instalación y seleccionaremos el idioma.

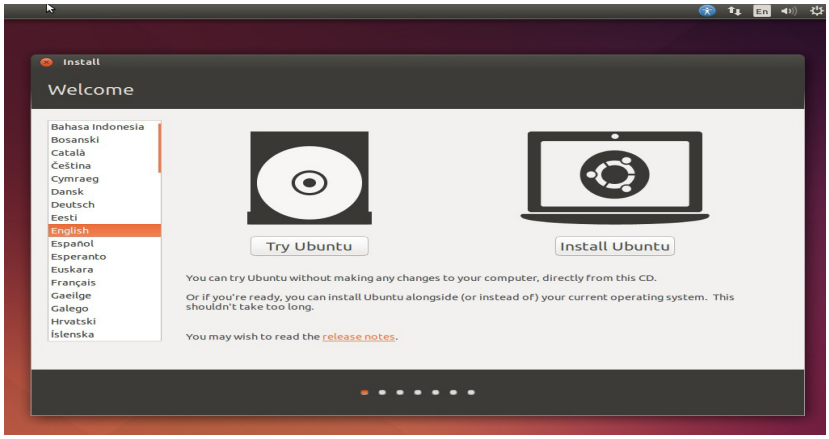


Figura 269: Arranuqe del ordenador con imagen ISO.

Paso 2: Luego de la instalación, si desea presione f4 para una instalación más alternativa para su desarrollo inicial.



Figura 270: f4 para una instalación más alternativa.

Paso 3: A continuación necesitamos indicarle cual será el nombre que le vamos a dar a la máquina (*En mi caso* **hsnet**).

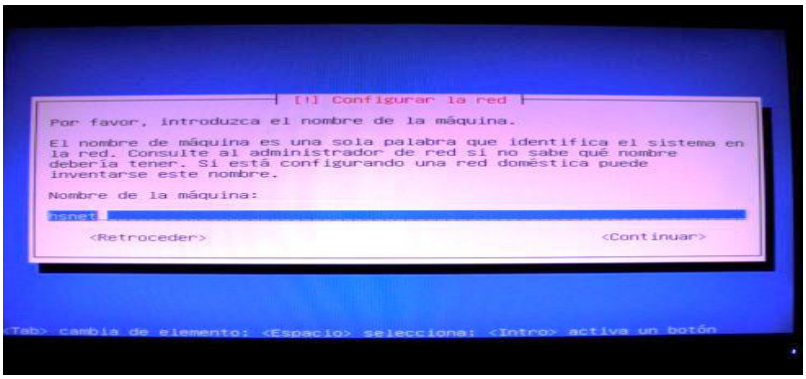


Figura 271: nombre que se le va a signar a la máquina.

Procedemos crear las particiones para nuestro Linux Ubuntu Server, y para ello vamos a usar todo el disco completo, ya que se supone que esta máquina que está montando es un servidor y estará 24 horas funcionando y no la vamos a usar para otra cosa que no sea un servidor (Esta es la opción más sencilla).

Paso 4: A continuación, seleccionaremos el disco duro donde queremos instalar la **Ubuntu Server**

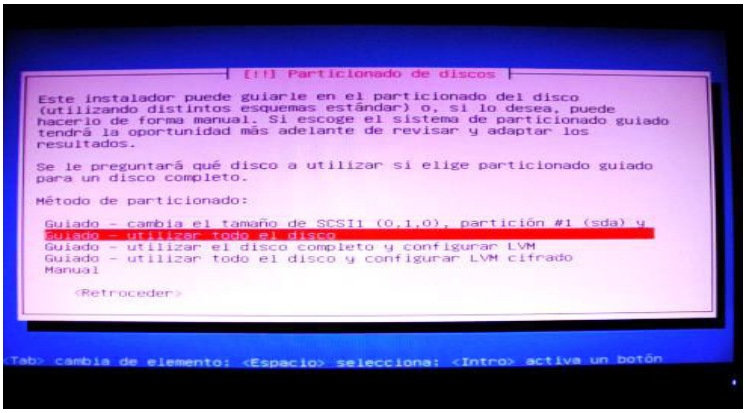


Figura 272: Selección de disco para instalación de Ubuntu Server.

Paso 5: Seguidamente introduciremos un nombre para nuestro usuario (en este caso **www**).

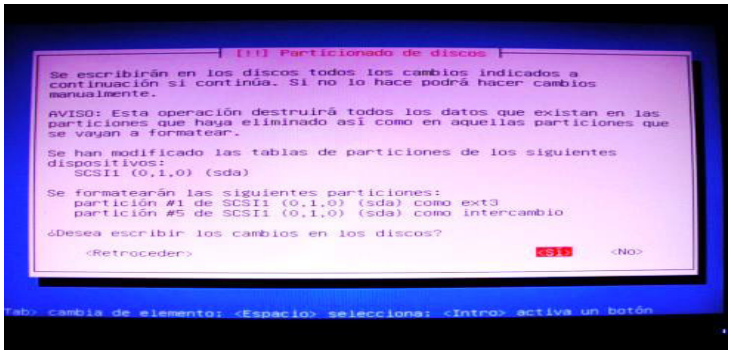


Figura 273: Introducción nombre del usuario.

Paso 6: Si nos encontramos detrás de un **Proxy**, ahora es el momento de indicarle la dirección; si no es tu caso, sigue con el botón "Continuar", ingresando la contraseña.

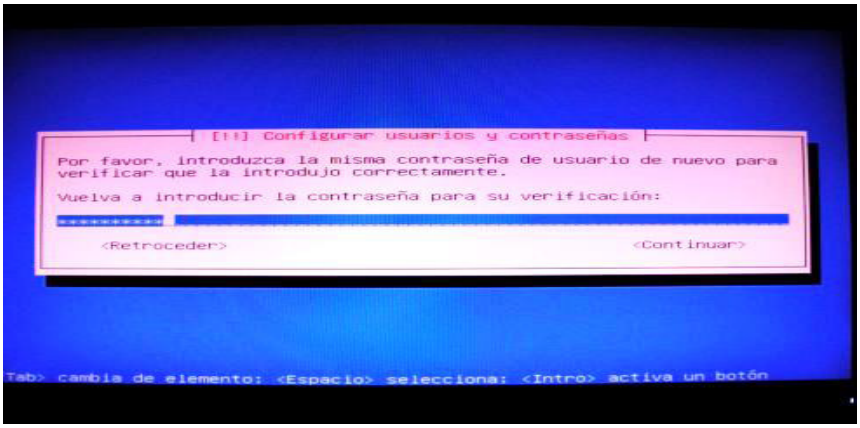


Figura 274: Indicar a proxi la dirección.

Paso 7: Elegir que servicios queremos instalar por defecto una vez concluya la instalación del sistema. En este caso se seleccionará LAMP (describir un sistema de infraestructura de internet) server para que nos instale automáticamente el servidor web Apache, MySQL y PHP, además de otros soportes con los que podremos montar webs o blogs. Con la opción server podemos montar un servidor de impresión con este ordenador y una impresora a la que podremos acceder vía red desde otro ordenador e imprimir lo que se desee. Samba File server también lo activaremos, ya que con él podremos compartir carpetas o particiones completas en nuestra red y serán compatibles con Windows, Linux y Mac.

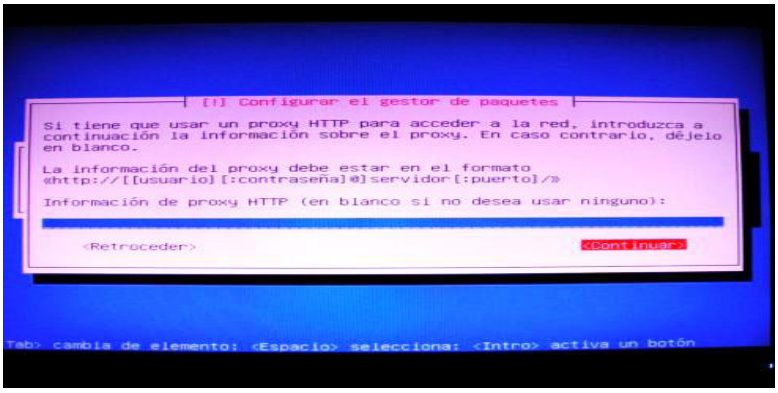


Figura 275: Selección de servicios.

Paso 8: Ingresamos y repetimos la contraseña para verificarla y continuamos.

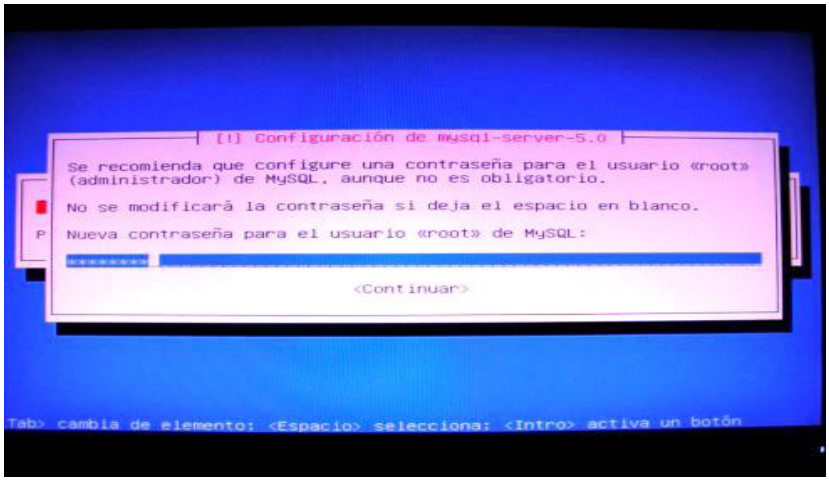


Figura 276: Ingreso y verificación de contraseña.

Paso 9: Terminada la instalación, el sistema expulsará el CD de instalación y lo extraemos de la unidad lectora.

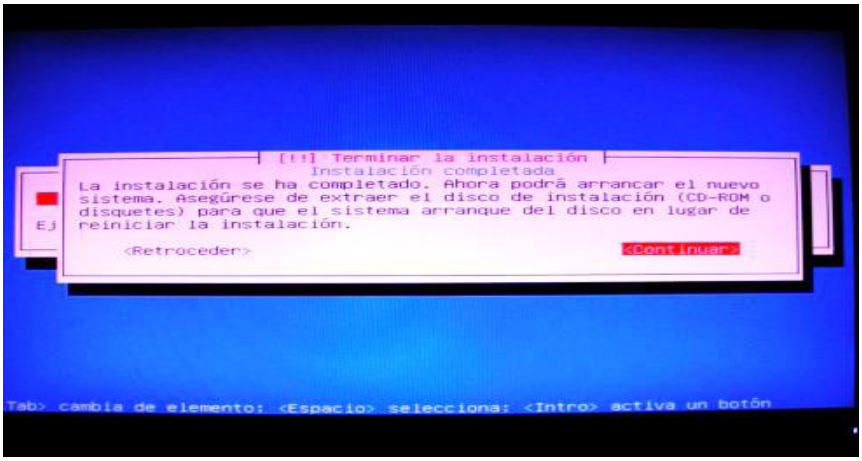


Figura 277: Finalización de instalación.

Paso10: Ingresar con el usuario que creamos anteriormente y darnos un paseo por los directorios para conocer un poco más de esta última versión de Linux Ubuntu Server 8.04.

Configuración de Red

En la instalación del sistema operativo se configuró automáticamente el servicio DHCP para que nuestro router asigne automáticamente una IP. No hemos tenido que configurar nuestra tarjeta de red para nada durante la instalación del sistema, pero vamos a tener que configurarla manualmente.

Vamos a necesitar que nuestra tarjeta de red tenga una IP estática, porque cuando compartamos un servicio Web o Ftp deberemos tenemos que abrir y redireccionar el puerto 80 para el Web y el 21 para el Ftp hacia nuestro servidor, y por consecuente a una IP que a continuación la configuraremos.

Si no configuramos una IP estática y, por el contrario, se nos asigna automáticamente una IP por el servicio DHCP, cuando queramos abrir puertos en nuestro router no vamos a poder decirle hacia que ip tiene que redireccionarse el puerto, ya que la IP de nuestro servidor siempre será diferente.

Paso 11: Ingreso de usuario creado anteriormente www

Paso 12: Vemos que nuestra tarjeta de red primaria está configurada para que se nos asigne una IP automáticamente vía DHCP.



Figura 278: /etc/network/interfaces.

Pasó 13: Configuración estática que se ha asignado.

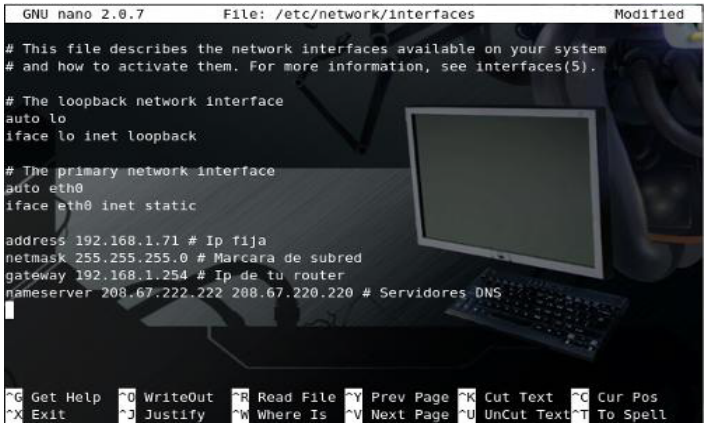


Figura 279: sudo /etc/init.d/networking restart

Asignado la IP 192.168.1.71 ya que mi servidor en Linux Debian tiene actualmente la 192.168.1.70 . Respecto a los servidores DNS se han usado las direcciones de OpenDNS un servicio de revolvedores de nombres que nos ofrecen gratuitamente desde Internet.

Una vez hechas todas las modificaciones al fichero (interfaces) guardaremos el archivo pulsando la tecla "F2", después la "Y" y después "Enter". Con esto hemos guardado los cambios en el fichero y salimos del editor nano.

Paso 14: Reiniciar la red para que los cambios surjan efecto.

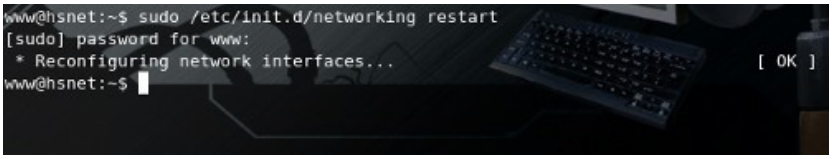


Figura 280: Reiniciar paraguardar cambios.

Ahora deberíamos tener la **IP** que configuramos anteriormente. (En mi caso la 192.168.1.71)

ifconfig

Paso 15: Ahora, cada vez que arranquemos, tendremos la **misma IP** y no una dinámica como teníamos antes.

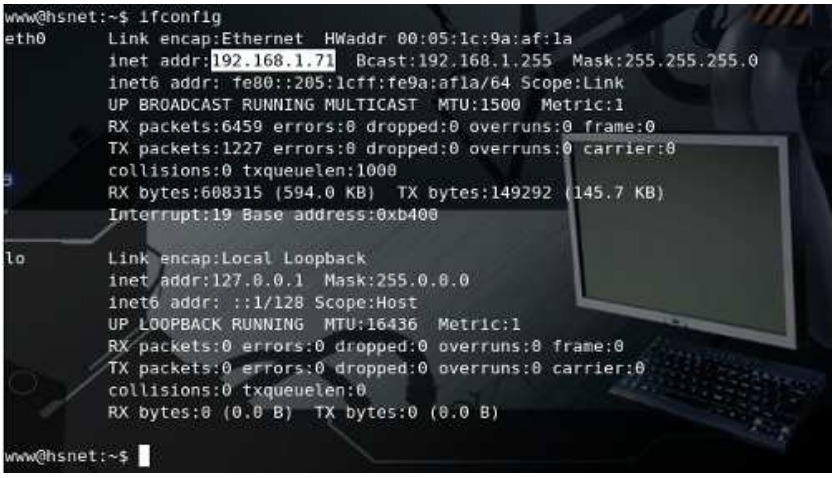


Figura 281: Dirección IP.

Configuración Del Servidor Web

Durante la instalación del sistema operativo Linux Ubuntu Server le indicamos que queríamos montar un servidor Web, y para ello activamos la casilla (LAMP Server). Una vez efectuada la instalación de LAMP Server tenemos que configurar algunas cosas para que todo funcione a nuestro gusto y podamos tener control sobre ello. Si nos sale esta pantalla es que de momento todo va bien y el Servidor Web Apache funciona correctamente.

cd /var/www

Crearemos un fichero llamado prueba.php con el editor nano.

sudo nano prueba.php



Figura 282: sudo nano prueba.php.

Tan solo nos queda abrir ese fichero en el navegador introduciendo la dirección **IP** del servidor seguido del fichero **prueba.php** (En mi caso **http://192.168.1.71/prueba.php**).

Ahora sí que podemos estar seguros de que nuestro servidor Web funciona y tiene soporte para **PHP**. Procedemos a configurar **MySQL** que formará parte de este **servidor Web** en el que podremos montar un **Blog** con **WordPress** o usar las bases de datos para lo que cada uno

quiera. Seguidamente instalaremos PhpMyAdmin para administrar nuestras bases de datos con :$ sudo apt-get install phpmyadmin

Paso 16: Seleccionar la opción Apache2.



Figura 283: Selección opción Apache.

A continuamos con la opción "**Ok**". Una vez terminada la instalación abriremos un navegador e introducimos la **url** de nuestro servidor seguido de la ruta **/phpmyadmin/** (En mi caso **http://192.168.1.71/phpmyadmin/**).

Paso 17: Si no se accedió a PhpMyAdmin con el usuario (root), accediéramos con el usuario admin y dejáramos la casilla para el password vacía también.

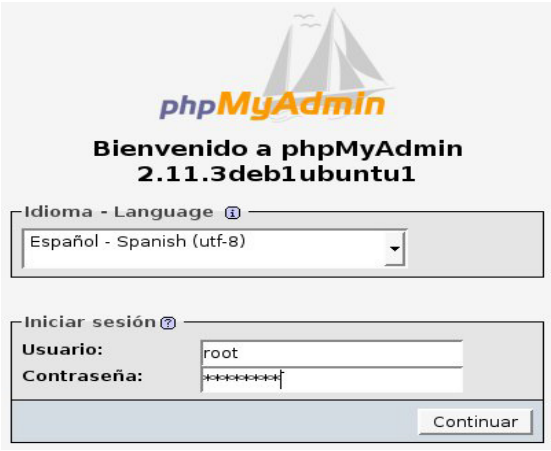


Figura 284: Acceso a PhpMyAdmin

Paso 18: Ahora marcamos los tres primeros usuarios llamados (**cualquiera**) y seguidamente hacemos clic sobre el botón "Continuar".

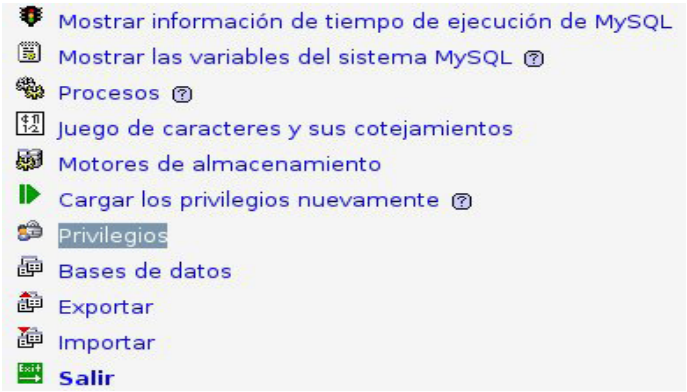


Figura 285: Selección de privilegios.

Para subir y bajar archivos hacia el servidor en Linux Ubuntu Server necesitamos instalar un software que sea capaz de ofrecer este servicio. Proftpd, para mí, es el mejor software para servidor FTP que he probado. Esta vez voy a usarlo para este servidor que estamos montando. A continuación, instalarla y configurarlo para que podamos subir y bajar archivos de nuestro servidor en Linux Ubuntu Server.

Editamos el fichero **proftpd.conf** con:**sudo nano /etc/proftpd/proftpd.conf**

Paso 19: Ingresar DefaultRoot.

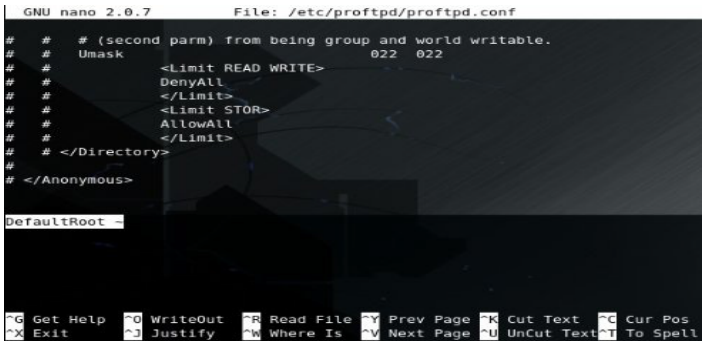


Figura 286: proftpd.conf con:sudo nano /etc/proftpd/proftpd.conf

Paso 20: Si accedemos a nuestra cuenta **FTP** con nuestro usuario podremos navegar por nuestro directorio **/home/usuario**

```
www@hsnet:/etc/proftpd$ sudo /etc/init.d/proftpd restart
 * Stopping ftp server proftpd                                    [ OK ]
 * Starting ftp server proftpd                                    [ OK ]
www@hsnet:/etc/proftpd$
```

Figura 287:sudo /etc/init.d/proftpd restart

Para esto, configuramos uno de los ficheros de Apache Web Server y le indicaremos que la raíz de nuestro servidor Web será uno de los directorios que se encuentra dentro de nuestra cuenta de usuario.

Para empezar, vamos a crear un directorio dentro de nuestro home donde todo lo que copiemos lo podremos compartir vía web.

sudo apt-get install no-ip

Paso 21: Se debe introducir el nombre con el que está identificada nuestra tarjeta de red. Esto podemos verlo con el comando **ifconfig**.

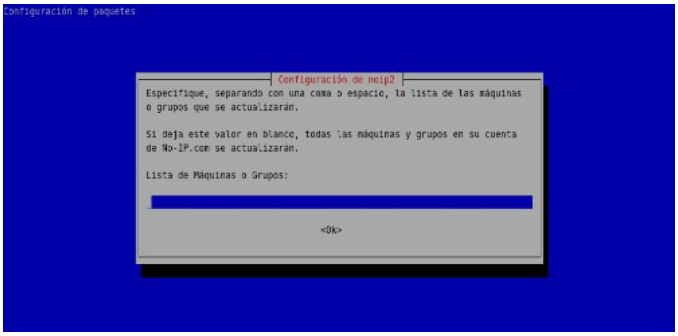


Figura 288: Listado de máquinas o grupos.

Paso 22: Seleccionamos **No** y listo.

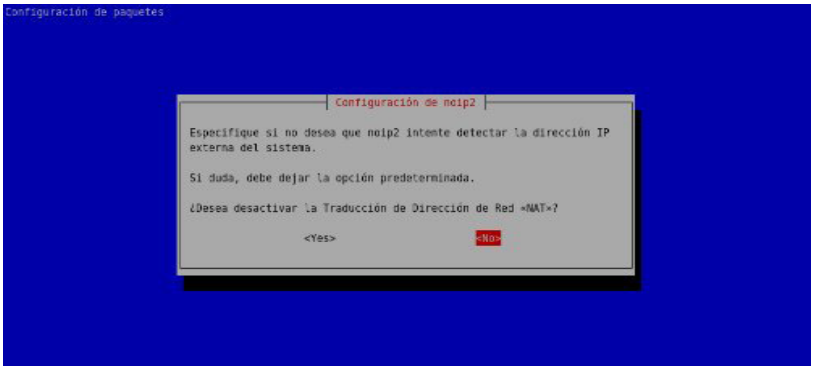


Figura 289: Configuración de no1p2.

Una vez completados todos los pasos podemos estar seguros de que cuando nuestra IP cambie, nuestro servidor mandará un aviso con nuestra IP hacia el servicio de No-IP y relacionará el dominio que registramos con nuestra IP actual.

Servidor FTP

En general, de cualquier distribución de Linux se pueden montar de forma muy sencilla diferentes servicios, y entre estos servicios el más interesantes que podemos disfrutar en nuestra máquina es un servicio ftp.

Un servicio o demonio es una aplicación o programa que se ejecuta en segundo plano, y cuya función más habitual es la de ofrecer servicios a otros programas, vamos a instalar de forma muy sencilla un servicio FTP, que es un protocolo de transferencia de archivos. Es más, se trata de la transferencia de archivos más utilizada en Internet.

Instalación servidor ftp

Paso 1: Para la Instalación vsftpd usaremos el siguiente comando:

Comando: yum -y install vsftpd

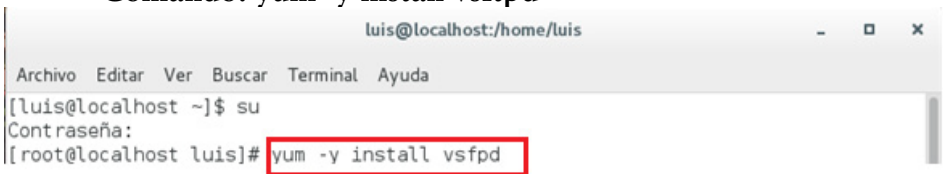


Figura 290: descarga de los paquetes del servidor.

Paso 2: A continuación, accederemos al archivo de configuración usando el editor vim; para ello, ingresamos esta línea y veremos lo siguiente, con el comando:

Comando: Vim /etc/vsftpd/vsftpd.conf

Y editamos lo siguente

allow_writeable_chroot=YES

pasv_enable=Yes

pasv_min_port=40000

pasv_max_port=40100



Figura 291:Vista de edición del archivo vsftpd.conf.

Paso 3: Reiniciamos el servicio con el comando:

Comando: systemctl restart vsftpd.service

```
[root@localhost vsftpd]# systemctl restart vsftpd.service
[root@localhost vsftpd]#
```

Figura 292:Vista de reinicio del servicio.

Paso 4: Ensamblamos el servicio para que se ejecute correctamente con el comando:

Comando: systemctl enable vsftpd.service

```
[root@localhost vsftpd]# systemctl enable vsftpd.service
[root@localhost vsftpd]#
```

Figura 293:vista de ensamblado del servicio.

Paso 5: Se tiene que permitir que el Firewall habilite el acceso vía FTP, e ingresamos el siguiente comando:

Comando: firewall-cmd --permanent --add-service=ftp

```
[root@localhost vsftpd]# firewall-cmd --permanent --add-service=ftp
Warning: ALREADY_ENABLED: ftp
success
[root@localhost vsftpd]#
```

Figura 294: vista del permiso de acceso del ferewall

Paso 6: Posteriormente recargamos el servicio usando el comando:

Comando: firewall-cmd –reload

```
[root@localhost vsftpd]# firewall-cmd --reload
success
[root@localhost vsftpd]#
```

Figura 295:vista del reinicio del firewall.

Paso 7: Recordemos que SEinux (Security-Enhanced Linux) es un módulo de seguridad que permite aplicar políticas de seguridad para el acceso de los usuarios. Para habilitarlo en Centos 7.0 ingresaremos el siguiente comando:

Comando: setsebool -P ftp_home_dir on

```
[root@localhost vsftpd]# setsebool -P ftp_home_dir on
setsebool:  SELinux is disabled.
[root@localhost vsftpd]#
```

Figura 296: vista del aplicar las políticas de Linux.

De esta forma, hemos habilitado permisos de FTP dentro de Centos 7.0.

Crear del usuario para el acceso por FTP

Para gestionar correctamente los permisos de los usuarios, hemos de crear dichos usuarios locales en el servidor, para así poder gestionar los permisos de acceso y que puedan utilizar y transferir documentos de un lado a otro entre cliente y servidor.

A continuación, crearemos el usuario cliente1, el cual será el usuario a utilizar para acceder vía FTP a Centos 7.0 y lo crearemos en la ruta /sbin/nologin para evitar que el Shell acceda al servidor

Paso 1: En este caso ingresaremos lo siguiente:

Comandos: useradd -m cliente1 -s /sbin/nologin

```
[root@localhost vsftpd]# useradd -m cliente1 -s /sbin/nologin
[root@localhost vsftpd]#
```

Figura 297: Creación del de un nuevo usuario.

Paso 2: Establecemos la contraseña usando el comando:

Comandos: passwd cliente1

```
[root@localhost vsftpd]# passwd cliente1
Cambiando la contraseña del usuario cliente1.
Nueva contraseña:
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 8 caracteres
Vuelva a escribir la nueva contraseña:
passwd: todos los símbolos de autenticación se actualizaron con éxito.
[root@localhost vsftpd]#
```

Figura 298: cambio de contraseña del cliente1

Conectar al cliente desde otra máquina

Paso 1: En este punto ya podemos conectarnos usando algún cliente con Filezilla, usando el puerto 21.

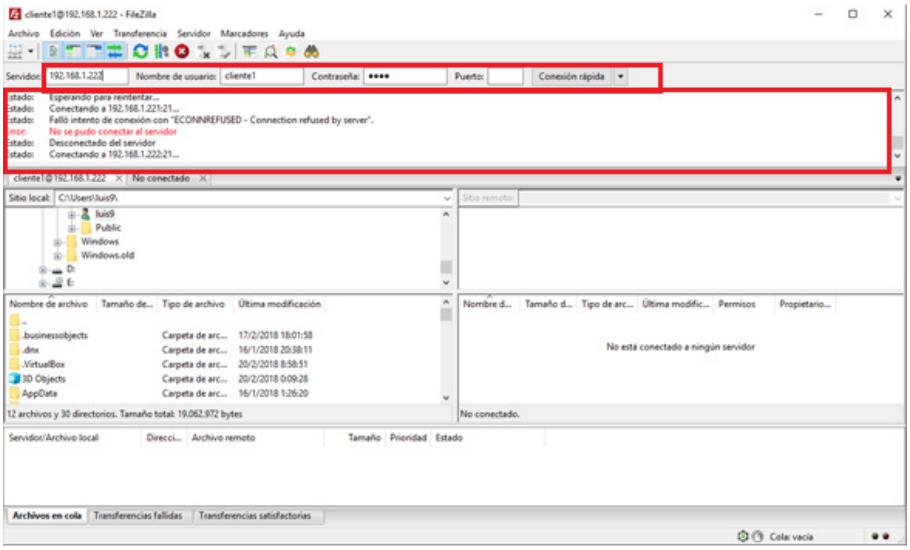


Figura 299: Entrada desde un cliente Windows con Filezilla.

Ingresamos nuestras credenciales con el usuario recién creado.

CAPÍTULO 15:
INSTALACIÓN DE SISTEMAS OPERATIVOS DE SOFTWARE LIBRE



En este capítulo usted encontrará:

- *Instalación de LINUX Ubuntu.*
- *Instalación de Kali Linux en la máquina virtual y cambio de contraseña del root.*
- *Debian 9.3.0.*
- *Instalación y configuración de openvpn de host a red desde un cliente FEDORA.*

Instalación de Linux Ubuntu 18.10

Paso 1: Una vez montada la máquina virtual con Ubuntu, arrancamos; en esta ocasión seleccionamos Instalar Ubuntu o bien, si estamos ante el escritorio, por haber arrancado en el modo de prueba, hacemos doble clic en el icono Instalar.



Figura 300: Instalación de UBUNTU

Paso 2: Se inicia entonces el asistente de instalación. Aunque no es estrictamente necesario, es muy conveniente que durante la instalación tenga acceso a Internet. En ese caso marcamos las casillas Descargar actualizaciones mientras se instala e Instalar software de terceros. Una vez hecho esto pulsamos en "Continuar".

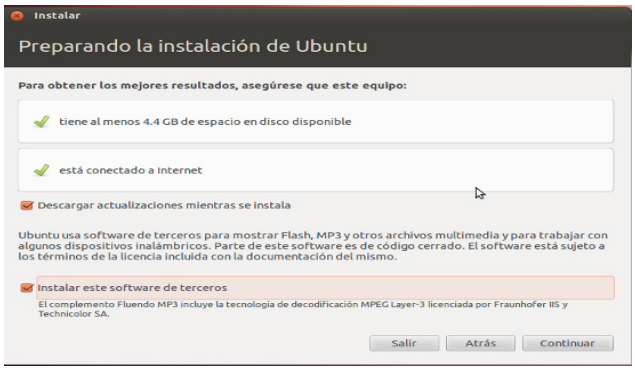


Figura 301: Preparación de instalación.

Paso 3: Si su ordenador dispone de una conexión Wifi y todavía no ha configurado la red, el asistente le dará ahora la oportunidad de hacerlo. Marque la casilla Conectarse a esta red, seleccione la red y escriba la contraseña de acceso.

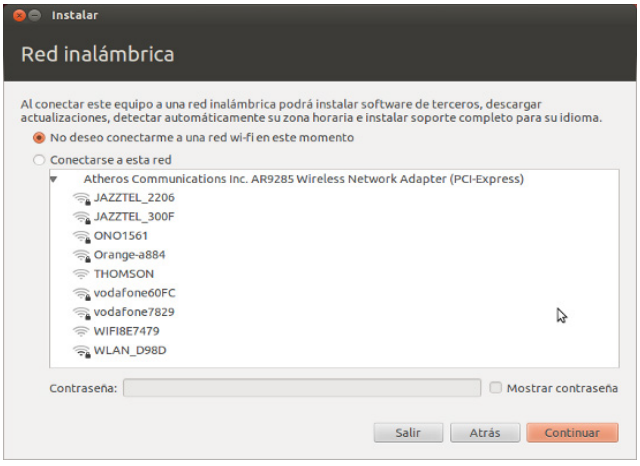


Figura 302: Conexión a redes wifi.

Paso 4: En la parte superior de la pantalla que veremos a continuación se muestra la capacidad de nuestro disco. En la parte inferior se observa una posible división del disco. Si queremos cambiar la asignación de espacio situamos el cursor entre las dos mitades y arrastramos hacia la derecha o izquierda según queramos dar más espacio a Windows (cuadro de la izquierda) o a Ubuntu (cuadro de la derecha). En todo caso, ambos cuadros tienen un límite hasta el que podemos reducirlos representado por el espacio que actualmente ocupa Windows, y el espacio mínimo que Ubuntu necesita para instalarse. Llegados a este límite no podremos seguir arrastrando. Una vez hecho esto, pulsamos en "Instalar ahora".



Figura 303: Asignación de espacio.

Paso 5: Se nos advierte ahora que se van a llevar a cabo las operaciones de cambio de asignación de espacio en el disco. Pulsamos en "Continuar".

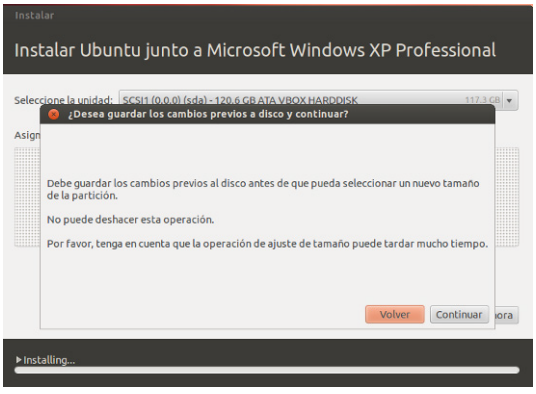


Figura 304: Alerta de instalación.

Paso 6: Comienza ahora un proceso de trabajo simultáneo. Mientras Ubuntu cambia el tamaño de asignación en el disco, le da fomato y copia los archivos necesarios, se nos irán preguntando los datos necesarios para personalizar la instalación. En primer lugar debemos seleccionar nuestra zona horaria. Para ello hacemos clic en el lugar adecuado del mapa o bien escribimos Ecuador en la caja de texto al pie de la ventana.



Figura 305:Zona horaria.

Paso 7: A continuación, seleccionamos nuestra distribución de teclado.

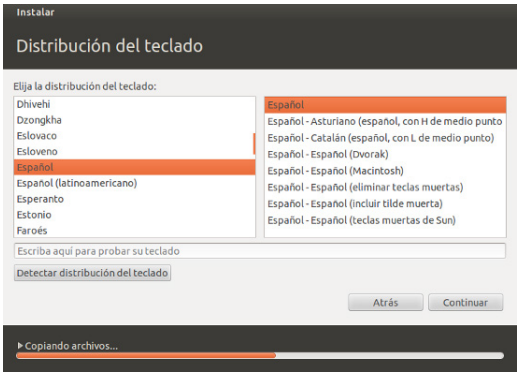


Figura 306: Idioma y teclado.

Paso 8: A partir de ahora y hasta el final de la instalación se irán mostrando una serie de diapositivas con algunas de las características más sobresalientes de Ubuntu. Si así lo indicó se descargarán las actualizaciones disponibles, con lo que el proceso de instalación se alargará considerablemente, dependiendo de la velocidad de su conexión a Internet.

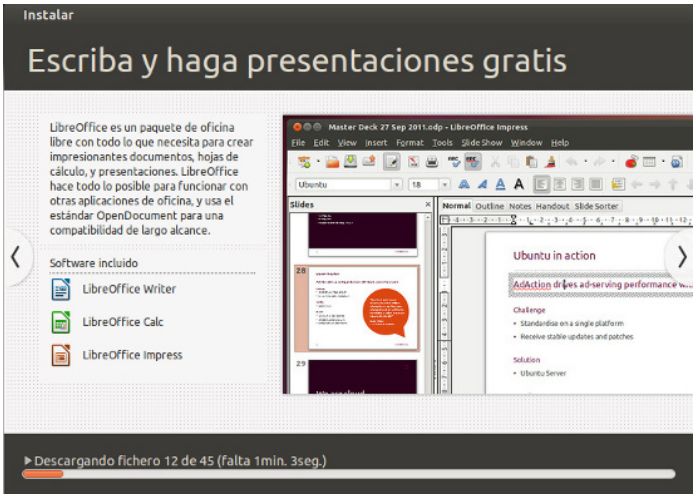


Figura 307: Contenido de Ubuntu.

Paso 9: Si todo va bien, se observará la pantalla final de instalación pidiendo que reinicie el sistema.

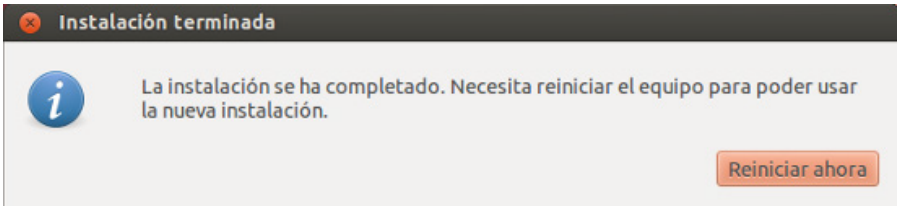


Figura 308: Mensaje de reinicio del equipo.

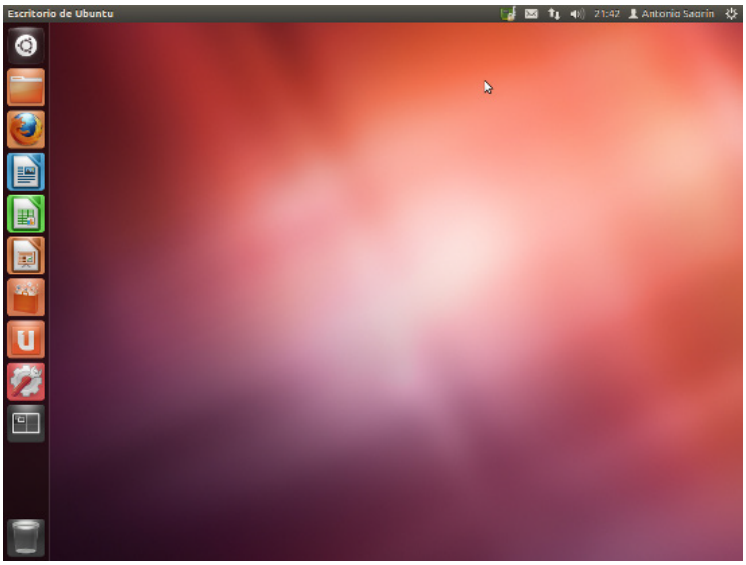


Figura 309: Escritorio de Ubuntu.

Qué es Kali Linux

Kali Linux es un sistema y una distribución basada en debian, la distribución en cuestión contiene cientos de herramientas que permiten llevar a cabo para realizar auditorías de seguridad. Kali es la distribución por excelencia en el sector de la seguridad informática y es utilizado por aficionados y profesionales del sector. Kali llegó en un rango bajo, pero en poco tiempo se hizo famoso; hoy en día es una de las herramientas más utilizadas. La distribución se basa en debían; y yesi tiene soporte para un gran número de escritorios como kde, genoma, mate, entre otros.

Instalación de Kali Linux en la máquina virtual y cambio de contraseña del root

Paso 1: Una vez descargado la iso del enlace siguiente:

https://www.kali.org/

Comenzaremos a instalarlo en la máquina virtual.

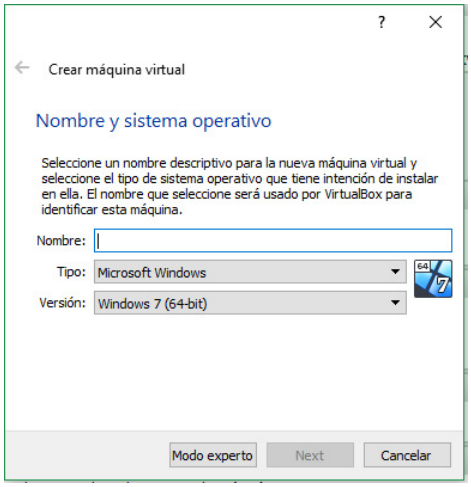


Figura 310: Crear la máquina.

Paso 2: Colocamos el nombre: **Kali Linux**

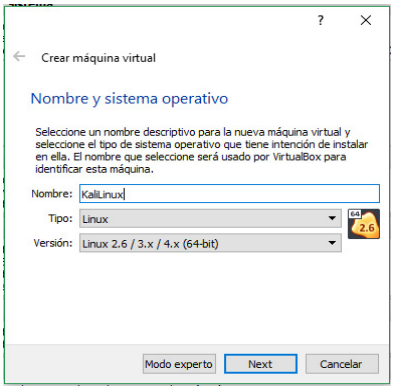


Figura 311: nombre Kali Linux.

Paso 3: Colocamos next hasta que se comience la instalación en la máquina, después tendremos que instalarlo como sistema operativo.

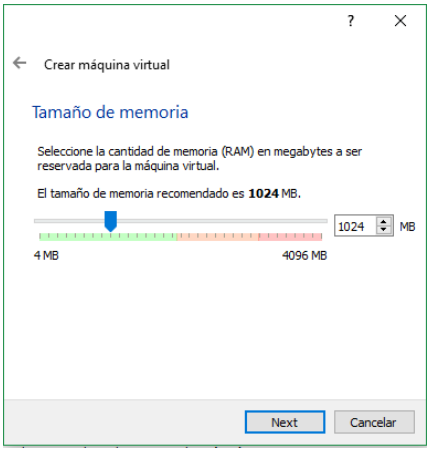


Figura 312: Asignamos el espacio.

Paso 4: Creamos el espacio en el disco.

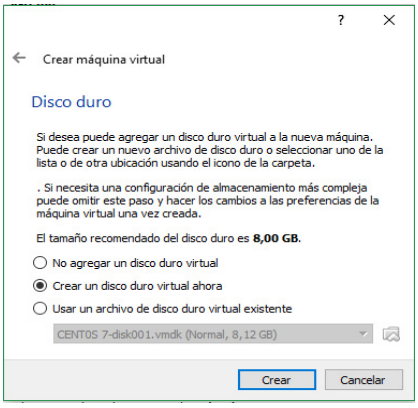
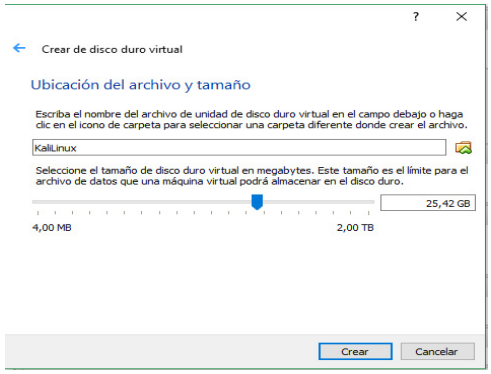


Figura 313: Creamos el disco.

Paso 5: Escogemos el tipo de archivo que es el siguiente: **VDI (VirtualBox Disk Image)**



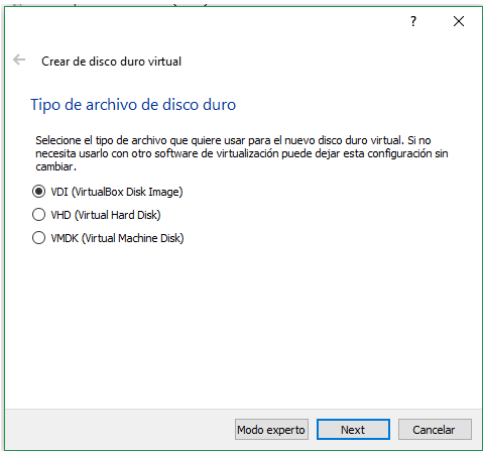


Figura 314:Tipo de archivo.

Paso 6: Escogemos el almacenamiento en la unidad de disco duro

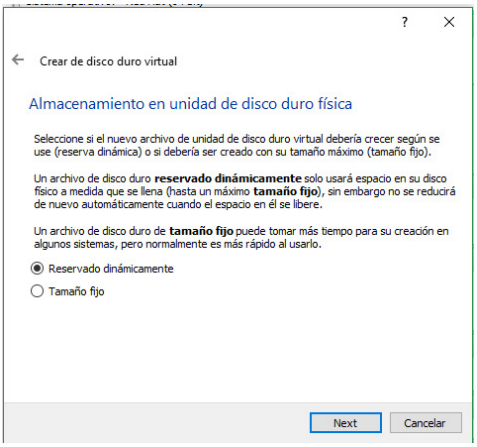


Figura 315: Almacenamiento en la unidad.

Paso 7: Escogeremos el tamaño de memoria dependiendo de su computador, colocamos crear y se nos creará la máquina.

Paso 8: Iniciamos la máquina para proceder a instalar Kali Linux, nos pedirá seleccionar dónde está descargada la iso. Se mostrará la siguiente ventana.

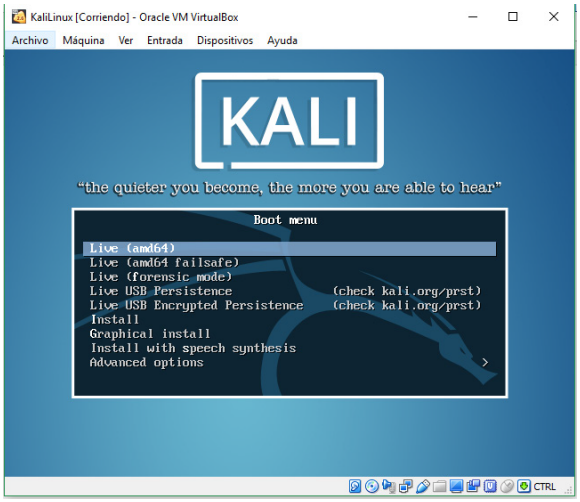


Figura 316: Inicio de la máquina.

Paso 9: Seleccionamos **Graphical install.**



Figura 317: Seleccionamos Graphical Install.

Paso 10: Escogemos el idioma.

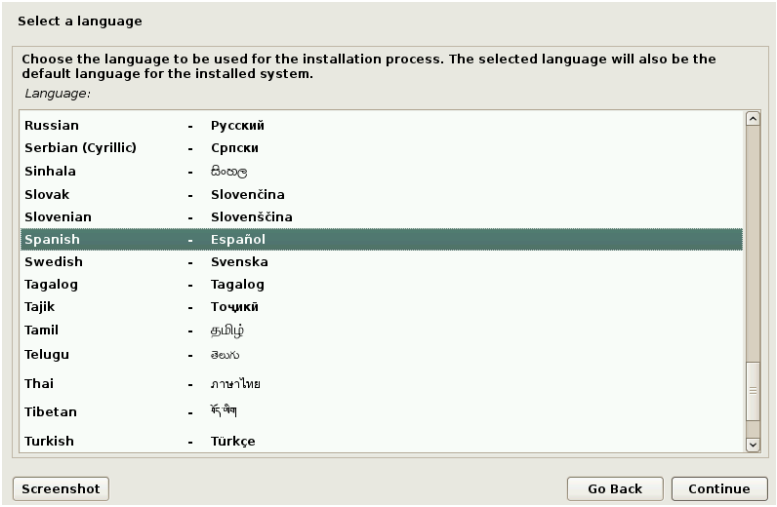


Figura 318: Idioma.

Paso 11: Colocamos la opción sí.



Figura 319: Confirmación de idioma.

Paso 12: Colocamos el país.

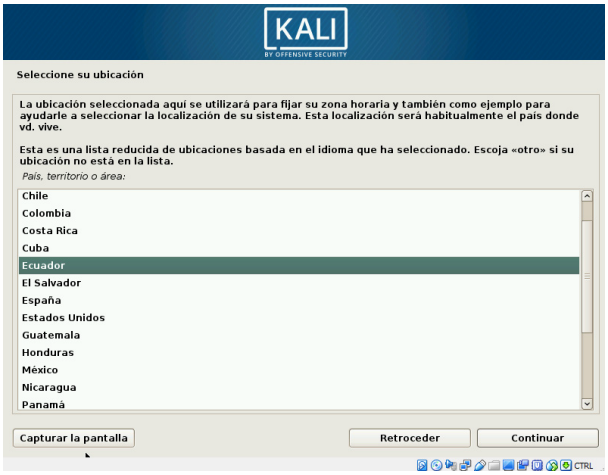


Figura 320: Seleccionamos Ecuador

Paso 13: Se cargarán los componentes.

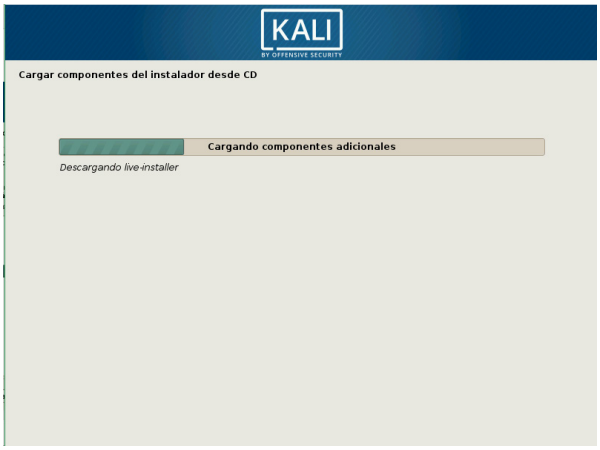


Figura 321: Cargando los componentes.

Paso 14: Lo dejamos con el nombre por defecto.

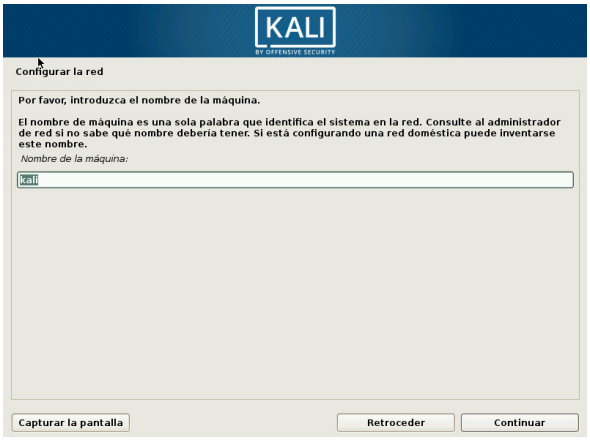


Figura 322:Nombre de la máquina.

Paso 15: Damos clic en "Continuar", y dejamos en blanco la casilla.



Figura 323: Nombre de dominio.

Paso 16: A continuación, colocamos la contraseña de root.



Figura 324: Contraseña de root.

Paso 17: Comenzará a configurar, colocamos en **UTILIZAR TODO EL DISCO DURO.**

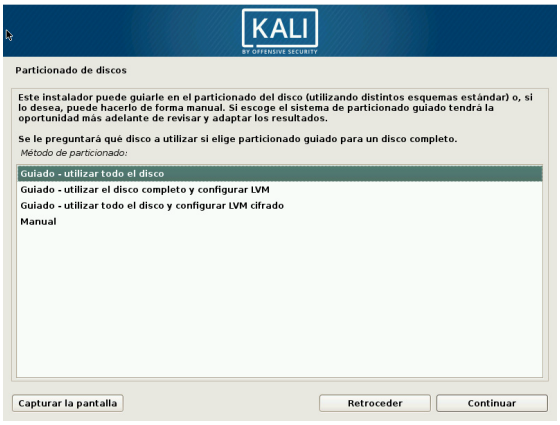


Figura 325: Seleccionar utilizar todo el disco duro.

Paso 18: Hacemos clic en "Continuar".



Figura 326: Clic en continuar.

Paso 19: Nos mostrará el siguiente mensaje advirtiendo que van a sobrescribir los datos, autorizamos colocando que **sí.**



Figura 327: Aprobamos el montaje.

Paso 20: Mostrará la siguiente ventana y comenzará a instalarse nuestro sistema.



Figura 328: Instalación.

Paso 21: Una vez acabada la instalación, pedirá el usuario, por defecto es **root** y la contraseña que colocamos al principio. Nos mostrará la siguiente interfaz.



Figura 329: Interfaz de Kali.

Paso 21: Reiniciaremos la máquina y nos aparecerá la siguiente ventana, colocamos en la opción que está marcada presionamos enter.

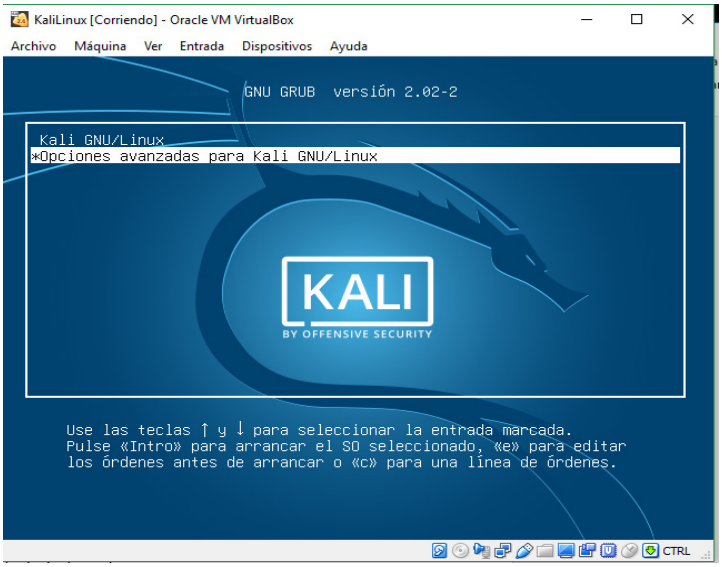


Figura 330: Reinicio de la máquina.

Paso 22: Presionamos la letra E y aparecerá la siguiente ventana.

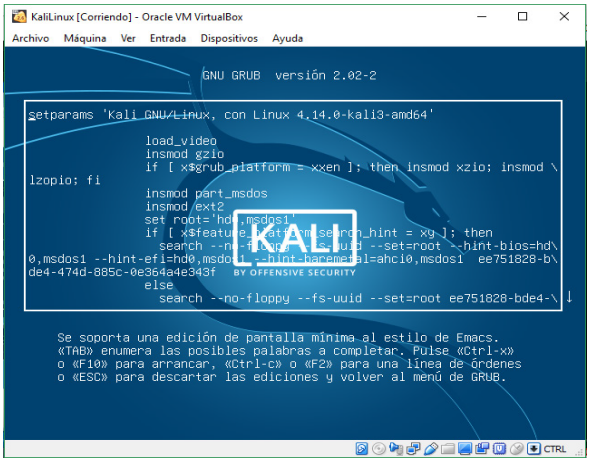


Figura 331: Comandos de Kali.

Paso 23: Nos ubicamos en la parte señalada. Borramos hasta la parte **ro** y remplazamos con la siguiente línea siguiente **rw init=/bin/bash**

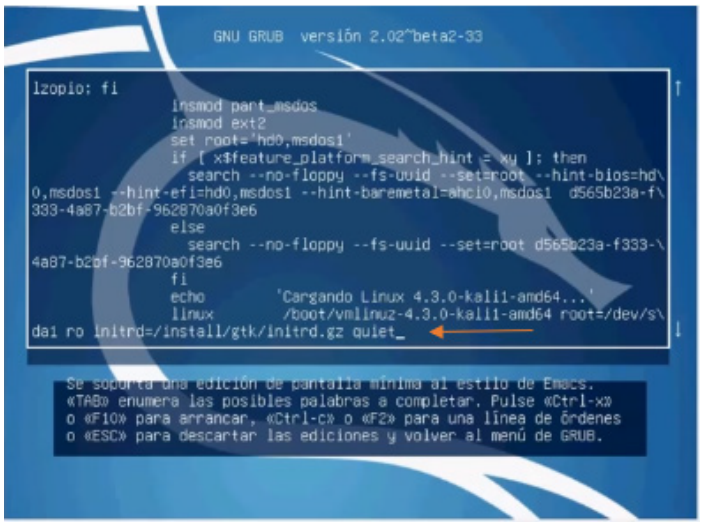


Figura 332: Cambiamos el código.

Paso 24: Presionamos "F10".

Paso 25: Nos mostrará la siguiente ventana, en la línea de **root none** indica que no hay ninguna contraseña para el root colocamos la nueva contraseña.

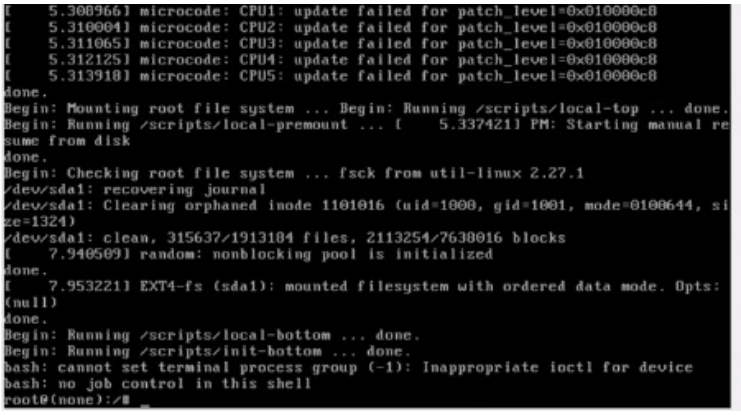


Figura 333: Contraseña de root.

Paso 26: Colocamos el siguiente comando para poner la nueva contraseña: passwd

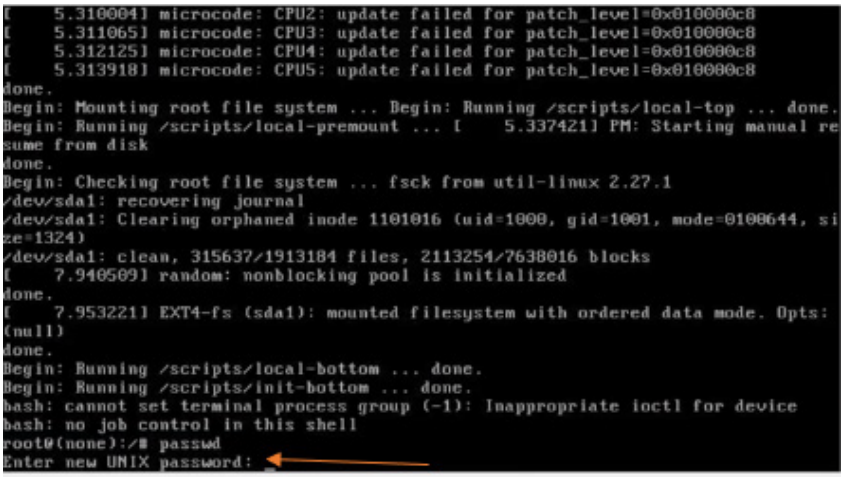


Figura 334: Nueva contraseña.

Paso 27: Nos pedirá que coloquemos la nueva contraseña, y la confirmación de la misma.

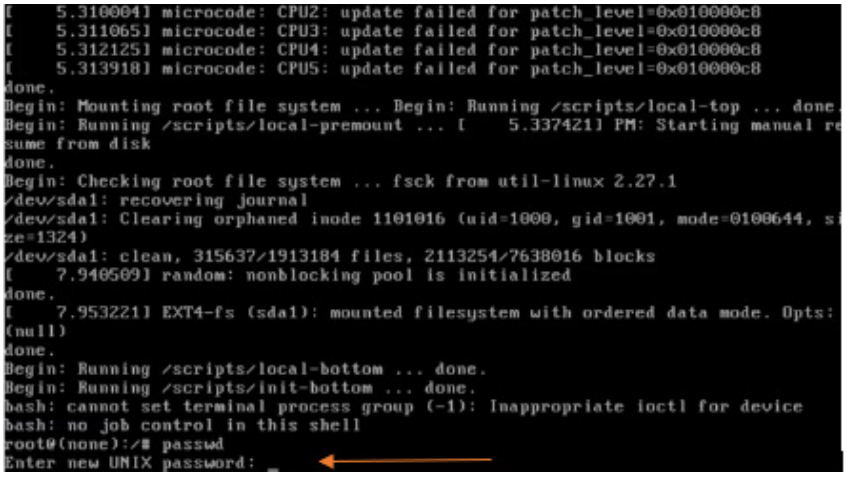


Figura 335:Repetimos la contraseña.

Paso 28: Se mostrará el siguiente mensaje que nuestra contraseña fue cambiada con éxito



Figura 336: Confirmación de contraseña.

Paso 29: Colocamos el siguiente comando para reiniciar la máquina: **reboot -f** y presionamos enter

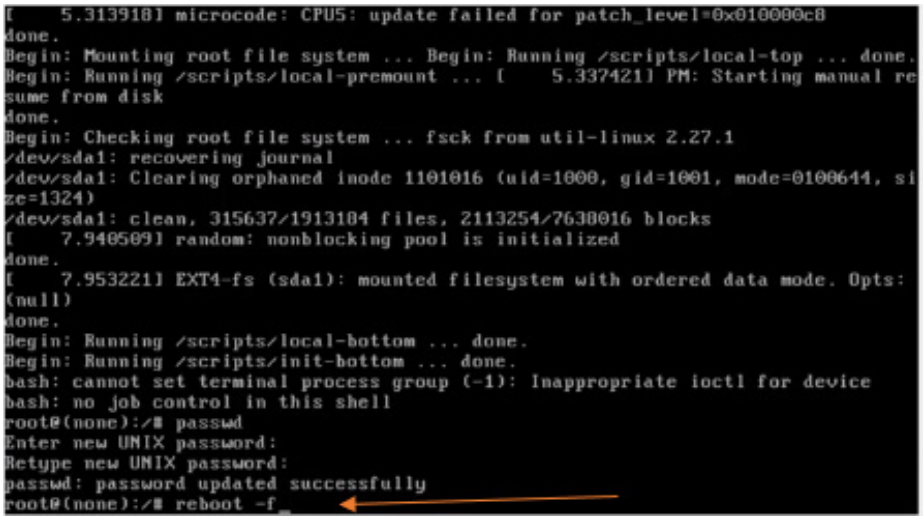


Figura 337: Reiniciar la máquina.

Paso 30: Se iniciará y colocaremos en el nombre root y la contraseña que hemos cambiado.

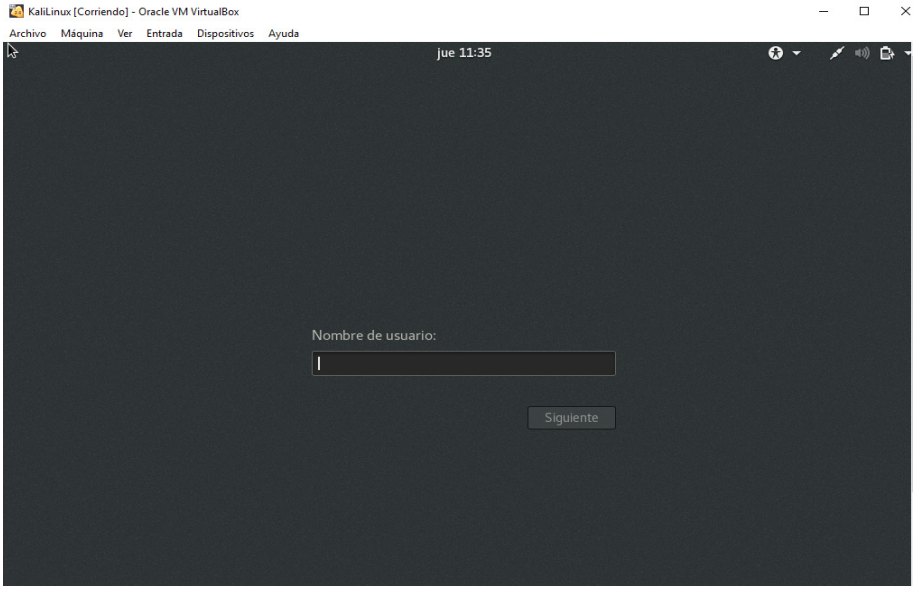


Figura 338: Inicio de sesión.

Paso 31: Colocamos la contraseña.

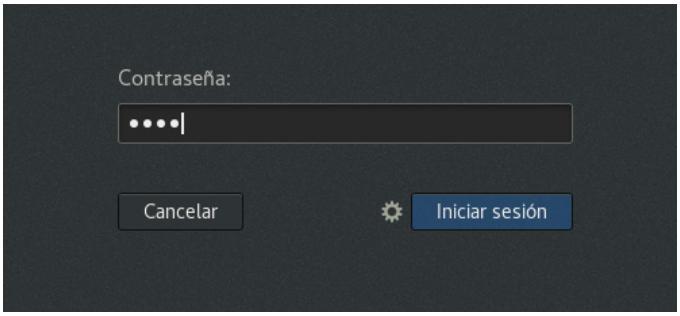


Figura 339: Ingreso de contraseña.

Paso 32: Se ha cambiado la contraseña del root.



Figura 340: Trabajo terminado

Debian 9.3.0

¿Qué es Debian 9.3.0?

Debian es una organización formada totalmente por voluntarios dedicada a desarrollar software libre y promocionar los ideales de la comunidad del software libre.

Los desarrolladores de Debian están involucrados en una gran variedad de tareas, incluyendo la administración del Web y FTP, diseño gráfico, análisis legal de licencias de software, escribir documentación y, por supuesto, mantener paquetes de software.

¿Para qué sirve Debian 9.3.0?

Debian se ha convertido en la distribución de Linux más empleada en servidores para portales web utilizando Linux. En concreto, Debian se utiliza en el 30% aproximadamente de estos servidores Linux. Con ello, se ha convertido en el sistema operativo que más ha crecido dando soporte a portales web en todo Internet.

Instalación Debian 9.3.0

Paso 1: Se debe tener el disco de instalación (iso) en nuestra máquina.

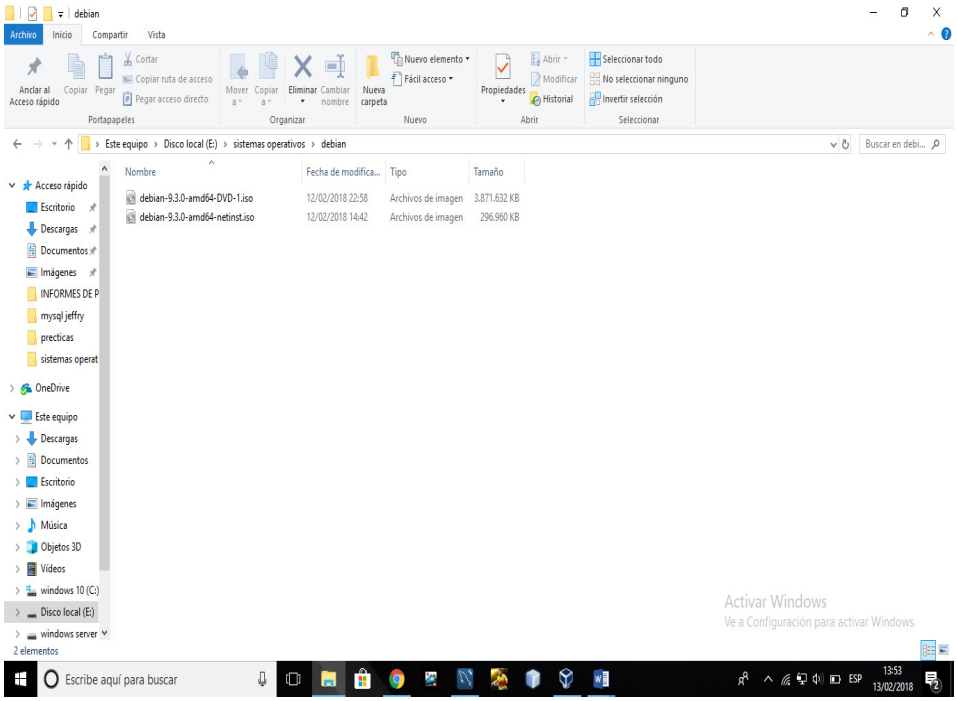


Figura 341: instaladores Debian.

Como se puede observar en la imagen, ya se tienen descargados los instaladores, o si no los tienen aquí está el link donde pueden hacer la descarga de Debian.

https://cdimage.debian.org/debian-cd/current/amd64/iso-dvd/debian-9.3.0-amd64-DVD-1.iso

Paso 2: Se procede a instalar Debian el virtual box, lo primero que se va a hacer es tener instalado virtual box en nuestro ordenador (computadora) luego lo abrimos y nos mostrará la siguiente pantalla.

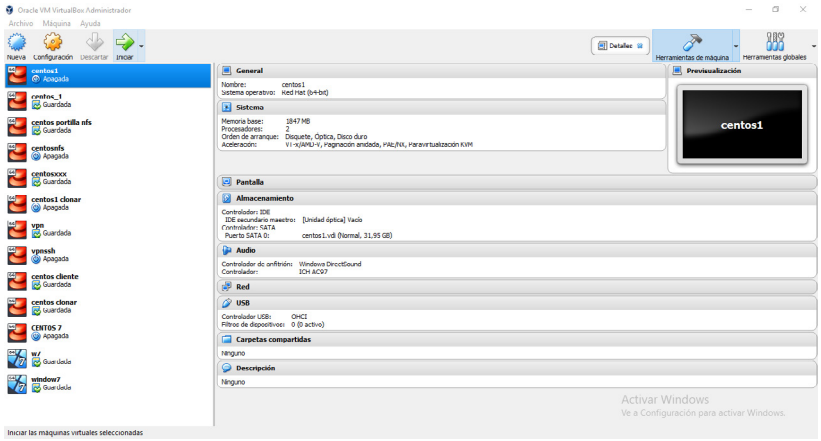


Figura 342: Instalación de virtual box.

Luego de tener abierto le hacemos clic en opción “Nueva” para crear una nueva máquina virtual.

Paso 3:



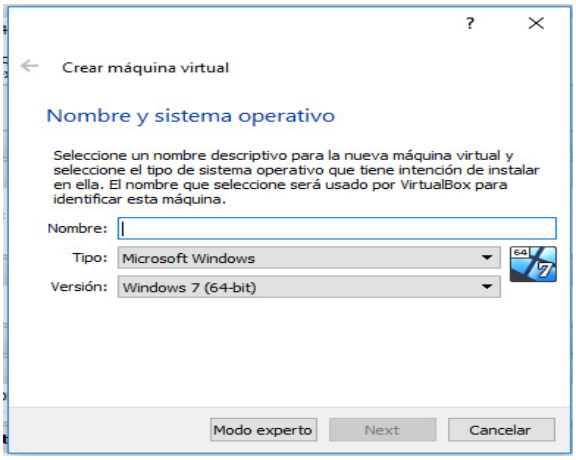


Figura 343: Nombre y sistema operativo.

La siguiente ventana permite crear el nombre de nuestra máquina virtual, el tipo de sistema operativo; y en la versión que tiene a continuación, esta será la pantalla que se mostrará cuando coloquemos los detalles solicitados.

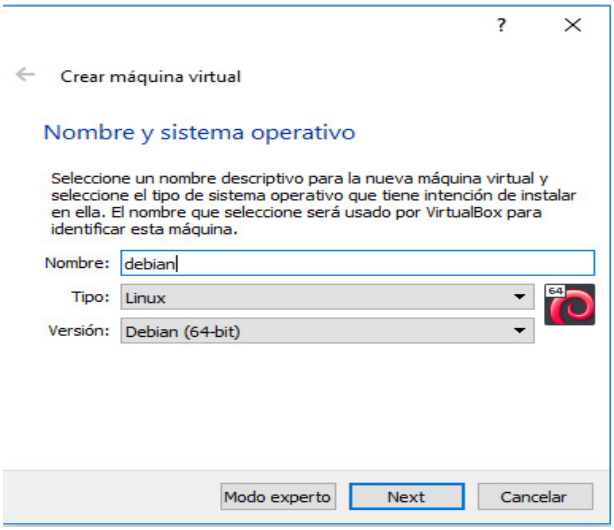


Figura 344:Creación máquina virtual.

Presionamos en el botón Next.

Paso 4:

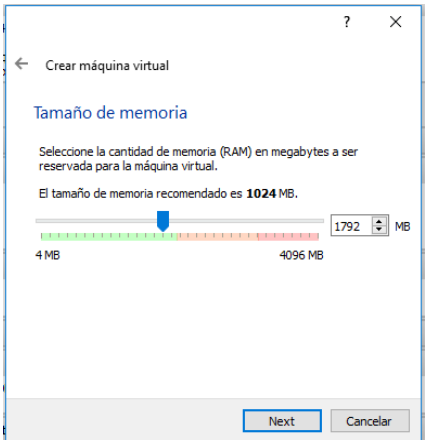


Figura 345: Creación máquina virtual.

En la siguiente pantalla mostrará la cantidad de memoria que reservará en nuestra máquina virtual. Después hacemos un clic en "next".

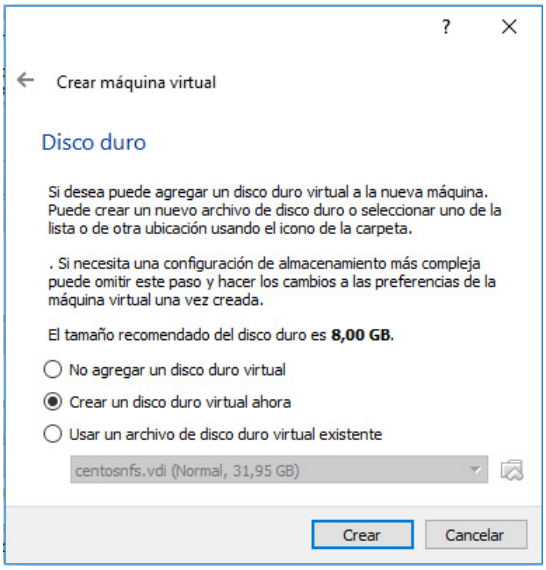
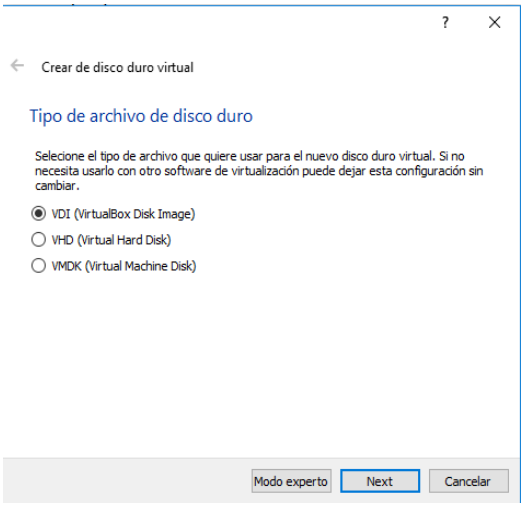


Figura 346: Memoria reservada para máquina virtual.

En esta pantalla pregunta si deseamos agregar un disco, crear un disco y utilizar un disco existente, vamos a seleccionar la opción crear.



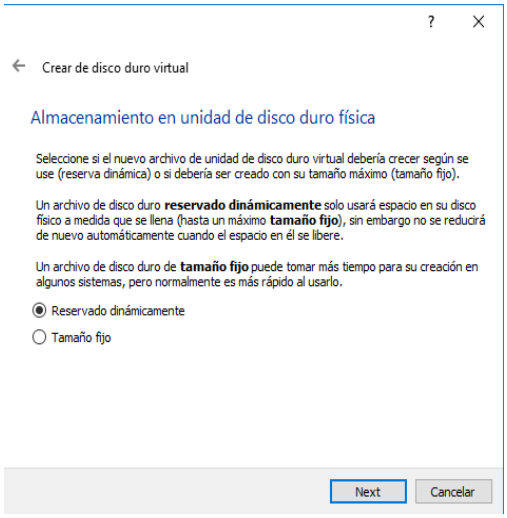


Figura 347: *Creación disco duro virtual.*

Paso 5:

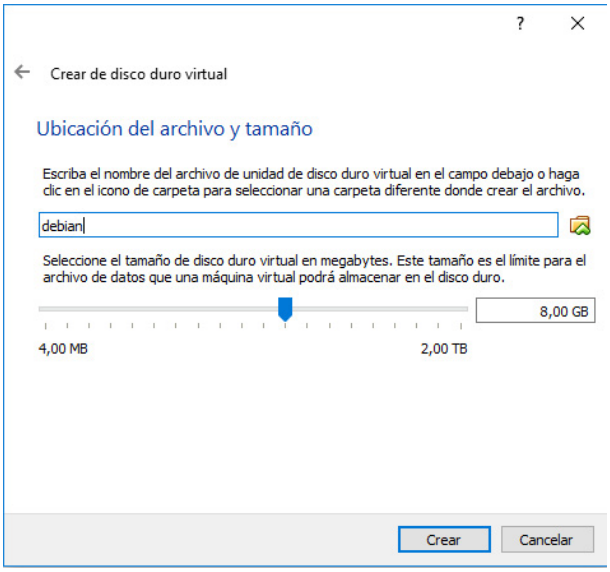


Figura 348: Ubicación de disco duro virtual.

Se muestra el tamaño que tendrá nuestro disco virtual, donde debemos asignar el tamaño, hacemos clic en crear.



Ya está lista nuestra máquina virtual para hacer la instalación Debian.

Paso 6:

Haga clic en iniciar



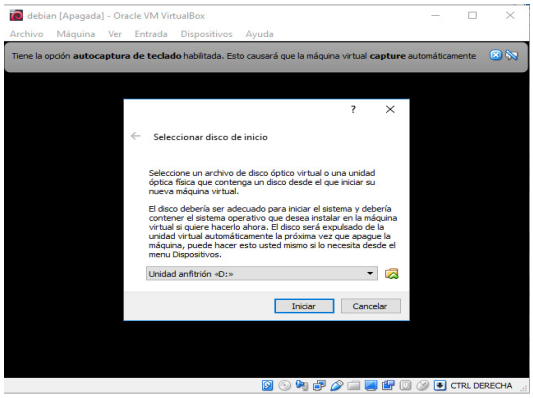


Figura 349: Selección de disco de inicio

Para buscar nuestro disco o nuestra iso, hacemos clic en la carpeta.



A continuación, mostrará dónde buscar nuestro sistema operativo.

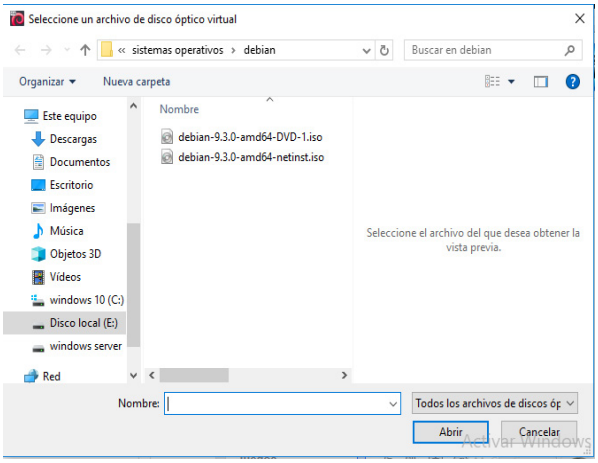


Figura 350: Selección de disco óptico virtual.

La ISO señalada es la que vamos a instalar. Después hacemos clic en abrir.

Paso 7:

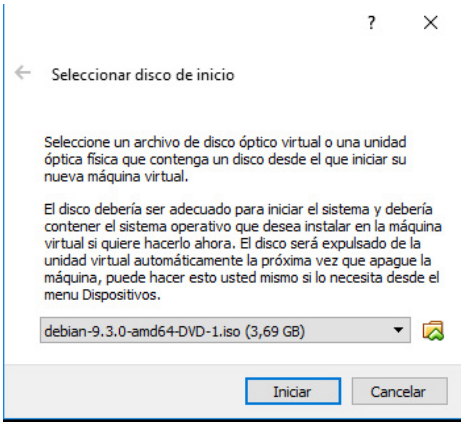


Figura 351: Selección de disco de incio.

Si todo ha salido correctamente, se verá una pantalla como esta: utilice Graphical Install.

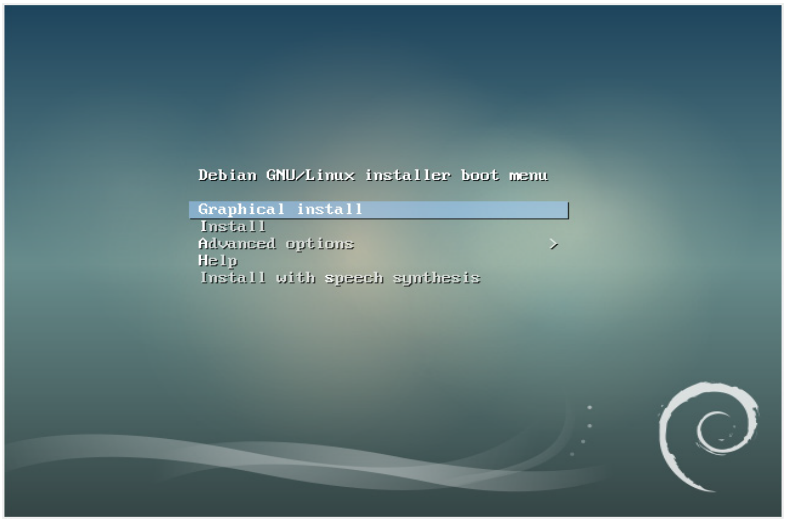


Figura 352: Menú de instalación.

Paso 8: Seleccionar el idioma y la ubicación geográfica con la que se mostrará nuestro S.O Debian.

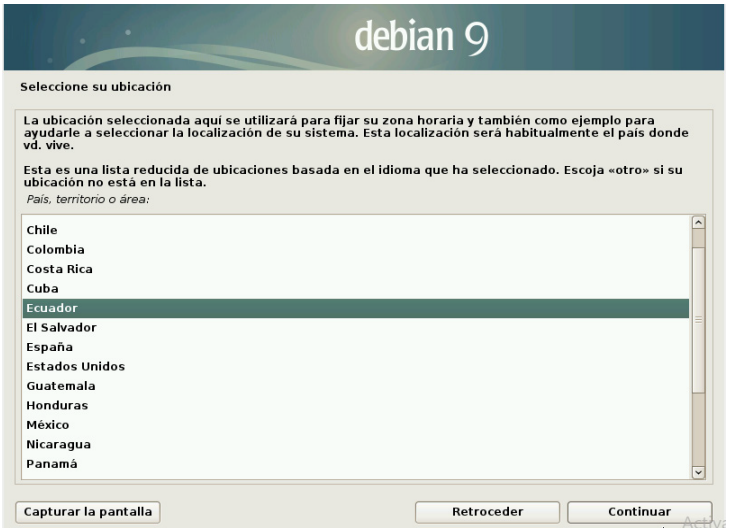


Figura 353: Selección de ubicación e idioma.

Paso 9: Indicar qué tipo de teclado se usará.



Figura 354: Selección del tipo de teclado.

Esperamos a la carga de los componentes y la configuración automática de red.



Figura 355: Configuración automática de red.

Paso 10: Indicar un nombre para la red (hostname).

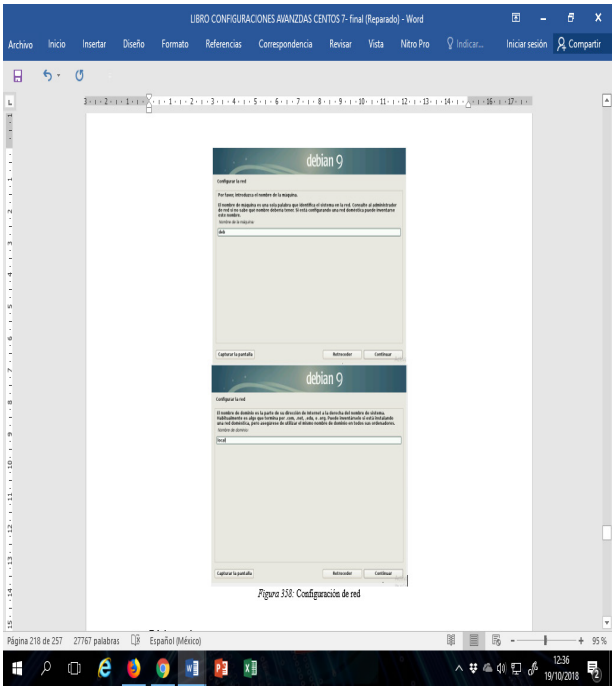


Figura 358: Configuración de red

Figura 356: Configuración de red.

Paso 11: Crear contraseña para el root.

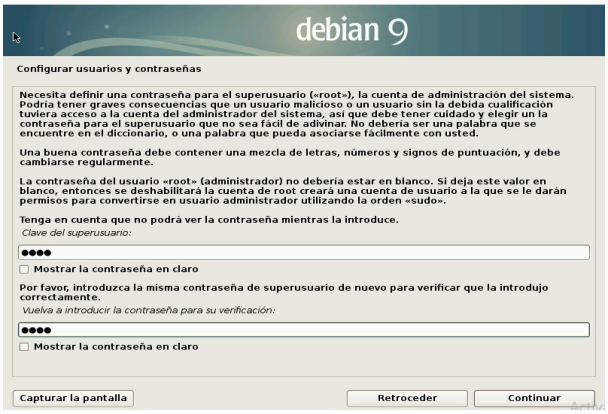


Figura 357: Configuración de root.

Paso 12: Crear un nombre de usuario y su contraseña.

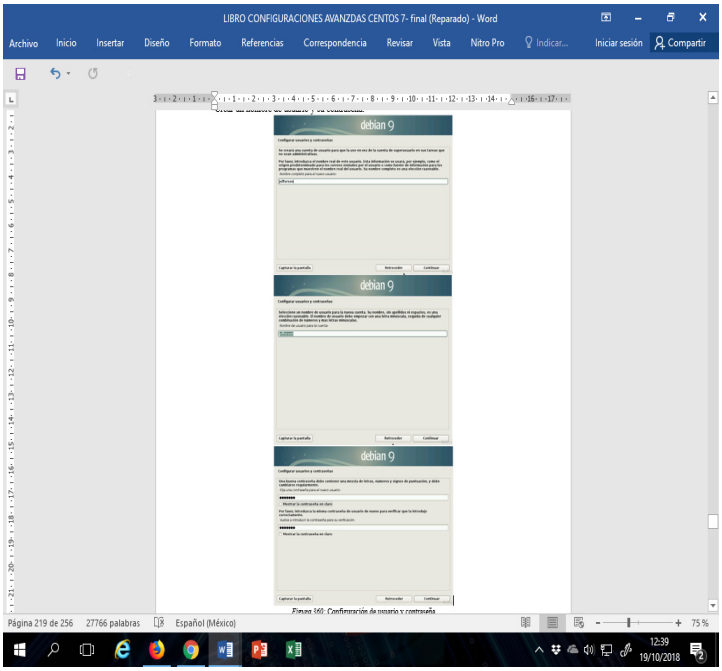


Figura 358: Configuración de usuario y contraseña.

Paso 13: Configurar el reloj.

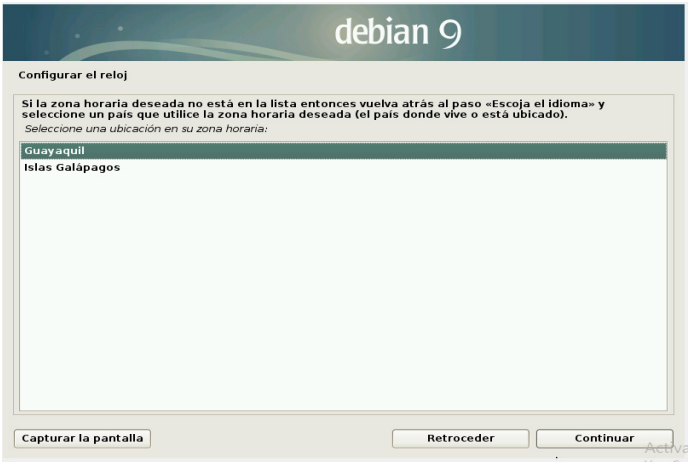


Figura 359:Configuración del reloj.

Paso 14: Vamos a crear las particiones de los discos, y para ello le hacemos en la opción manual.

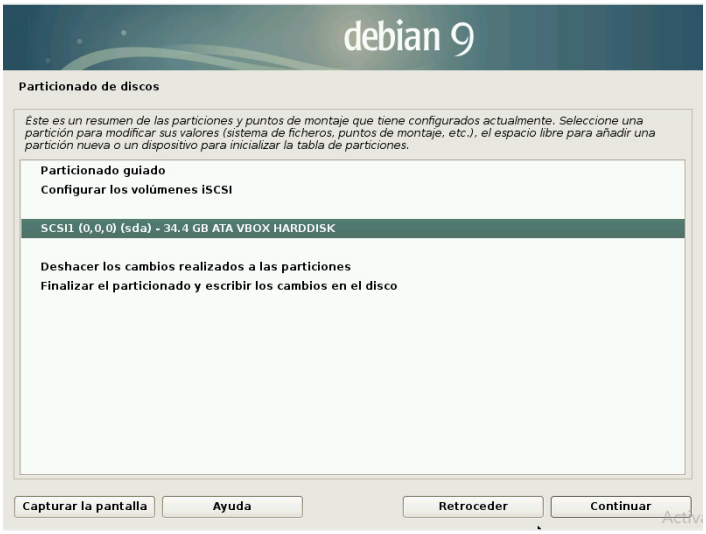


Figura 360: Partición de discos.



Figura 361: Crear nueva tabla de partición.

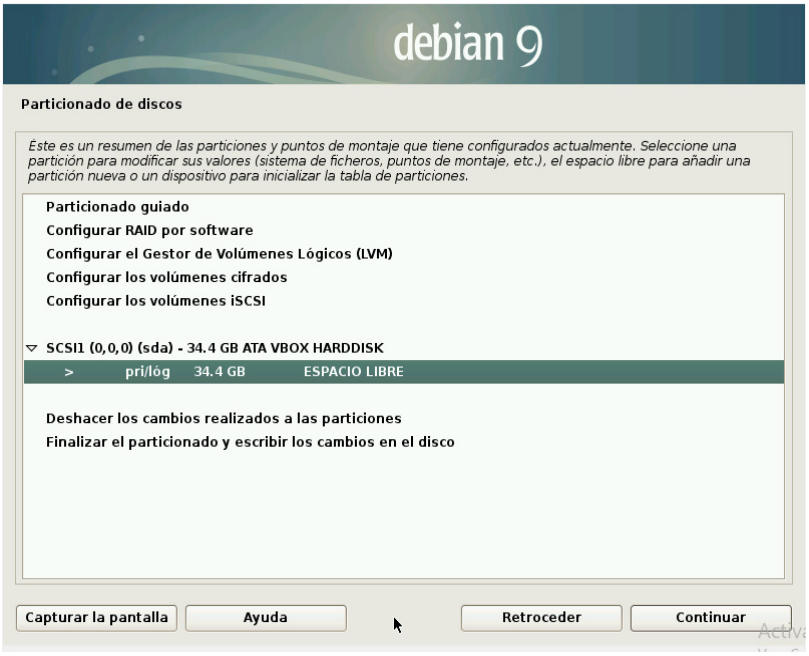


Figura 362: Particionado guiado.



Figura 363: Crear una partición nueva.

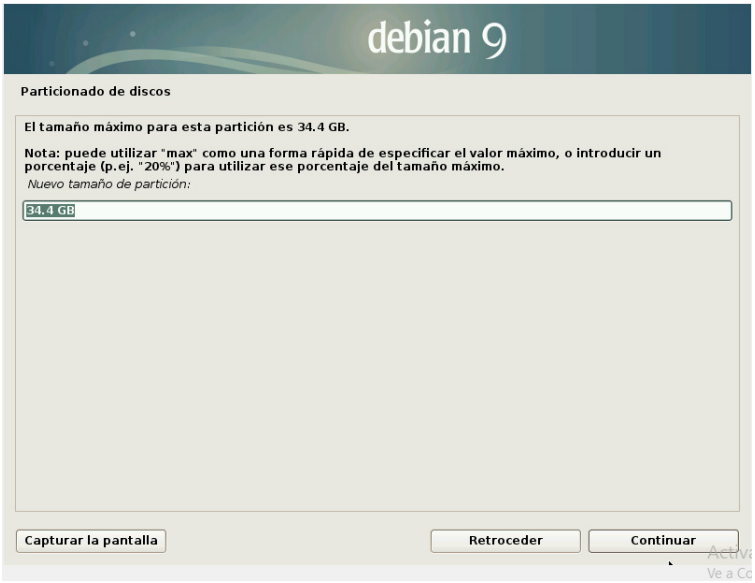


Figura 364: Tamaño de la nueva partición.

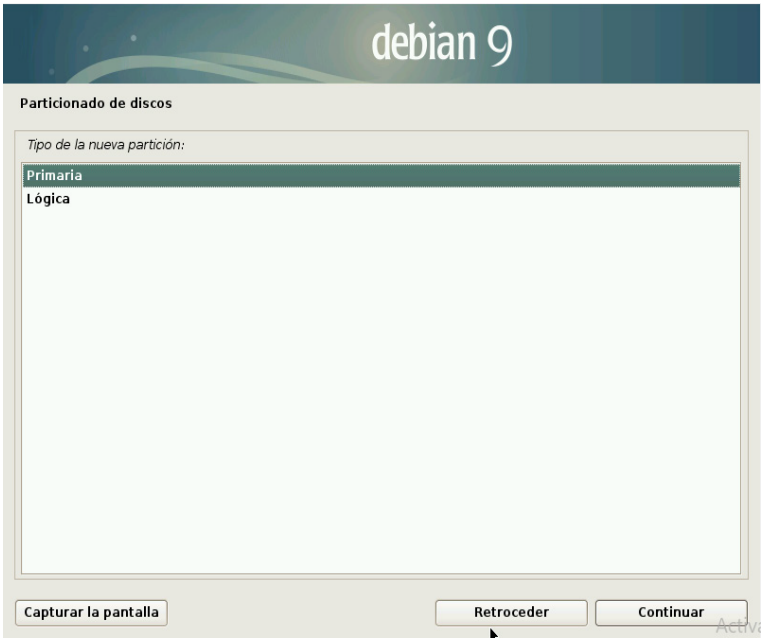


Figura 365: Tipo de nueva partición.

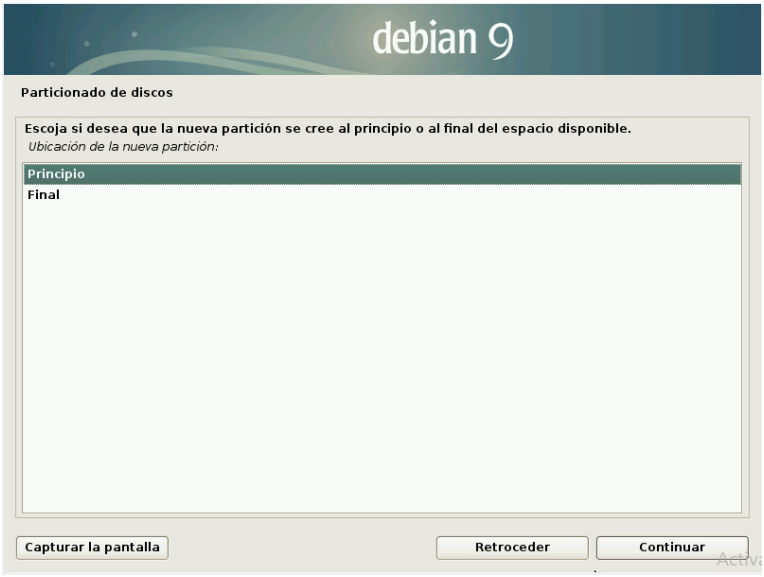


Figura 366: Orden de la nueva partición.



Figura 367: Definición de partición.



Figura 368: Partición creada.

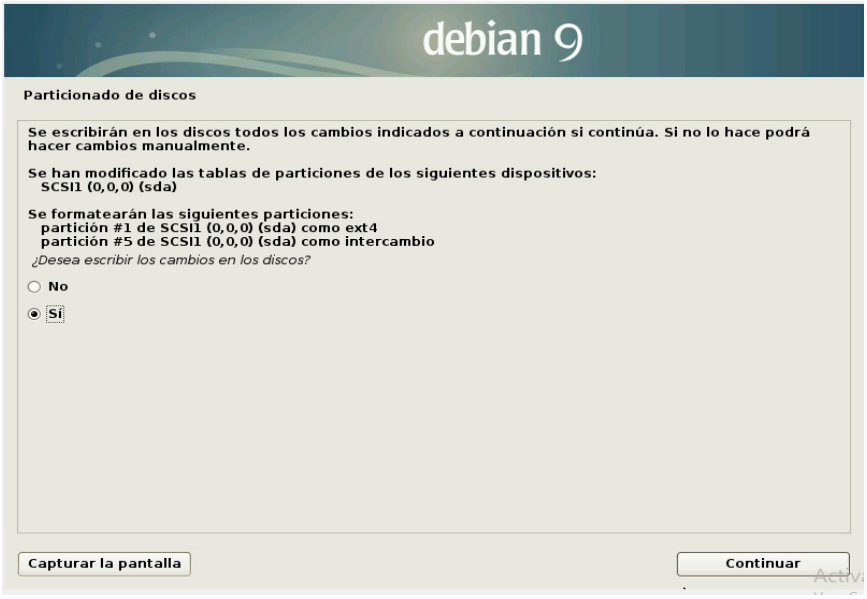


Figura 369: Creación de particiones de disco duro.

Paso 15:



Figura 370: Instalación del sistema base.



Figura 371: Configuración del gestor de paquetes.

Paso 16: Seleccione de los paquetes que deseas instalar en Debian: utilice GNOME. El escritorio GNOME es un entorno de escritorio atractivo y útil. GNOME es libre y es uno de los entornos de escritorio más utilizados en el sistema operativo GNU/Linux.

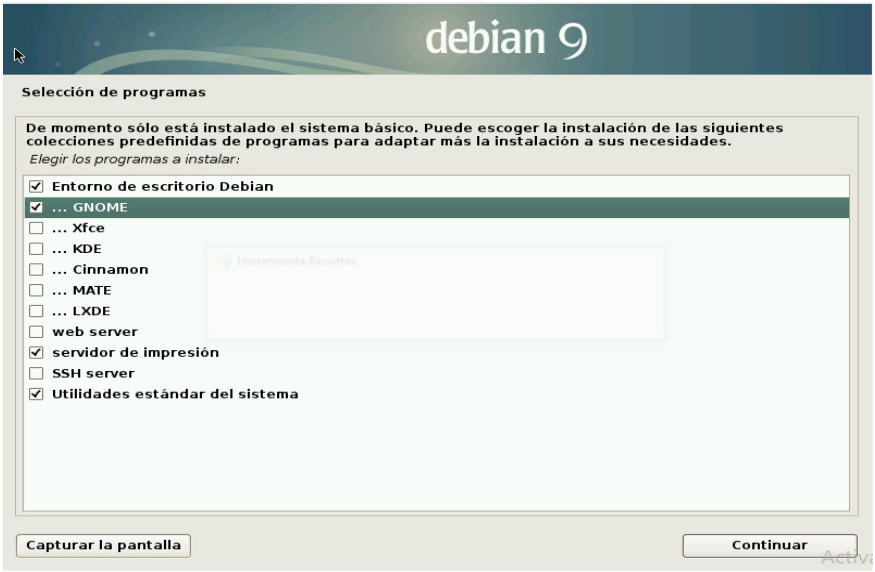


Figura 372: Selección de los programas a instalar.

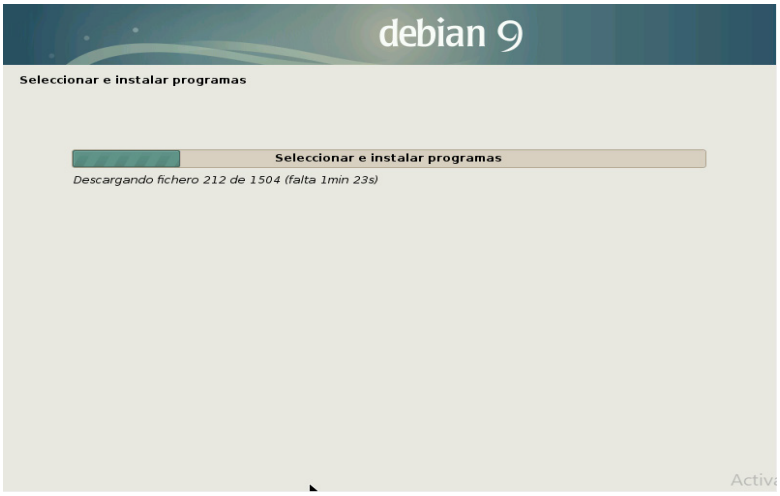


Figura 373: Elección de paquetes a instalar.

Paso 17: Instalar el cargador de arranque GRUB. La magia de poder instalar varios sistemas operativos en un mismo equipo se debe a los gestores de arranque múltiple.

¿Qué es un gestor de arranque? Es el primer software que se ejecuta en el ordenador luego del BIOS. Su misión es cargar el kernel de un sistema operativo y pasarle el control de ejecución para que continúe con el resto del proceso de inicialización. Los gestores de arranque que permiten iniciar más de un sistema operativo se denominan gestores de arranque múltiple.

Dicho esto, podemos definir a GNU GRUB (o simplemente GRUB) como un gestor de arranque múltiple muy poderoso que permite cargar una amplia variedad de sistemas operativos, tanto libres como propietarios.



Figura 374: Instalación del cargador de arranque GRUB en disco duro.



Figura 375: Instalación del cargador de arranque GRUB en disco duro.



Figura 376: Instalador del cargador de arranque.

Cuando se muestre esta pantalla se afirma que ya está instalado el sistema operativo Debian.

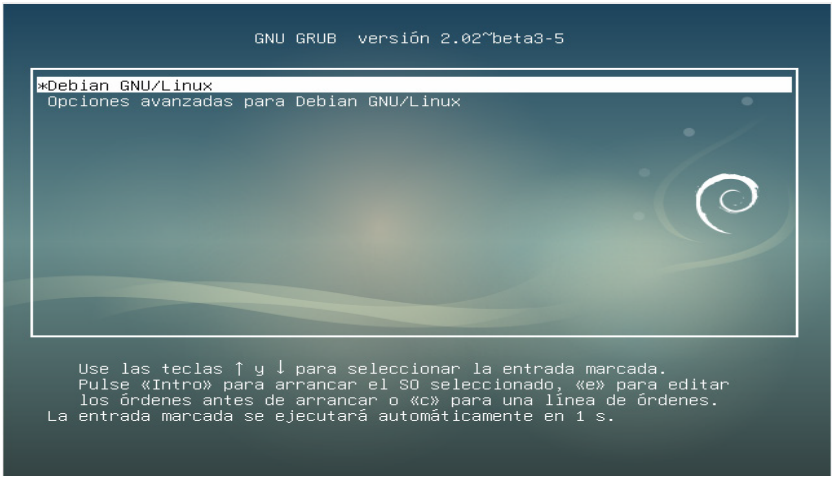


Figura 377: Debian instalado.

Terminado este proceso, se reiniciará automáticamente la máquina y ya estará correctamente instalado el sistema operativo.

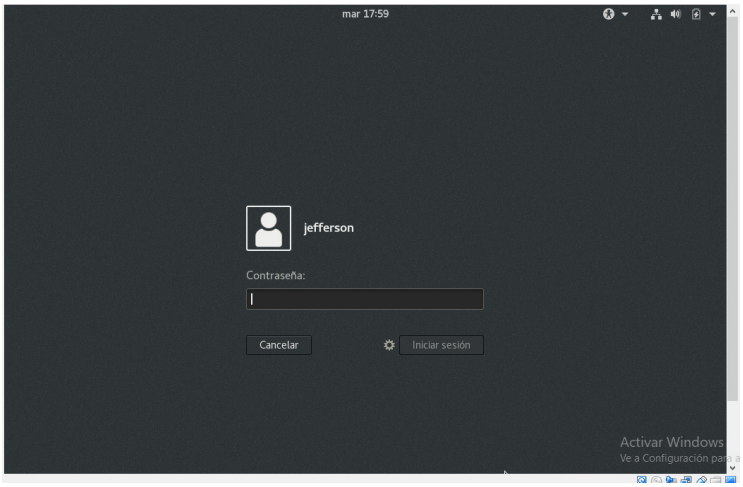


Figura 378: Ingreso de contraseña.

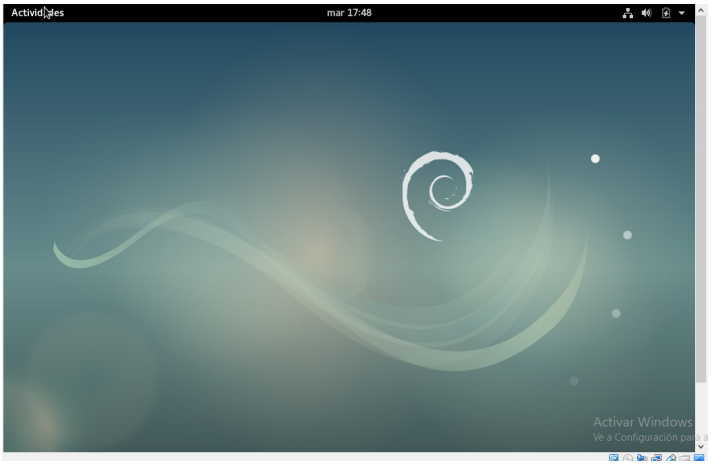


Figura 379: Página principal.

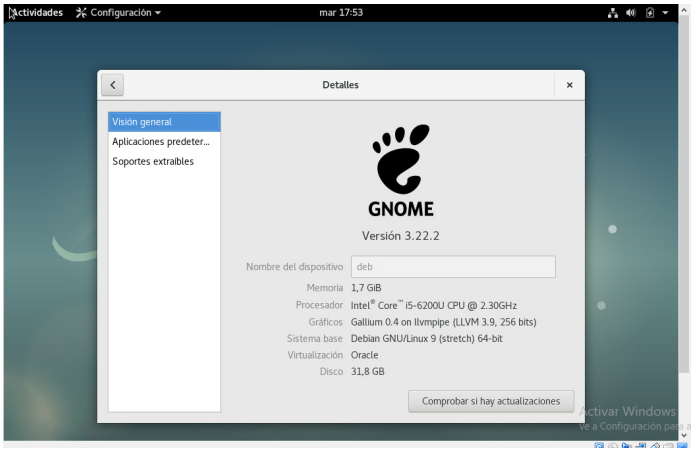


Figura 380: Ventana Principal de Gnome

Instalación y configuración de openvpn de host a red desde un cliente FEDORA

Una red privada virtual (VPN por sus siglas en inglés de Virtual Private Network) es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada. Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa, permitir a los miembros del equipo de soporte técnico la

conexión desde su casa al centro de cómputo, entre otros. Todo ello utilizando la infraestructura de red interna en la virtualización de máquinas.

Al construir una VPN, lo que se desea es tener la posibilidad de acceder a una red local (protegida detrás de un Firewall/Gateway) desde Internet (o desde cualquier otra red insegura). El objetivo es que un cliente ubicado físicamente fuera de la red local (y posiblemente a kilómetros de distancia) parezca conectado de forma local. El servidor de VPN es el que posibilita la "extensión" y es quien provee una conexión segura entre el cliente y la red local, al utilizar certificados se obtiene autenticación mutua y confidencialidad.

Pasos para la instalación de OpenVpn de host a red con un cliente Fedora

Paso 1:

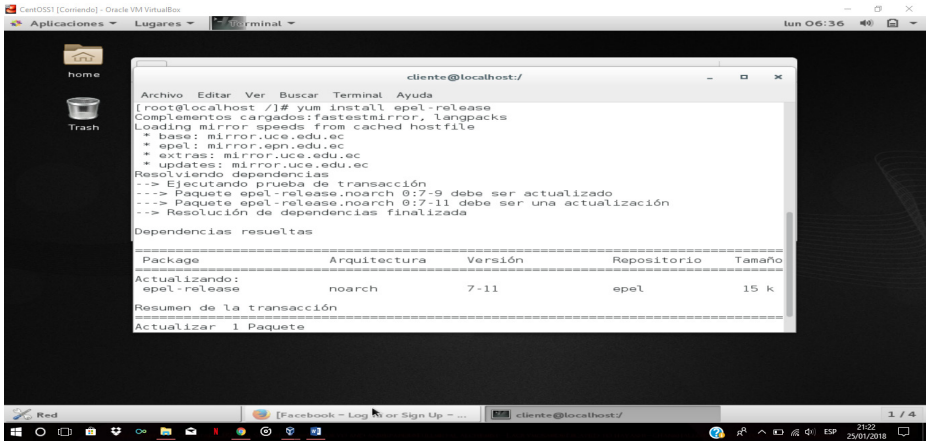


Figura 381: Instalar Epel-release en el servidor Centos 7.0

Paso 2: Instalar OpenVPN en el servidor Centos 7.0

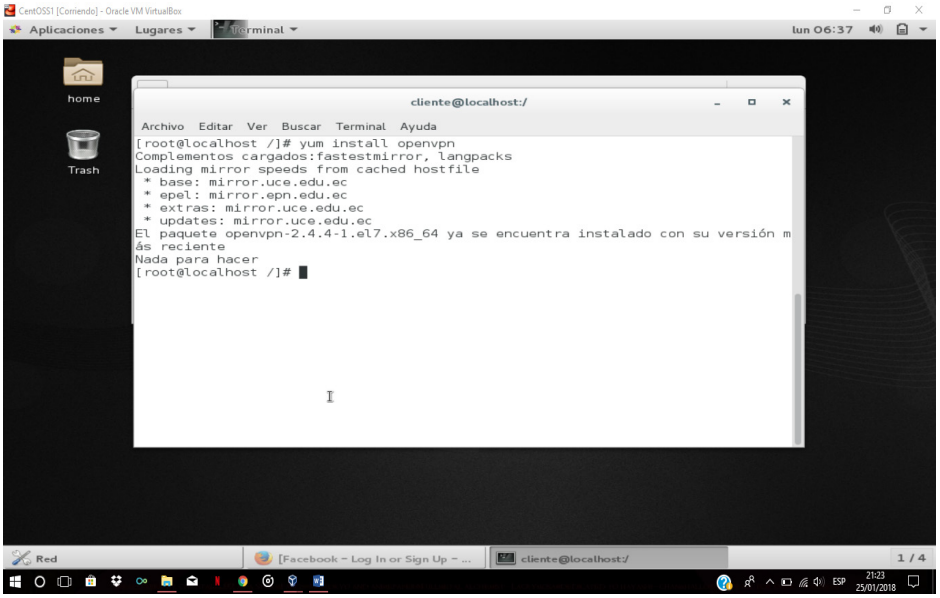


Figura 382: Ingreso del comando yum install OpenVpn

Paso 3: Copiar los archivos de Easy-rsa desde el directorio usando el comando cp -r /usr/share/easy-rsa al directorio /etc/openvpn (el comando cp se utiliza para copiar archivos de un directorio a otro).

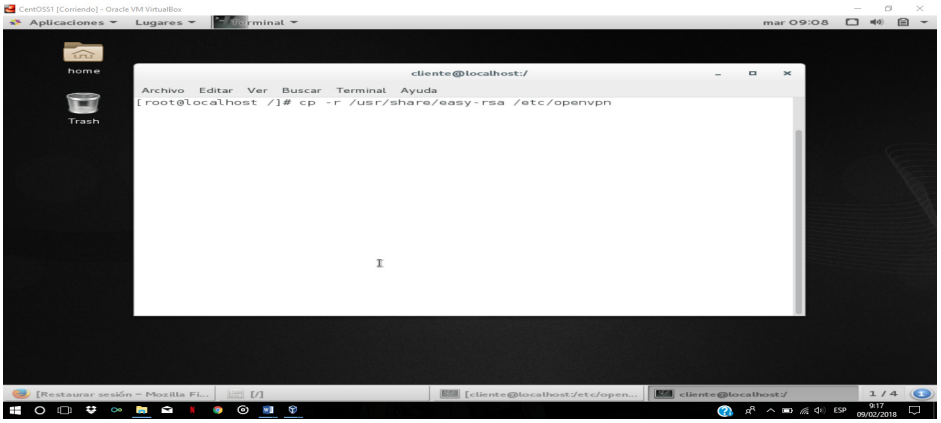


Figura 383: Copiar los archivos de Easy-rsa

Paso 4: Generar los certificados para el cliente Fedora que en este caso es el cliente número 2, antes de eso ingresamos el siguiente comando cd /etc/openvpn/easy-rsa/2.0/.vars

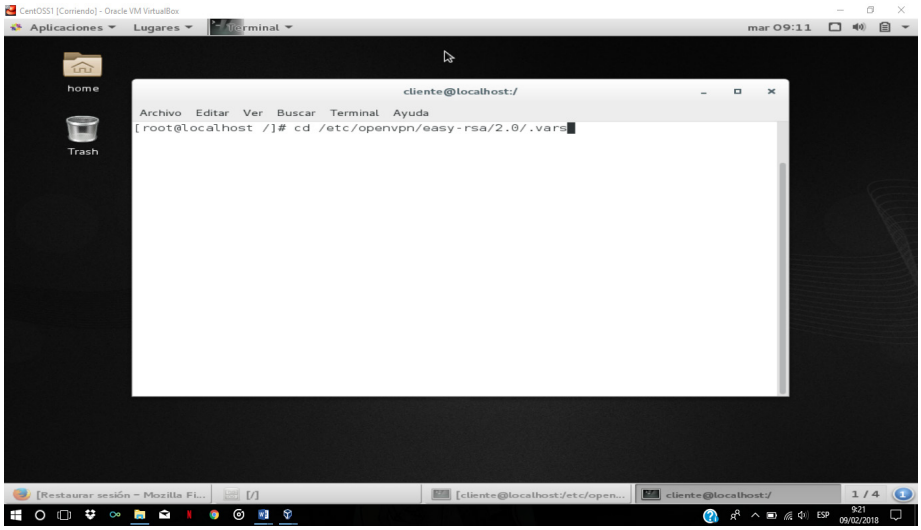


Figura 384: Generación de certificados

Paso 5: Limpiar la configuración de los certificados con el siguiente comando: sh clean-all

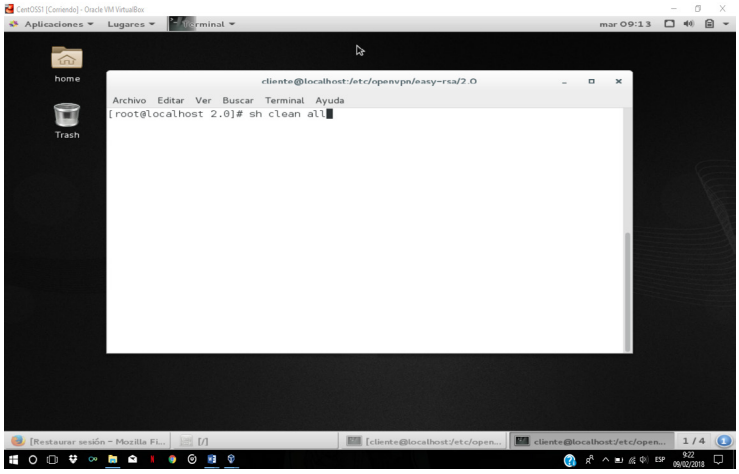


Figura 385: Comando para limpiar la configuración de certificados

Paso 6: Crear una carpeta en la cual se guardarán los certificados dentro del directorio /etc/openvpn/easy-rsa/2.0 con el comando mkdir -p keys.

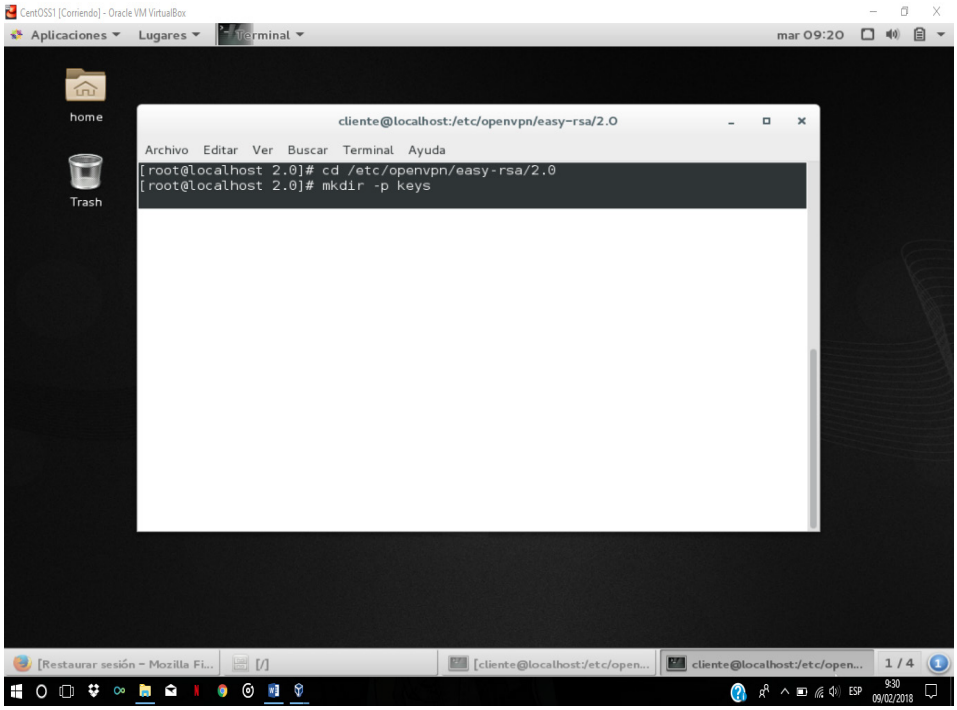


Figura 386: Directorio en el que se guaran los certificados

Paso 7: Generar los certificados ca.crt server.key build-dh y client2. key con los siguientes comandos:

- sh build-ca (Autoridad de Certificación que se utilizará para firmar los certificados de los clientes y el servidor)
- sh build-key-server server (certificado para el servidor)
- sh build-dh (genera los parámetros Diffie Hellman)
- sh build-key client2 (genera los certificados para el equipo cliente)

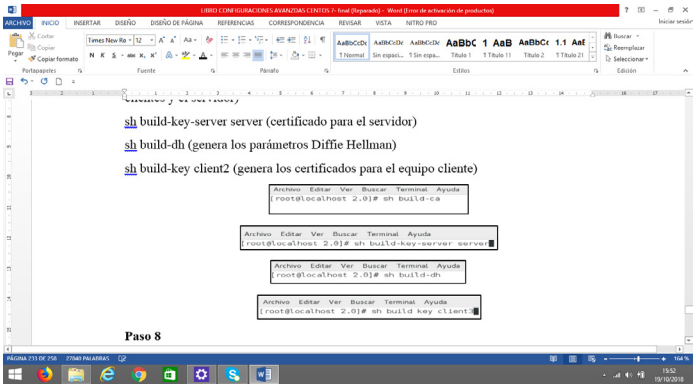


Figura 387: certificados ca.crt server.key build-dh y client2.key

Paso 8: Ingresar al directorio /etc/openvpn/easy-rsa/2.0 y luego escribir el comando ls para comprobar que los certificados se hayan generado correctamente.

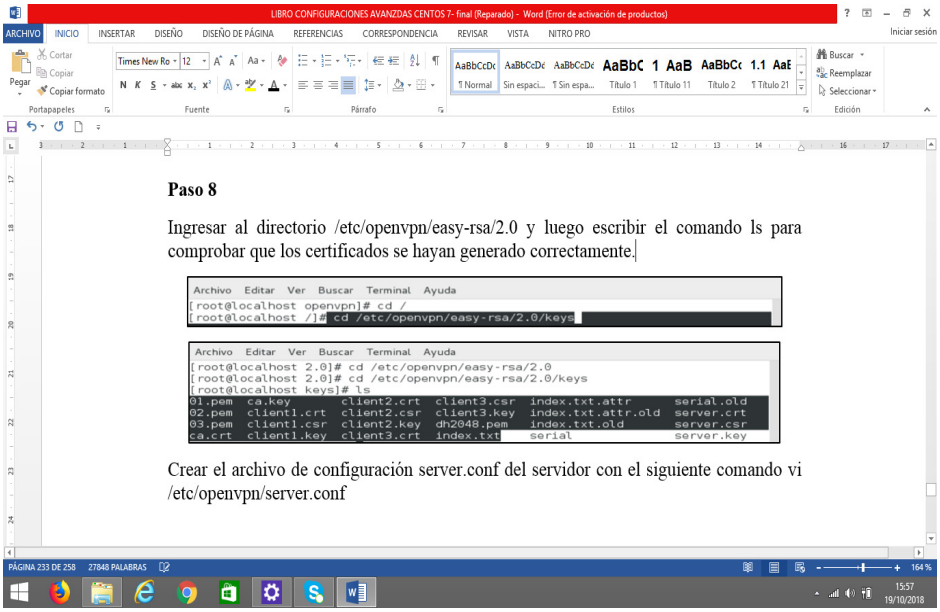


Figura 388: /etc/openvpn/easy-rsa/2.0

Crear el archivo de configuración server.conf del servidor con el siguiente comando vi /etc/openvpn/server.conf

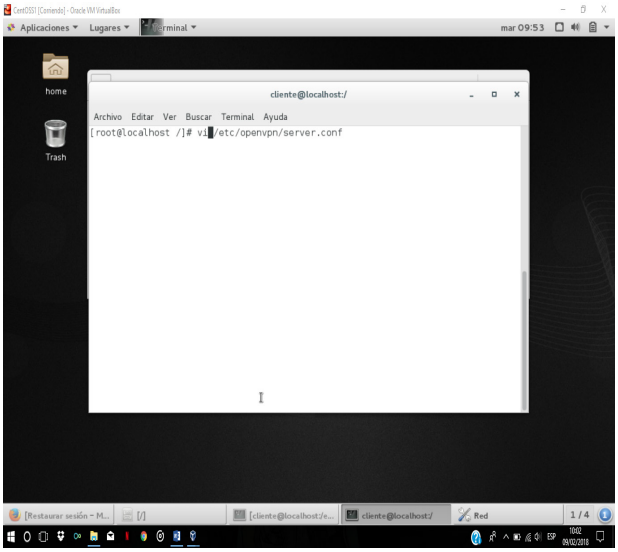


Figura 389: /etc/openvpn/server.conf

Paso 9: Este archivo contiene la dirección IP virtual 10.8.0.0 con la máscara de red 255.255.255.0 también contiene al ámbito de red 192.168.0.0 hacia la cual el servidor va a redireccionar la IP del cliente Fedora mediante el uso de la IP virtual además de los certificados generados anteriormente.

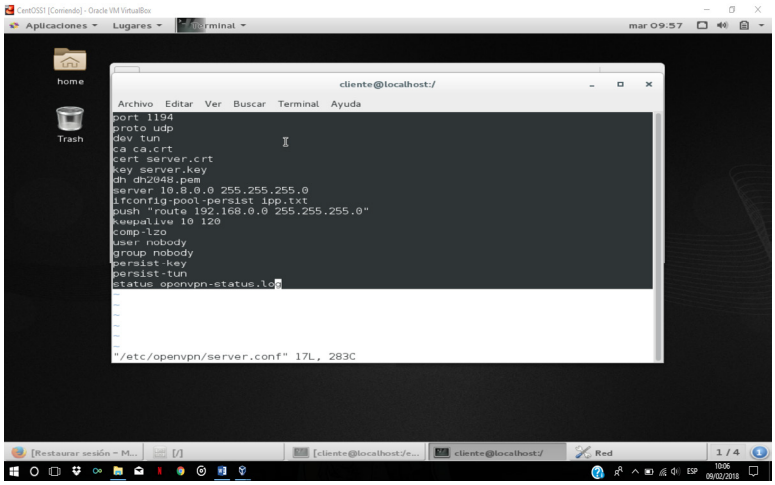


Figura 390: Configuración del diccionamiento IP

Paso 10: Generar un archivo comprimido .tar el cual contendrá los certificados ca.crt client2.crt y client2.key del cliente2 con el comando tar zcf /root/client2.tar.gz ca.crt client2.crt client2.key

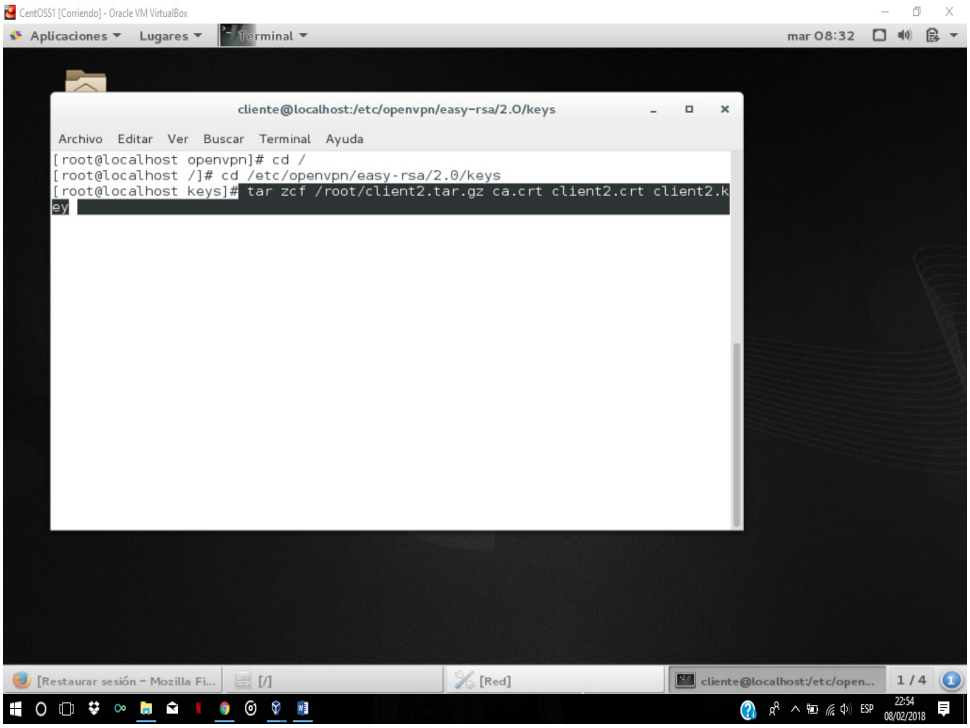


Figura 391: Generación de un archive comprimido .tar

Paso 11: Comprobar la creación del archivo .tar mediante el comando ls en el directorio root.



Figura 392: Verifiación del archivo creado .tar

Paso 12: Verificar la IP del servidor que será utilizada para transferir los archivos hacia el cliente, ingresando a la opción configuración de red que se encuentra en la esquina superior derecha de la pantalla.

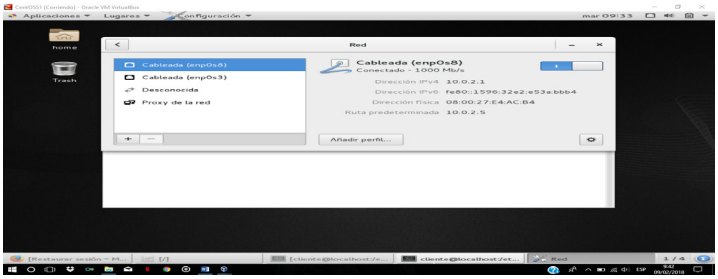


Figura 393: Veerificación de IPdel servidor.

Paso 13: Ingresar al cliente Fedora y en el terminal ingresar el siguiente comando scp root@10.0.2.1:client2.tar.gz el cual contiene la IP del servidor y el nombre del archivo .tar generado anteriormente.

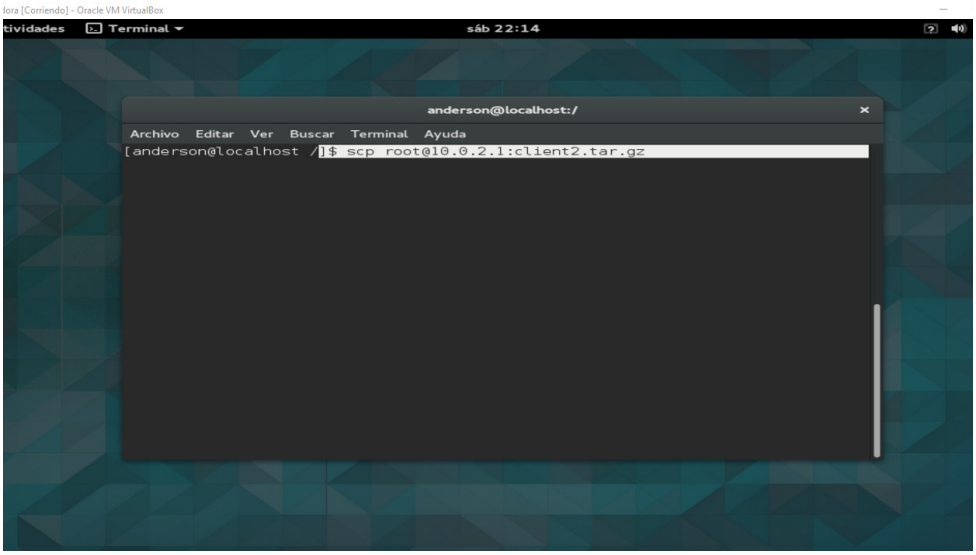


Figura 394: scp root@10.0.2.1:client2.tar.gz

Paso 14: Dentro del cliente Fedora crear un directorio en el cual se descomprimirán los archivos transferidos mediante el comando mkdir Fedora.

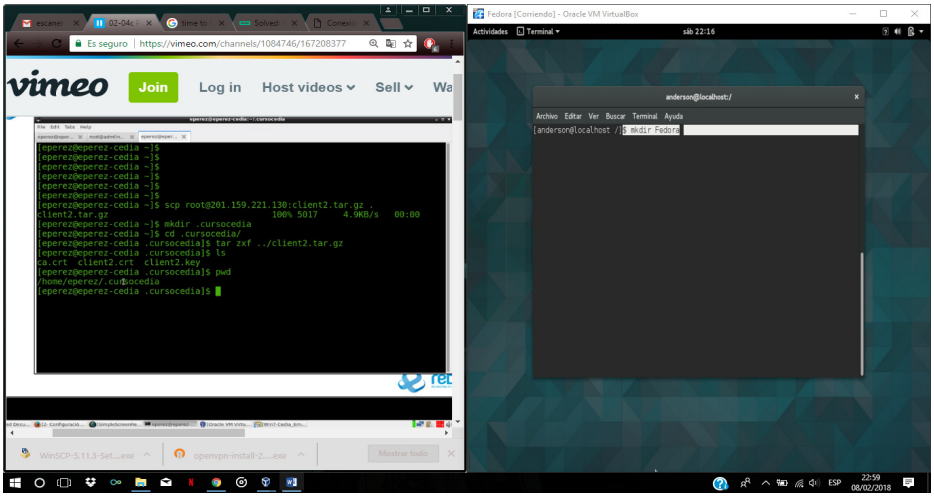


Figura 395: Creación de directorio Fedora.

Paso 15: Escribir el siguiente comando en el terminal para descomprimir el archivo .tar en el directorio creado en el paso anterior tar zxf ../client2.gz

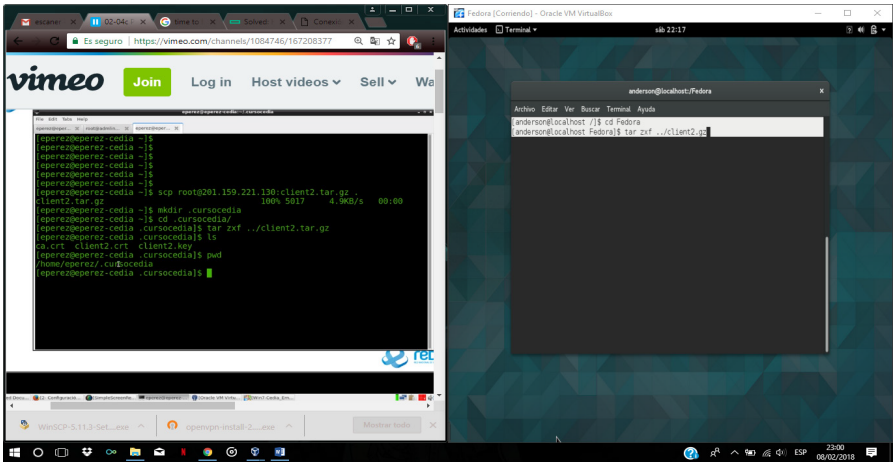


Figura 396: Descomprimir archivo .tar

Paso 16: Comprobar que los archivos se hayan descomprimido mediante el comando ls dentro del directorio Fedora, es decir, ingresamos al directorio Fedora mediante el comando cd Fedora y luego ingresar el comando ls.

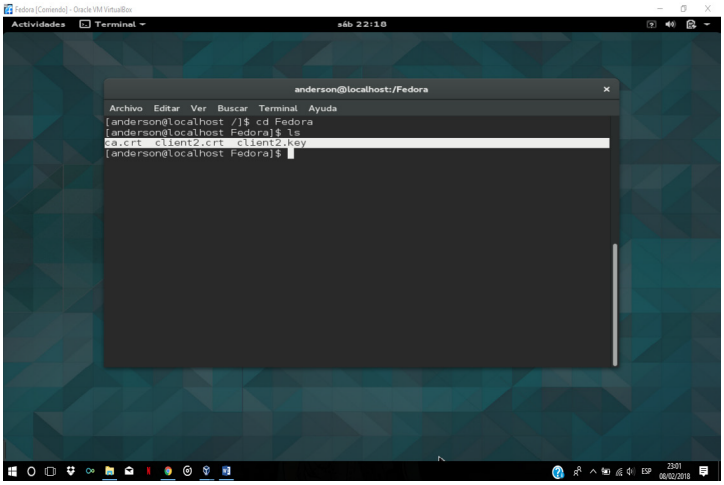


Figura 397: Aplicación del comando ls al directorio Fedora.

Paso 17: En el cliente Fedora comprobamos que estén instaladas las dependencias de OpenVpn mediante el comando rpm -qalegrep NetworkManager

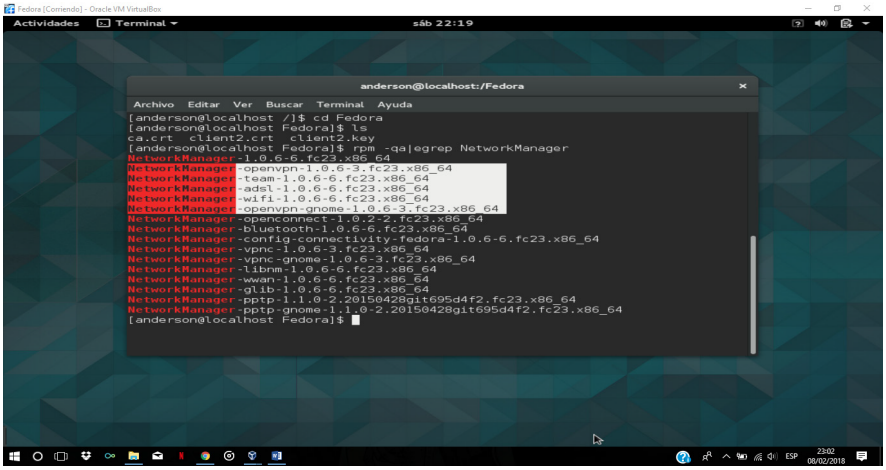


Figura 398: Comando rpm -qalegrep NetworkManager

Paso 18: Abrir la configuración de red en el cliente Fedora y dar clic en el símbolo + y añadir conexión de red VPN.

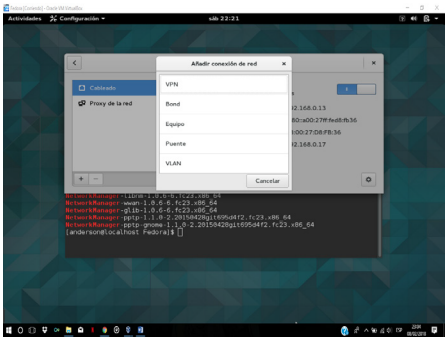


Figura 399: Añadir conexión de red.

Paso 19: En la opción conexión de red elegir la opción OpenVpn

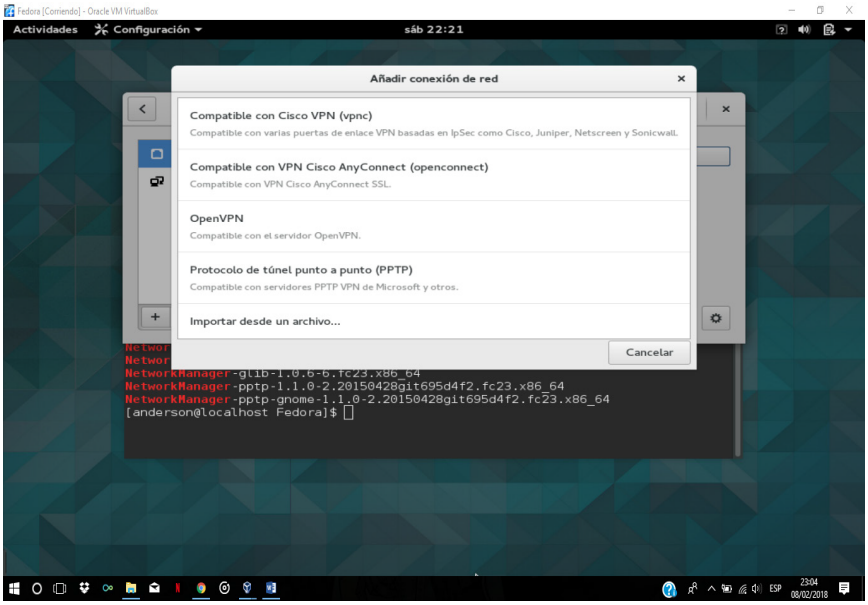


Figura 400: Añadir conexión de red.

Paso 20: Colocar un nombre a la conexión, en pasarela colocar la dirección IP del servidor en este caso es la 10.0.2.1 y en la autentificación en el tipo colocar certificados TLS.

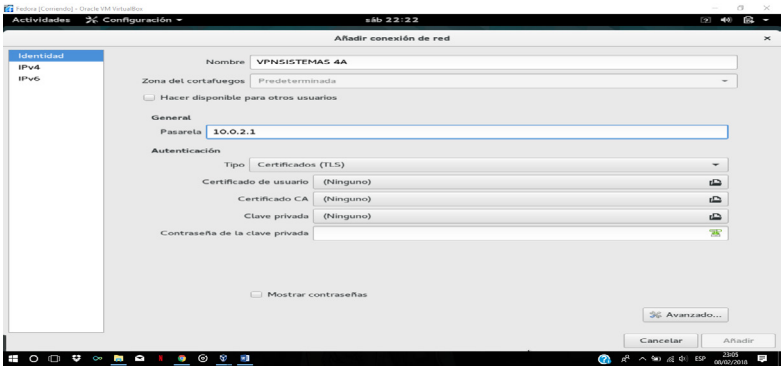


Figura 401: Añadir conexión de red.

Paso 21: El siguiente paso es colocar los certificados que fueron transferidos desde el servidor al cliente en el siguiente orden:

- Certificado de usuario: client2.crt
- Certificado CA: ca.crt
- Clave privada: client2.key

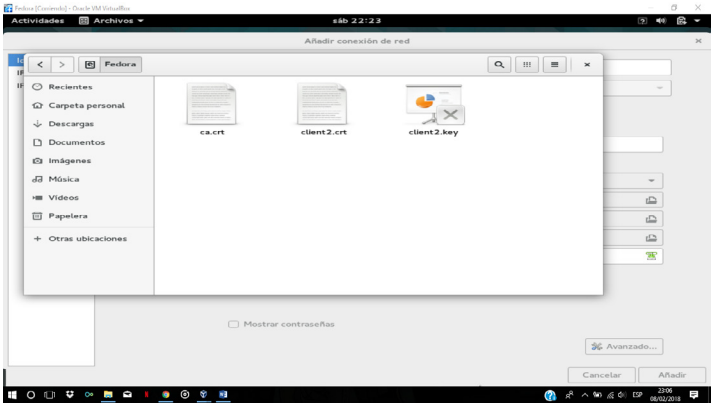


Figura 402: Certificadoss transferidos desde el servidor hacia el cliente.

Al final colocado los certificados respectivos nos debe quedar así:

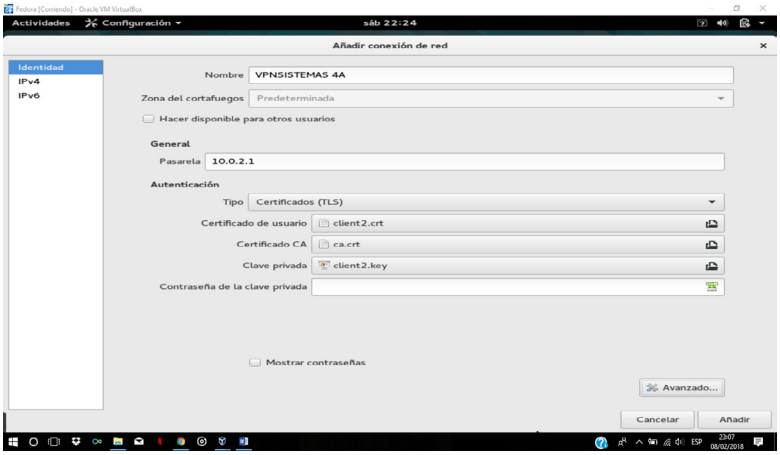


Figura 403: Certificados colocados.

Paso 22: Ir al menú de opciones avanzadas y en la pestaña "General" escoger la opción "Usar compresión LZO" y luego en "Aceptar".

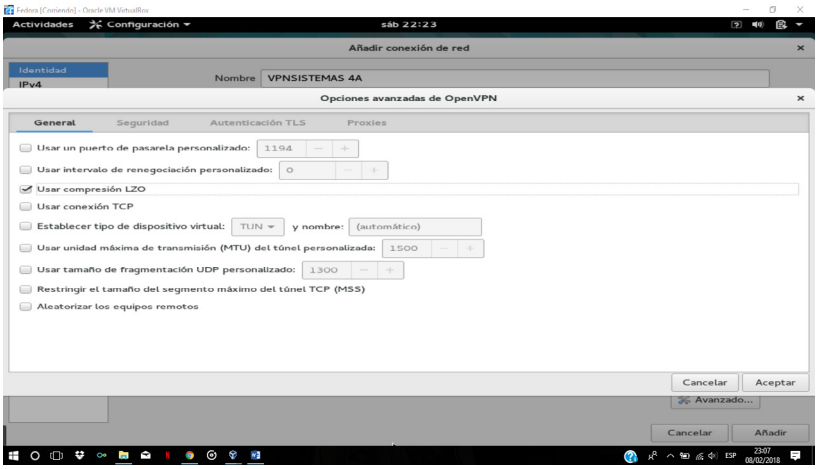


Figura 404: Opciones Avanzadas de VPN

Paso 23: En la opción IPV4 colocar una IP estática al equipo Fedora en este caso 10.0.2.5 una máscara de red 255.255.255.0 y en la puerta de enlace colocar la IP del servidor en este caso 10.0.2.1

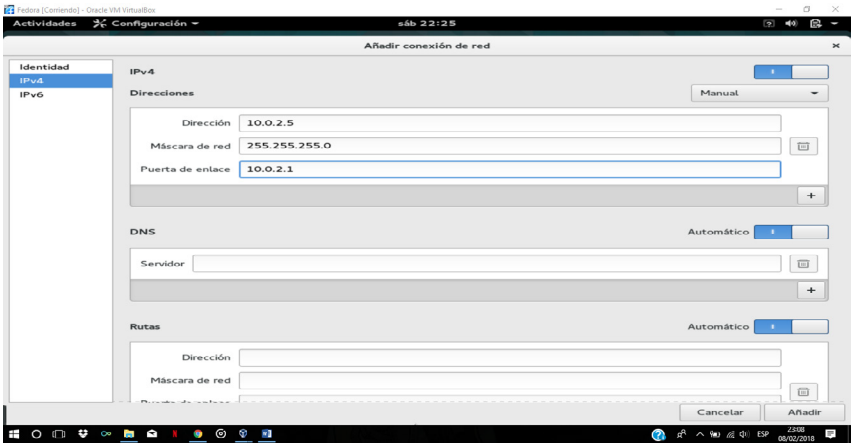


Figura 405: Añadir conexión de red.

Paso 24: En la parte posterior donde se ubican rutas, elegir la opción usar esta conexión solo para recursos en la red y finalmente hacemos clic en "Añadir".

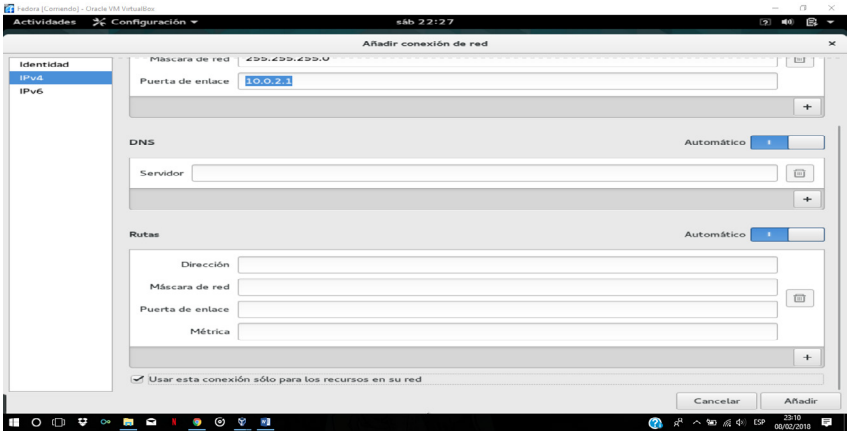


Figura 406: Ventana de rutas.

Paso 25: Al final nos mostrará una conexión parecida a esta y se procede a encender la conexión:

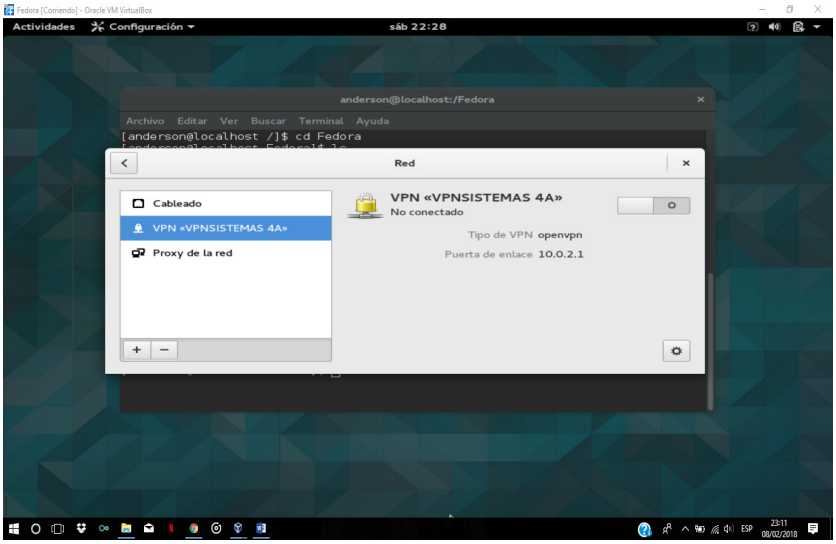


Figura 407: Ventana de red.

Paso 26: En el servidor configuramos los dos adaptadores de red, primero vamos a configurar el adaptador de red que va hacia el cliente Fedora colocando en la ruta predeterminada la IP del cliente Fedora (10.02.5).

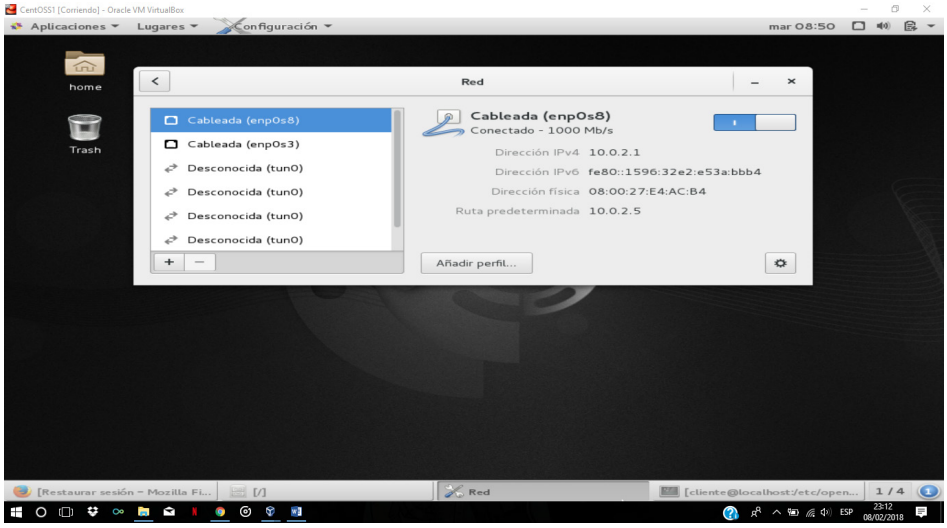


Figura 408: Configuración de adaptadores de red.

Configurar el otro adaptador que va hacia el cliente conectado en red LAN con el servidor el cual posee una IP 192.168.0.13, la cual será colocada en la ruta predeterminada del segundo adaptador de red.

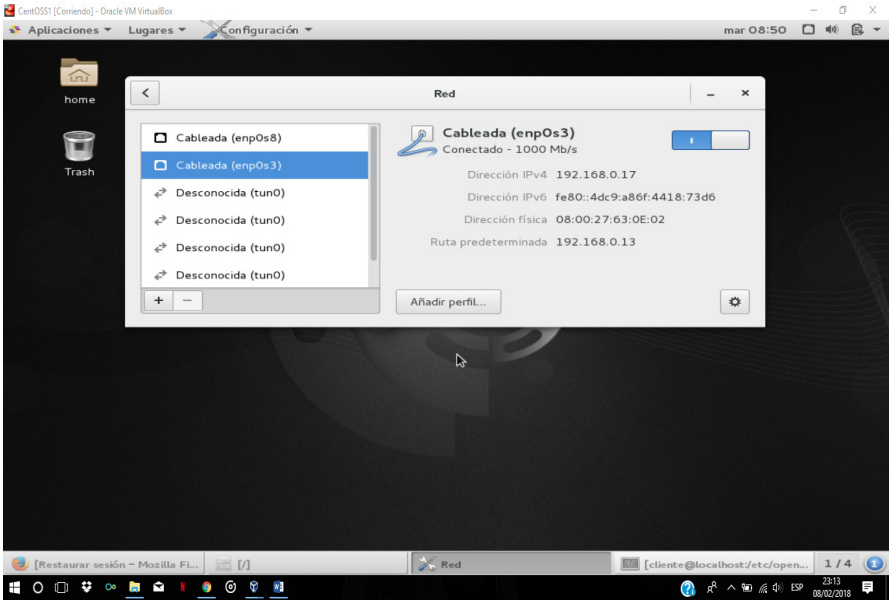


Figura 409: Configución de adaptador que va hacia el cliente conectado en red LAN

Paso 27: Desde el cliente conectado en red LAN con el servidor comprobar que la IP esté colocada correctamente y en la ruta predeterminada colocar la IP del servidor del segundo adaptador de red (192.168.0.17).

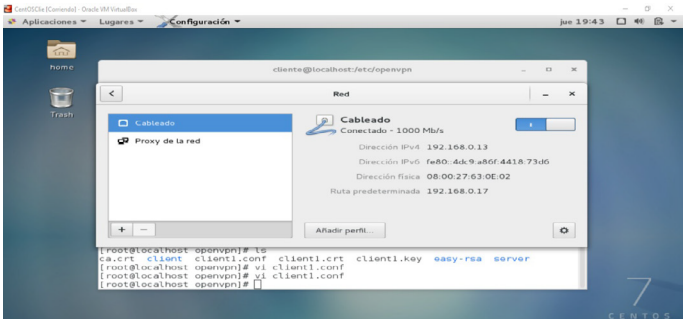


Figura 410: Comprobación de IP.

Paso 28: Por último, comprobar que la VPN esté funcionando haciendo ping desde el cliente Fedora hacia el cliente conectado en red LAN con el servidor es decir hacia la IP 192.168.0.13

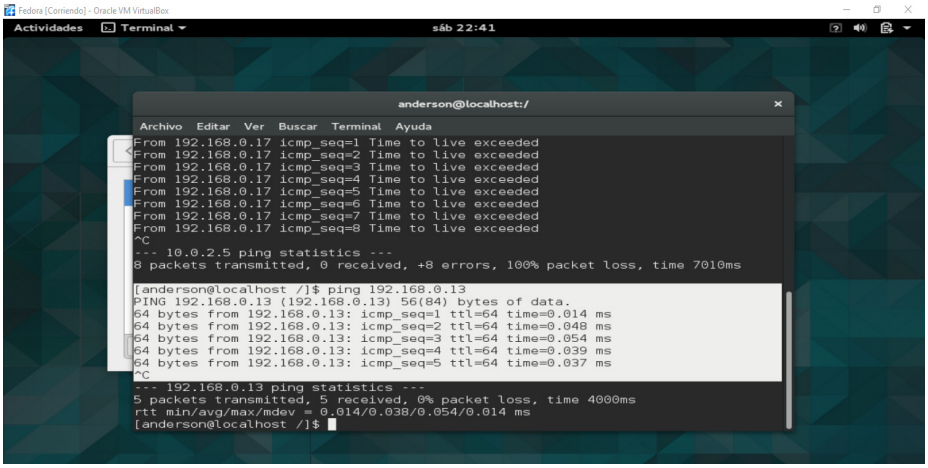


Figura 411: Verificación con el comando ping desde cliente Fedora a cliente en red LAN.

Paso 29: Desde el cliente conectado en LAN también comprobar que haga ping hacia la IP del cliente Fedora es decir a la 10.0.2.5

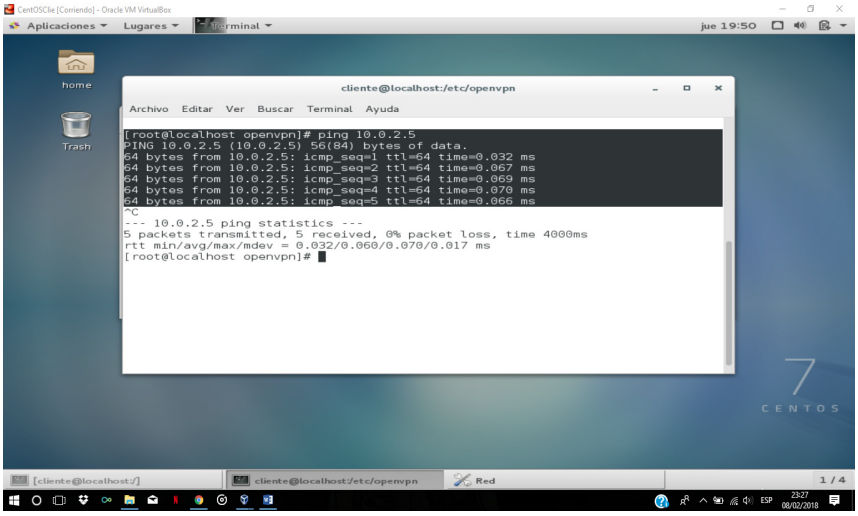


Figura 412: Ping desde cliente en red LAN cliente Fedora.

Si entre las dos máquinas funciona correctamente la conexión, la práctica se llevó a cabo con éxito.

TÉRMINOS TÉCNICOS

XFS Gómez, R. (2010). XFS (a partir de la v22), es un sistema de archivos de diario robusto y de alta escalabilidad de 64 bits. Este sistema se basa totalmente en la extensión, por lo tanto, soporta grandes archivos y sistemas de archivos muy grandes. El número de archivos que pueden contener un sistema XFS está limitado únicamente por el espacio disponible en el sistema de archivos (p. 14)

Fedora Workstation es un sistema operativo pulido y fácil de usar, para ordenadores portátiles y de sobremesa, con un conjunto completo de herramientas para desarrolladores y creadores de todo tipo.

Ficheros .tar empaqueta varios archivos en uno solo, pero no comprime.

LZO es una librería de compresión de datos, la cual es muy apropiada para compresión.

Comandos de centos7.0

Información del sistema

1. arch → mostrar la arquitectura de la máquina (1).
2. uname -m → mostrar la arquitectura de la máquina (2).
3. uname -r → mostrar la versión del kernel usado.
4. uname -a → mostrar la información completa.
5. lsb_release -a → mostrar la información completa de la distribución.
6. cat /etc/issue → mostrar el nombre de la distribución

7. dmidecode -q → mostrar los componentes (hardware) del sistema.
8. hdparm -i /dev/hda → mostrar las características de un disco duro.
9. hdparm -tT /dev/sda → realizar prueba de lectura en un disco duro.
10. cat /proc/cpuinfo → mostrar información de la CPU.
11. grep -c ^processor /proc/cpuinfo → mostrar número de procesadores.
12. cat /proc/interrupts → mostrar las interrupciones.
13. cat /proc/meminfo → verificar el uso de memoria.
14. cat /proc/swaps → Mostar ficheros swap.
15. cat /proc/version → mostrar la versión del kernel.
16. cat /proc/net/dev → mostrar adaptadores de red y estadísticas.
17. cat /proc/mounts → mostrar el sistema de ficheros montado.
18. lscpu → mostrar información sobre el microprocesador.
19. lspci -tv → mostrar los dispositivos PCI.
20. lsusb -tv → mostrar los dispositivos USB.
21. lshw → listar el hardware.
22. discover → listar el hardware.
23. date → mostrar la fecha del sistema.
24. cal 2011 → mostrar el almanaque de 2011.
25. cal 07 2011 → mostrar el almanaque para el mes julio de 2011.
26. date 041217002011.00 → colocar (declarar, ajustar) fecha y hora.
27. clock -w → guardar los cambios de fecha en el BIOS.

28. blkid → mostrar información (nombre, etiqueta, UUID, tipo de partición) sobre los dispositivos de bloque (discos rígidos, etc.)

Apagar, reiniciar o cerrar sesión

1. shutdown -h now → apagar el sistema (1).
2. init 0 → apagar el sistema (2).
3. telinit 0 → apagar el sistema (3).
4. halt → apagar el sistema (4).
5. poweroff → apagar sistema (5).
6. shutdown -h hours: minutes & → apagado planificado del sistema.
7. shutdown -c → cancelar un apagado planificado del sistema.
8. shutdown -r now → reiniciar (1).
9. reboot → reiniciar (2).
10. logout → cerrar sesión.
11. skill nombre_de_usuario → cerrar sesión (2)[1)]
12. exit → salir del intérprete de comandos (si solo hay uno, equivale a cerrar sesión).

Gestionar archivos y directorios

1. cd → ir al directorio personal.
2. cd /home → cambiar al directorio "/home".
3. cd .. → retroceder un nivel.

4. cd ../.. → retroceder 2 niveles.
5. cd ~user1 → ir al directorio user1.
6. cd - → ir (regresar) al directorio anterior.
7. pwd → mostrar el camino del directorio actual.
8. ls → listar el contenido de un directorio.
9. ls -F → listar el contenido de un directorio (distinguiendo los directorios con una barra)
10. ls -l → listar el contenido de un directorio, mostrando los detalles.
11. ls -lh → listar el contenido de un directorio, mostrando los detalles (y el tamaño en un formato "humanizado").
12. ls -a → listar el contenido de un directorio, incluendo los ficheros ocultos.
13. ls *[0-9] → listar los ficheros y carpetas que contienen números.
14. ls -laR | less → listar recursivamente el contenido del directorio actual y todos los subdirectorios y archivos, incluyendo los ocultos, separados por página.
15. tree → mostrar los ficheros y carpetas en forma de árbol comenzando por la raíz.(1)
16. lstree → mostrar los ficheros y carpetas en forma de árbol comenzando por la raíz.(2)
17. mkdir dir1 → crear un directorio de nombre 'dir1'.
18. mkdir dir1 dir2 → crear dos directorios a la vez (en la ubicación actual).
19. mkdir -p /tmp/dir1/dir2 → crear una estructura de directorios, si no existe.
20. rm file1 → eliminar el archivo 'file1'.

21. rm -f file1 → eliminar el archivo 'file1' en modo forzado.
22. rmdir dir1 → borrar el directorio 'dir1'.
23. rm -rf dir1 → eliminar recursivamente y en modo forzado el directorio 'dir1' con todo lo que contenga.
24. rm -rf dir1 dir2 → borrar dos directorios con su contenido de forma recursiva.
25. mv dir1 new_dir → renombrar o mover un fichero o carpeta (directorio).
26. cp file1 destino/ → copiar un fichero al destino elegido.
27. cp file1 file2 destino/ → copiar a la vez dos ficheros a un mismo directorio.
28. cp file1 file2 → copiar file1 en file2.
29. cp dir /* . → copiar todos los ficheros de un directorio dentro del directorio de trabajo actual.
30. cp -a /tmp/dir1 . → copiar un directorio dentro del directorio actual de trabajo.
31. cp -a dir1 → copiar un directorio.
32. cp -a dir1 dir2 → copiar dos directorios al unísono.
33. ln -s file1 lnk1 → crear un enlace simbólico al fichero o directorio.
34. ln file1 lnk1 → crear un enlace físico al fichero o directorio.
35. touch file1 → actualizar la fecha de modificación de file1, o crearlo si no existe.
36. touch -t 0712250000 file1 → modificar el tiempo real (tiempo de creación) de un fichero o directorio.
37. file file1 → salida (volcado en pantalla) del tipo mime de un fichero texto.

38. iconv -l → listas de cifrados conocidos.
39. iconv -f fromEncoding -t toEncoding inputFile > outputFile → crea una nueva forma del fichero de entrada asumiendo que está codificado en fromEncoding y convirtiéndolo a ToEncoding.

Encontrar archivos

1. find / -name file1 → buscar fichero y directorio a partir de la raíz del sistema.
2. find / -user user1 → buscar ficheros y directorios pertenecientes al usuario "user1".
3. find /home/user1 -name *.bin → buscar ficheros con extensión". bin" dentro del directorio / home/user1.
4. find /usr/bin -type f -atime +100 → buscar ficheros binarios no usados en los últimos 100 días.
5. find /usr/bin -type f -mtime -10 → buscar ficheros creados o cambiados dentro de los últimos 10 días.
6. find / -name *.rpm -exec chmod 755 '{}' \; → buscar ficheros con extensión". rpm" y modificar permisos.
7. find. -type f -print0 | xargs -0 chmod 644 → modificar recursivamente los permisos a todos los ficheros bajo el directorio actual.[2)]
8. find / -xdev -name *.rpm → Buscar ficheros con extensión '.rpm' ignorando los dispositivos removibles como cdrom, pen-drive, etc.…
9. find. -maxdepth 1 -name *.jpg -print -exec convert "{}" -resize 80×60 "thumbs/{}" \; → agrupar ficheros redimensionados en el directorio actual y enviarlos a directorios en vistas de miniaturas (requiere convertir desde Imagemagick).

10. locate *.ps → encuentra ficheros con extensión".ps" ejecutados primeramente con el command updatedb.
11. whereis halt → mostrar la ubicación de un fichero binario, de ayuda o fuente. En este caso pregunta dónde está el comando halt.
12. which comando → mostrar la ruta completa a un comando.

Montando un sistema de ficheros

1. mount /dev/hda2 /mnt/hda2 → montar un disco llamado hda2. Verifique primero la existencia del directorio '/ mnt/ hda2'; si no está, debe crearlo.
2. umount /dev/hda2 → desmontar un disco llamado hda2. (Antes es necesario salir del punto '/mnt/hda2'.
3. fuser -km /mnt/hda2 → forzar el desmontaje cuando el dispositivo está ocupado.
4. umount -n /mnt/hda2 → correr el desmontaje sin leer el fichero /etc/mtab. Útil cuando el fichero es de solo lectura o el disco duro está lleno.
5. mount /dev/fd0 /mnt/floppy → montar un disco flexible (floppy).
6. mount /dev/cdrom /mnt/cdrom → montar un cdrom / dvdrom.
7. mount /dev/hdc /mnt/cdrecorder → montar un cd regrabable o un dvdrom.
8. mount /dev/hdb /mnt/cdrecorder → montar un cd regrabable / dvdrom (un dvd).
9. mount -t udf, iso9660 -o loop file.iso /mnt/cdrom → montar un fichero de imagen de un medio óptico (como un CD o DVD en formato ISO).

10. mount -t vfat /dev/hda5 /mnt/hda5 → montar un sistema de ficheros FAT32.
11. mount -t ntfs-3g /dev/hda5 /mnt/hda5 → montar un sistema de ficheros NTFS.
12. mount /dev/sda1 /mnt/usbdisk → montar un usb pen-drive o una memoria (sin especificar el tipo de sistema de ficheros).

Espacio en disco

1. df -h → mostrar una lista de las particiones montadas.
2. ls -lSr | more → mostrar el tamaño de los ficheros y directorios ordenados por tamaño.
3. du -sh dir1 → Estimar el espacio usado por el directorio 'dir1'.
4. du -sk * | sort -nr → mostrar en orden descendente el tamaño de los ficheros y subdirectorios en la ubicación actual, en KiB.
5. du -h --max-depth=1 | sort -nr → mostrar en orden descendente el tamaño de todos los subdirectorios en la ubicación actual, usando unidades de medida adaptables.

Usuarios y grupos

1. groupadd nombre_del_grupo → crear un nuevo grupo.
2. groupdel nombre_del_grupo → borrar un grupo.
3. groupmod -n nuevo_nombre_del_grupo viejo_nombre_del_grupo → renombrar un grupo.
4. adduser usuario1 → Crear un nuevo usuario, mediante un asistente.
5. useradd -c "Nombre Apellido" -g admin -d /home/usuario1 -s /bin/bash usuario1 → Crear un nuevo usuario perteneciente al grupo "admin".

6. useradd usuario1 → crear un nuevo usuario.
7. userdel -r usuario1 → borrar un usuario, eliminando su directorio Home.
8. usermod -c "Usuario de FTP" -g system -d /ftp/usuario1 -s /sbin/nologin usuario1 → cambiar los atributos de un usuario.
9. usermod -aG plugdev,dialout,pip user1 → agregar el usuario user1 a otros grupos existentes, para incrementar sus permisos (en este caso, agregar la posibilidad de conectar dispositivos, configurar y utilizar el modem)
10. passwd → cambiar contraseña.
11. passwd usuario1 → cambiar la contraseña de 'usuario1' (solamente ejecutable como superusuario).
12. chage -E 2011-12-31 user1 → colocar un plazo para la contraseña del usuario. En este caso dice que la clave expira el 31 de diciembre de 2011.
13. pwck → chequear la sintaxis correcta el formato de fichero de '/etc/passwd' y la existencia de usuarios.
14. grpck → chequear la sintaxis correcta y el formato del fichero '/etc/group' y la existencia de grupos.
15. newgrp grupo1 → registra a un nuevo grupo para cambiar el grupo predeterminado de los ficheros creados recientemente.

Permisos en ficheros (usar "+" para colocar permisos y "-" para eliminar)

1. ls -lh → Mostrar permisos.
2. ls /tmp | pr -T5 -W$COLUMNS → dividir la terminal en 5 columnas.

3. chmod ugo+rwx directory1 → colocar permisos de lectura ®, escritura (w) y ejecución(x) al propietario (u), al grupo (g) y a otros (o) sobre el directorio 'directory1'.
4. chmod go-rwx directory1 → quitar permiso de lectura ®, escritura (w) y (x) ejecución al grupo (g) y otros (o) sobre el directorio 'directory1'.
5. chown user1 file1 → cambiar el dueño de un fichero.
6. chown -R user1 directory1 → cambiar el propietario de un directorio y de todos los ficheros y directorios contenidos dentro.
7. chgrp group1 file1 → cambiar grupo de ficheros.
8. chown user1:group1 file1 → cambiar usuario y el grupo propietario de un fichero.
9. find / -perm -u+s → visualizar todos los ficheros del sistema con SUID configurado.
10. chmod u+s /bin/file1 → colocar el bit SUID en un fichero binario. El usuario que corriendo ese fichero adquiere los mismos privilegios como dueño.
11. chmod u-s /bin/file1 → deshabilitar el bit SUID en un fichero binario.
12. chmod g+s /home/public → colocar un bit SGID en un directorio –similar al SUID pero por directorio.
13. chmod g-s /home/public → desabilitar un bit SGID en un directorio.
14. chmod o+t /home/public → colocar un bit STIKY en un directorio. Permite el borrado de ficheros solamente a los dueños legítimos.
15. chmod o-t /home/public → desabilitar un bit STIKY en un directorio.

Atributos especiales en ficheros (usar "+" para colocar permisos y "-" para eliminar)

1. chattr +a file1 → permite escribir abriendo un fichero solamente modo append.
2. chattr +c file1 → permite que un fichero sea comprimido / descomprimido automaticamente.
3. chattr +d file1 → asegura que el programa ignore borrar los ficheros durante la copia de seguridad.
4. chattr +i file1 → convierte el fichero en inmutable o invariable, por lo que no puede ser eliminado, alterado, renombrado, ni enlazado.
5. chattr +s file1 → permite que un fichero sea borrado de forma segura.
6. chattr +S file1 → asegura que un fichero sea modificado, los cambios son escritos en modo synchronous como con sync.
7. chattr +u file1 → te permite recuperar el contenido de un fichero aún si este está cancelado.
8. lsattr → mostrar atributos especiales.

Archivos y ficheros comprimidos

1. 7za a -mx=9 -ms=on -mhe=on -p archivocomprimido directorio1 archivo1 archivo2 → comprimir un directorio y dos archivos en formato 7zip, con compresión sólida máxima, y protección por contraseña (la extensión 7z se agrega automáticamente).
2. 7za x archivocomprimido.7z → extraer un archivo comprimido en 7zip (7zip también permite descomprimir otros formatos, como por ejemplo, zip).

3. bunzip2 file1.bz2 → descomprime in fichero llamado 'file1.bz2'.
4. bzip2 file1 → comprime un fichero llamado 'file1'.
5. gunzip file1.gz → descomprime un fichero llamado 'file1.gz'.
6. gzip file1 → comprime un fichero llamado 'file1'.
7. gzip -9 file1 → comprime con compresión máxima.
8. rar a file1.rar test_file → crear un fichero rar llamado 'file1.rar'.
9. rar a file1.rar file1 file2 dir1 → comprimir 'file1', 'file2' y 'dir1' simultáneamente.
10. rar x file1.rar → descomprimir archivo rar.
11. unrar x file1.rar → descomprimir archivo rar.
12. tar -cvf archive.tar file1 → crear un tarball descomprimido.
13. tar -cvf archive.tar file1 file2 dir1 → crear un archivo conteniendo 'file1', 'file2' y'dir1'.
14. tar -tf archive.tar → mostrar los contenidos de un archivo.
15. tar -xvf archive.tar → extraer un tarball (si el archivo además está comprimido con gzip, bzip2 o xz, descomprimirlo automáticamente).
16. tar -xvf archive.tar -C /tmp → extraer un tarball en /tmp.
17. tar -cjvf archive.tar.bz2 dir1 → crear un tarball comprimido en bzip2.
18. tar -xjvf archive.tar.bz2 → descomprimir un archivo tar comprimido en bzip2
19. tar -cJvf archive.tar.xz dir1 → crear un tarball comprimido en xz.

20. XZ_OPT=-9e tar -cJvf archive.tar.xz dir1 → crear un tarball comprimido en xz (con máxima compresión).
21. tar -xJvf archive.tar.xz → descomprimir un archivo tar comprimido en xz.
22. tar -czvf archive.tar.gz dir1 → crear un tarball comprimido en gzip.
23. tar -I pigz -cf archive.tar.gz dir1 → crear un tarball comprimido en gzip, pero utilizando pigz, que comprime en paralelo aprovechando todos los núcleos de los microprocesadores del equipo.
24. GZIP=-9 tar -czvf archive.tar.gz dir1 → crear un tarball comprimido en gzip (con máxima compresión).
25. tar -xzvf archive.tar.gz → descomprimir un archive tar comprimido en gzip.
26. zip file1.zip file1 → crear un archivo comprimido en zip.
27. zip -r file1.zip file1 file2 dir1 → comprimir, en zip, varios archivos y directorios de forma simultánea.
28. unzip file1.zip → descomprimir un archivo zip.

Paquetes rpm (Red Hat, Fedora y similares)

1. rpm -ivh package.rpm → instalar un paquete rpm.
2. rpm -ivh --nodeeps package.rpm → instalar un paquete rpm ignorando las peticiones de dependencias.
3. rpm -U package.rpm → actualizar un paquete rpm sin cambiar la configuración de los ficheros.
4. rpm -F package.rpm → actualizar un paquete rpm solamente si este está instalado.
5. rpm -e package_name.rpm → eliminar un paquete rpm.

6. rpm -qa → mostrar todos los paquetes rpm instalados en el sistema.
7. rpm -qa | grep httpd → mostrar todos los paquetes rpm con el nombre "httpd".
8. rpm -qi package_name → obtener información en un paquete específico instalado.
9. rpm -qg "System Environment/Daemons" → mostar los paquetes rpm de un grupo software.
10. rpm -ql package_name → mostrar lista de ficheros dados por un paquete rpm instalado.
11. rpm -qc package_name → mostrar lista de configuración de ficheros dados por un paquete rpm instalado.
12. rpm -q package_name --whatrequires → mostrar lista de dependencias solicitada para un paquete rpm.
13. rpm -q package_name --whatprovides → mostar la capacidad dada por un paquete rpm.
14. rpm -q package_name --scripts → mostrar los scripts comenzados durante la instalación /eliminación.
15. rpm -q package_name --changelog → mostar el historial de revisions de un paquete rpm.
16. rpm -qf /etc/httpd/conf/httpd.conf → verificar cuál paquete rpm pertenece a un fichero dado.
17. rpm -qp package.rpm -l → mostrar lista de ficheros dados por un paquete rpm que aún no ha sido instalado.
18. rpm --import /media/cdrom/RPM-GPG-KEY → importar la firma digital de la llave pública.
19. rpm --checksig package.rpm → verificar la integridad de un paquete rpm.

20. rpm -qa gpg-pubkey → verificar la integridad de todos los paquetes rpm instalados.
21. rpm -V package_name → chequear el tamaño del fichero, licencias, tipos, dueño, grupo, chequeo de resumen de MD5 y última modificación.
22. rpm -Va → chequear todos los paquetes rpm instalados en el sistema. Usar con cuidado.
23. rpm -Vp package.rpm → verificar un paquete rpm no instalado todavía.
24. rpm2cpio package.rpm | cpio --extract --make-directories *bin → extraer fichero ejecutable desde un paquete rpm.
25. rpm -ivh /usr/src/redhat/RPMS/`arch`/package.rpm → instalar un paquete construido desde una fuente rpm.
26. rpmbuild --rebuild package_name.src.rpm construir un paquete rpm desde una fuente rpm.

Actualizador de paquetes yum (Fedora, Redhat y otros)

1. yum install package_name → descargar e instalar un paquete rpm.
2. yum localinstall package_name.rpm → este instalará un RPM y tratará de resolver todas las dependencies para ti, usando tus repositorios.
3. yum update → actualizar todos los paquetes rpm instalados en el sistema.
4. yum update package_name → modernizar / actualizar un paquete rpm.
5. yum remove package_name → eliminar un paquete rpm.
6. yum list → listar todos los paquetes instalados en el sistema.

7. yum search package_name → Encontrar un paquete en repositorio rpm.
8. yum clean packages → limpiar un caché rpm borrando los paquetes descargados.
9. yum clean headers → eliminar todos los ficheros de encabezamiento que el sistema usa para resolver la dependencia.
10. yum clean all → eliminar desde los paquetes caché y ficheros de encabezado.

Gestión de paquetes deb (Debian, Ubuntu y otros)

1. dpkg -i elpaquete.deb → instalar / actualizar un paquete.
2. dpkg -r elpaquete → eliminar un paquete deb del sistema.
3. dpkg -l → mostrar todos los paquetes deb instalados en el sistema.
4. dpkg -l | grep httpd → mostrar todos los paquetes deb con el nombre "httpd"
5. dpkg -s elpaquete → obtener información en un paquete específico instalado en el sistema.
6. dpkg -L elpaquete → mostar lista de ficheros utilizados por un paquete instalado en el sistema.
7. dpkg -c elpaquete.deb → mostrar contenido de un paquete (no necesariamente instalado).
8. dpkg -S /bin/ping → verificar a qué paquete pertenece un fichero dado.

Actualizador de paquetes apt y aptitude (Debian, Ubuntu y otros)

1. apt-get install package_name → instalar / actualizar un paquete deb.
2. apt-cdrom install package_name → instalar / actualizar un paquete deb desde un cdrom.
3. apt-get update → actualizar la lista de paquetes.
4. apt-get upgrade → actualizar todos los paquetes instalados.
5. apt-get remove package_name → eliminar un paquete deb del sistema.
6. apt-get check → verificar la correcta resolución de las dependencias.
7. apt-get clean → limpiar cache desde los paquetes descargados.
8. apt-cache search searched-package → retorna lista de paquetes que corresponde a la serie «paquetes buscados».
9. aptitude search paquete → busca un paquete por el nombre.
10. aptitude search ~dpaquete → busca un paquete por la descripción.
11. aptitude show paquete | less → muestra información sobre un paquete.
12. aptitude install paquete1 paquete2 … → instala varios paquetes con sus dependencias y recomendaciones.
13. aptitude -R install paquete → instala un paquete con sus dependencias, pero sin las recomendaciones.
14. aptitude why paquete → lista las razones por las que se debería instalar el paquete.
15. aptitude why-not paquete → lista las razones por las que no se puede instalar el paquete.

16. aptitude -rsvW install paquete → simula la instalación de un paquete con sus dependencias y recomendaciones, detallando cada una.
17. aptitude remove paquete → desinstala un paquete.
18. aptitude purge paquete → desinstala un paquete y lo limpia de la cache.
19. aptitude clean → limpia la cache de paquetes.
20. apt-file -xi search 'sql' → busca todos los paquetes que contengan un archivo o directorio con la expresión *sql* (sin considerar mayúsculas o minúsculas).

Ver el contenido de un fichero

1. cat file1 → ver los contenidos de un fichero comenzando desde la primera línea.
2. tac file1 → ver los contenidos de un fichero comenzando desde la última línea.
3. more file1 → ver el contenido de un fichero de manera paginada.
4. less file1 → parecido al commando 'more' pero permite avanzar, retroceder, y buscar (compatible con algunos comandos de vi).
5. head -2 file1 → ver las dos primeras líneas de un fichero (ó 10, si no se especifica la cantidad de líneas).
6. tail -2 file1 → ver las dos últimas líneas de un fichero (ó 10, si no se especifica la cantidad de líneas).

Manipulación de texto

1. cat file1 file2 … | command <> file1_in.txt_or_file1_out.txt → sintaxis general para la manipulación de texto utilizando PIPE, STDIN y STDOUT.

2. cat file1 | command(sed, grep, awk, grep, etc…) > result.txt → sintaxis general para manipular un texto de un fichero y escribir el resultado en un fichero nuevo.
3. cat file1 | command(sed, grep, awk, grep, etc…) >> result.txt → sintaxis general para manipular un texto de un fichero y añadir resultado en un fichero existente.
4. grep Aug /var/log/messages → buscar palabras "Aug" en el fichero '/var/log/messages'.
5. grep ^Aug /var/log/messages → buscar palabras que comienzan con "Aug" en fichero '/var/log/messages'
6. grep [0-9] /var/log/messages → seleccionar todas las líneas del fichero '/var/log/messages' que contienen números.
7. grep Aug -R /var/log/ → buscar la cadena "Aug" en el directorio '/var/log' y debajo.
8. sed 's/string1/string2/g' ejemplo.txt → reemplazar en ejemplo. txt todas las ocurrencias de "string1" con "string2"
9. sed '/^$/d' ejemplo.txt → eliminar todas las líneas en blanco desde el ejemplo.txt
10. sed '/ *#/d; /^$/d' ejemplo.txt → eliminar comentarios y líneas en blanco de ejemplo.txt
11. echo 'ejemplo' | tr '[:lower:]' '[:upper:]' → convertir "ejemplo" de minúsculas a mayúsculas.
12. sed -e '1d' ejemplo.txt → elimina la primera línea del fichero ejemplo.txt
13. sed -n '/string1/p' → visualizar solamente las líneas que contienen la palabra "string1".
14. sed -r 's/(cadena1)(cadena2)/\2\1/g' → utilizar expresiones regulares extendidas para intercambiar el orden de dos cadenas de texto, en todas las instancias que aparezcan.

Establecer caracteres y conversión de ficheros

1. dos2unix filedos.txt fileunix.txt → convertir un formato de fichero texto desde MSDOS a UNIX.
2. unix2dos fileunix.txt filedos.txt → convertir un formato de fichero de texto desde UNIX a MSDOS.
3. recode ..HTML < page.txt > page.html → convertir un fichero de texto en html.
4. recode -l | more → mostrar todas las conversiones de formato disponibles.

Análisis del sistema de ficheros

1. badblocks -v /dev/hda1 → Chequear los bloques defectuosos en el disco hda1.
2. fsck /dev/hda1 → reparar / chequear la integridad del fichero del sistema Linux en el disco hda1.
3. fsck.ext2 /dev/hda1 → reparar / chequear la integridad del fichero del sistema ext 2 en el disco hda1.
4. e2fsck /dev/hda1 → reparar / chequear la integridad del fichero del sistema ext 2 en el disco hda1.
5. e2fsck -j /dev/hda1 → reparar / chequear la integridad del fichero del sistema ext 3 en el disco hda1.
6. fsck.ext3 /dev/hda1 → reparar / chequear la integridad del fichero del sistema ext 3 en el disco hda1.
7. fsck.vfat /dev/hda1 → reparar / chequear la integridad del fichero sistema fat en el disco hda1.
8. fsck.msdos /dev/hda1 → reparar / chequear la integridad de un fichero del sistema dos en el disco hda1.

9. dosfsck /dev/hda1 → reparar / chequear la integridad de un fichero del sistema dos en el disco hda1.

Formatear un sistema de ficheros

1. mkfs /dev/hda1 → crear un fichero de sistema tipo Linux en la partición hda1.
2. mke2fs /dev/hda1 → crear un fichero de sistema tipo Linux ext 2 en hda1.
3. mke2fs -j /dev/hda1 → crear un fichero de sistema tipo Linux ext3 (periódico) en la partición hda1.
4. mkfs -t vfat 32 -F /dev/hda1 → crear un fichero de sistema FAT32 en hda1.
5. fdformat -n /dev/fd0 → formatear un disco flooply.
6. mkswap /dev/hda3 → crear un fichero de sistema swap.

Partición de sistema swap

1. mkswap /dev/hda3 → crear fichero de sistema swap.
2. swapon /dev/hda3 → activando una nueva partición swap.
3. swapon /dev/hda2 /dev/hdb3 → activar dos particiones swap.

Salvas

1. dump -0aj -f /tmp/home0.bak /home → hacer una salva completa del directorio '/home'.
2. dump -1aj -f /tmp/home0.bak /home → hacer una salva incremental del directorio '/home'.

3. restore -if /tmp/home0.bak → restaurando una salva interactivamente.
4. rsync -rogpav --delete /home /tmp → sincronización entre directorios.
5. rsync -rogpav -e ssh --delete /home ip_address:/tmp → rsync a través del túnel SSH.
6. rsync -az -e ssh --delete ip_addr:/home/public /home/local →sincronizar un directorio local con un directorio remoto a través de ssh y de compresión.
7. rsync -az -e ssh --delete /home/local ip_addr:/home/public → sincronizar un directorio remoto con un directorio local a través de ssh y de compresión.
8. dd bs=1M if=/dev/hda | gzip | ssh user@ip_addr 'dd of=hda.gz' → hacer una salva de un disco duro en un host remoto a través de ssh.
9. dd if=/dev/sda of=/tmp/file1 → salvar el contenido de un disco duro a un fichero. (En este caso el disco duro es "sda" y el fichero "file1").
10. tar -Puf backup.tar /home/user → hacer una salva incremental del directorio '/home/user'.
11. tar -czv --exclude=/root/dir1/* -f /var/salvas/cfg_$(date +%F_%H%M).tgz /etc /root → salvar los directorios /etc y /root (excluyendo el contenido del subdirectorio /root/dir1/) en un archivo comprimido, cuyo nombre contenga la fecha y hora actual.
12. (cd /tmp/local/ && tar c .) | ssh -C user@ip_addr 'cd /home/share/ && tar x -p' → copiar el contenido de un directorio en un directorio remoto a través de ssh.
13. (tar c /home) | ssh -C user@ip_addr 'cd /home/backup-home && tar x -p' → copiar un directorio local en un directorio remoto a través de ssh.

14. tar cf - . | (cd /tmp/backup ; tar xf -) → copia local conservando las licencias y enlaces desde un directorio a otro.
15. find /home/user1 -name '*.txt' | xargs cp -av --target-directory=/home/backup/ --parents → encontrar y copiar todos los ficheros con extensión '.txt' de un directorio a otro.
16. find ~/ -type f -not -iname '*.mp*' -not \(-iregex '.*\.mozilla/.*' -o -iregex '.*\.thumbnails/.*' \) -prune -mtime 14 -print0 | xargs -0 tar -czf /var/salvas/myhome.tgz → realizar una salva de todos los archivos de nuestro perfil de usuario modificados dentro de los últimos 14 días, exceptuando los archivos mp3, mpg y similares, y los directorios .mozilla/ y .thumbnails/.
17. find /var/log -name '*.log' | tar cv --files-from=- | bzip2 > log.tar.bz2 → encontrar todos los ficheros con extensión '.log' y hacer un archivo bzip.
18. dd if=/dev/hda of=/dev/fd0 bs=512 count=1 → hacer una copia del MRB (Master Boot Record) a un disco floppy.
19. dd if=/dev/fd0 of=/dev/hda bs=512 count=1 → restaurar la copia del MBR (Master Boot Record) salvada en un floppy.

CDROM

1. cdrecord -v gracetime=2 dev=/dev/cdrom -eject blank=fast -force → limpiar o borrar un cd regrabable.
2. mkisofs /dev/cdrom > cd.iso → crear una imagen iso de cdrom en disco.
3. mkisofs /dev/cdrom | gzip > cd_iso.gz → crear una imagen comprimida iso de cdrom en disco.
4. mkisofs -J -allow-leading-dots -R -V "Label CD" -iso-level 4 -o ./cd.iso data_cd → crear una imagen iso de un directorio.
5. cdrecord -v dev=/dev/cdrom cd.iso → quemar una imagen iso.

6. gzip -dc cd_iso.gz | cdrecord dev=/dev/cdrom - → quemar una imagen iso comprimida.
7. mount -t udf,iso9660 -o loop cd.iso /mnt/iso → montar una imagen iso.
8. cd-paranoia -B → llevar canciones de un cd a ficheros wav.
9. cd-paranoia -- "-3" → llevar las 3 primeras canciones de un cd a ficheros wav.
10. cdrecord --scanbus → escanear bus para identificar el canal scsi.
11. dd if=/dev/hdc | md5sum → hacer funcionar un md5sum en un dispositivo, como un CD.
12. eject -v → expulsar un medio o disco extraíble, ofreciendo información adicional.

Trabajo con la red (LAN Y WIFI)

1. ifconfig eth0 → mostrar la configuración de una interfaz de red Ethernet.
2. ifup eth0 → activar la interfaz eth0.
3. ifdown eth0 → deshabilitar la interfaz eth0.
4. ifconfig eth0 192.168.1.1 netmask 255.255.255.0 → configurar una dirección IP.
5. ifconfig eth0 promisc → configurar eth0 en modo promiscuo para obtener los paquetes (*sniffing*).
6. dhclient eth0 → activar la interface 'eth0' en modo dhcp.
7. route -n → mostrar tabla de rutas.
8. route add -net 0/0 gw IP_Gateway → configurar entrada predeterminada.

9. ip route show | grep default | awk {'print $3'} → conocer la puerta de enlace predeterminada.
10. route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.1.1 → configurar ruta estática para buscar la red 192.168.0.0/16.
11. route del 0/0 gw IP_gateway → eliminar la ruta estática.
12. echo 1 > /proc/sys/net/ipv4/ip_forward → activar el redireccionamiento de paquetes ip.
13. hostname → mostrar el nombre del host del sistema.
14. host www.example.com → buscar el nombre del host para resolver el nombre a una dirección ip (1).
15. nslookup www.example.com → buscar el nombre del host para resolver el nombre a una direcciόm ip y viceversa (2).
16. ip link show → mostar el estado de enlace de todas las interfaces.
17. mii-tool eth0 → mostar el estado de enlace de eth0.
18. ethtool eth0 → mostrar las estadísticas de la interfaz de red eth0.
19. netstat -tup → mostrar todas las conexiones de red activas y sus PID.
20. netstat -tupl → mostrar todos los servicios de escucha de red en el sistema y sus PID.
21. netstat -punta → mostrar todas las conexiones activas por dirección IP y puerto.
22. tcpdump tcp port 80 → mostrar todo el tráfico HTTP.
23. iwlist scan → mostrar las redes inalámbricas.
24. iwconfig eth1 → mostrar la configuración de una interfaz de red inalámbrica.

25. whois www.example.com → buscar en base de datos Whois.
26. iftop -nNP -i eth0 → mostrar en tiempo real las conexiones abiertas en eth0 y su tasa de transferencia.
27. sockstat → mostrar información sobre las conexiones abiertas.
28. arp-scan -l → descubrir en la red las direcciones IP y MAC.
29. nm-tool → muestra configuración de red (en caso de usar Network Manager obtiene los DNS).

Redes de Microsoft Windows (Samba)

1. nbtscan ip_addr → resolución de nombre de red bios.
2. nmblookup -A ip_addr → resolución de nombre de red bios.
3. smbclient -L ip_addr/hostname → mostrar acciones remotas de un host en windows.

Cortafuegos (iptables)

1. iptables -t filter -L → mostrar todas las cadenas de la tabla de filtro.
2. iptables -t nat -L → mostrar todas las cadenas de la tabla nat.
3. iptables -t filter -F → limpiar todas las reglas de la tabla de filtro.
4. iptables -t nat -F → limpiar todas las reglas de la tabla nat.
5. iptables -t filter -X → borrar cualquier cadena creada por el usuario.
6. iptables -t filter -A INPUT -p tcp --dport telnet -j ACCEPT → permitir las conexiones telnet para entar.

7. iptables -t filter -A OUTPUT -p tcp --dport http -j DROP →bloquear las conexiones HTTP para salir.
8. iptables -t filter -A FORWARD -p tcp --dport pop3 -j ACCEPT → permitir las conexiones POP a una cadena delantera.
9. iptables -t filter -A INPUT -p tcp -m multiport --dports 80,443,8080 -m state --state NEW -m limit --limit 4/sec --limit-burst 8 -j ACCEPT → establecer un límite de 4 peticiones por segundo de nuevas conexiones, con posibles ráfagas ocasionales (útil para políticas de denegación por defecto).
10. iptables -t filter -A INPUT -p tcp -m multiport --dports 80,443,8080 -m state --state ESTABLISHED,RELATED -m connlimit ! --conlimit-above 6 -j ACCEPT → establecer un límite de 6 conexiones simultáneas por equipo a nuestro servidor web (útil para políticas de denegación por defecto).
11. iptables -t filter -A INPUT -j LOG --log-prefix "DROP INPUT" → registrando una cadena de entrada.
12. iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE → configurar un PAT (Puerto de traducción de dirección) en eth0, ocultando los paquetes de salida forzada. (Indicado para enlaces tipo ppp)
13. iptables -t nat -A POSTROUTING -s 192.168.0.127 -o eth0 -j SNAT --to-source 169.158.158.169 → enrutar los paquetes desde 192.168.0.127 hacia otras redes por eth0 y asignarles un dirección ip externa. (Indicado para enlaces tipo ADSL)
14. iptables -t nat -A PREROUTING -d 192.168.0.1 -p tcp -m tcp --dport 22 -j DNAT --to-destination 10.0.0.2:22 →redireccionar los paquetes diriguidos de un host a otro.
15. iptables -t nat -S → Listar todas las reglas activas en la tabla nat.
16. iptables-save -c > archivo → Salvar las reglas en un archivo (incluyendo los contadores de paquetes y bytes).

17. iptables-restore -c < archivo → Restaurar las reglas desde un archivo (incluyendo los contadores de paquetes y bytes).

Monitoreando y depurando

1. top → mostrar en tiempo real las tareas de linux.
2. htop → mostrar y gestionar las tareas con una interfaz amistosa.
3. ps -eafw → muestra las tareas Linux.
4. ps -e -o pid,args --forest → muestra las tareas Linux en un modo jerárquico.
5. ps -o pid,cmd -ww -C wget → listar todas las instancias del comando wget con sus argumentos.
6. pstree → mostrar un árbol sistema de procesos.
7. pidof pppd → mostrar el pid del proceso pppd.
8. kill -9 ID_Processo → forzar el cierre de un proceso y terminarlo.
9. kill -1 ID_Processo → forzar un proceso para recargar la configuración.
10. killall Nombre_Proceso → terminar un proceso por el nombre del comando y no por el ID.
11. kill -HUP $(ps -A -o state,pid --no-header | grep -e '^[Zz]' | awk '{print $2}' | xargs) → terminar todos los procesos *zombies*.
12. lsof -p $$ →mostrar una lista de ficheros abiertos por procesos.
13. lsof /home/user1 → muestra una lista de ficheros abiertos en un camino dado del sistema.

14. strace -c ls >/dev/null → mostrar las llamadas del sistema hechas y recibidas por un proceso.
15. strace -f -e open ls >/dev/null → mostrar las llamadas a la biblioteca.
16. watch -n1 'cat /proc/interrupts' → mostrar interrupciones en tiempo real.
17. last reboot → mostrar historial de reinicio.
18. lsmod → mostrar los módulos del kernel cargados.
19. free -m → muestra el estado de la RAM en megabytes.
20. smartctl -A /dev/hda → monitorear la fiabilidad de un disco duro a través de SMART.
21. smartctl -i /dev/hda → chequear si SMART está activado en un disco duro.
22. tail -f /var/log/dmesg → mostrar eventos inherentes al proceso de carga del kernel.
23. tail -f /var/log/messages → mostrar los eventos del sistema.
24. multitail --follow-all /var/log/{dmesg,messages} → mostrar dos registros de eventos en una misma pantalla.

Seguridad y Cifrado

1. base64 /home/archivo > /home/archivo-codificado → codifica "archivo" en 'base64' y lo guarda en /home
2. base64 -d /home/archivo-codificado > /home/archivo →decodifica "archivo-codificado" y lo guarda en /home
3. openssl req -x509 -nodes -days 3650 -newkey rsa:1024 -out /etc/millave.crt -keyout /etc/millave.key → crea un certificado auto-firmado para cifrar el tráfico web con SSL.

4. htpasswd -c -m /etc/apache2/.htpasswd nombreusuario genera un archivo '.htpasswd' para proteger un sitio web con auntenticación.

Otros comandos útiles

1. apropos palabraclave → mostrar una lista de comandos que pertenecen a las palabras claves de un programa; son útiles cuando tú sabes qué hace tu programa, pero desconoces el nombre del comando.
2. man ping → mostrar las páginas del manual on-line; por ejemplo, en un comando ping, usar la opción '-k' para encontrar cualquier comando relacionado.
3. man -t ping | ps2pdf - ping.pdf → convertir las páginas del manual del comando ping en un archivo pdf (para lo cual es necesario haber instalado Ghostscript).
4. mkbootdisk --device /dev/fd0 `uname -r` → crear un floppy boteable.
5. gpg -c file1 → codificar un fichero con guardia de seguridad GNU.
6. gpg file1.gpg → decodificar un fichero con Guardia de seguridad GNU.
7. wget -r www.example.com → descargar un sitio web completo.
8. wget -c www.example.com/file.iso → descargar un fichero con la posibilidad de parar la descargar y reanudar más tarde.
9. echo 'wget -c www.example.com/files.iso' | at 09:00 → Comenzar una descarga a cualquier hora. En este caso empezaría a las 9 horas.
10. ldd /usr/bin/ssh → mostrar las bibliotecas compartidas requeridas por el programa ssh.

11. alias hh='history' → colocar un alias para un commando. En este caso, para invocar el historial con hh.
12. chsh → cambiar el comando Shell.
13. chsh --list-shells → es un comando adecuado para saber si tienes que hacer remoto en otra terminal.
14. who -a → mostrar quien está registrado, e imprimir hora del último sistema de importación, procesos muertos, procesos de registro de sistema, procesos activos producidos por init, funcionamiento actual y últimos cambios del reloj del sistema.
15. echo "128*1024*1024" | bc → calcular desde la consola el tamaño en bytes de 128 MiB.
16. sudo !! → ejecutar como superusuario el último comando tecleado.
17. clear → limpiar la pantalla.
18. uncomando > archivodesalida.txt 2>&1 → ejecuta un comando y redirige la salida a un archivo, combinando en este tanto STDOUT como STDERR.
19. uncomando > archivodesalida.txt 2> archivoerrores.txt → ejecuta un comando, redirige la salida (STDOUT) a un archivo, y los errores (STDERR) a otro.
20. uncomando | tee archivodesalida.txt → ejecuta un comando, muestra la salida en la pantalla y simultáneamente la escribe a un archivo.

Referencias Bibliograficas

Anasagasti, P. d. (2016). Sistemas Operativos. MADRID: Universidad Politécnica de Madrid.

Felici, S. (2003). Sistemas operativos. Telemática.

López, W. I. (2003). Fundamentos de sistema operativos con énfasis en GNU/LINUX. Lsi.

Robles, D. (2015). Fundamentos de Sistemas Operativos. Universidad Nacional Autónoma de México.

Pelús, B. (2018). Cloud Hosting Tecnology. http://www.grupotelfor.com Recuperado de http://www.grupotelfor.com/blog/7-centos-7/8-configurar-las-interfaces-de-red-en-centos-7

Mediavilla et al (2015). Recuperado de https://mirror.jkanetwork.com/

Digital Guide. España. Recuperado de: https://www.1and1.es/digitalguide/servidores/know-how/que-es-centos-versiones-y-requisitos-del-sistema/

Operating system. (2018). Estados Unidos. Recuperado de https://www.debian.org/releases/stable/i386/install.pdf.es

Ministerio de Educación Cultura y Deporte. Introducción a Linux. España. Instituto Nacional de Tecnologías Educativas y de

formación de Profesorado. Recuperado de: http://www.ite.educacion.es

García, P (2012). Instalación de ssh en CentOS virtualizado. Recuperado de:https://riunet.upv.es/ bitstream/handle /10251/75446/ ServidorSSHCentos_v2.pdf?sequence=1

Hernandez, F.(2018). USA. Ssh (Secure Shell). Recuperado de: https:// www.ssh.com/ssh/

Cerecedo, O. (2016). Instalación de Moodle 3.3.2 en Centos 7.0. Infinite Latinoamerica. Recuperado de: https://omarcerecedo. wordpress.com/2016/10/10/instalacion-de-moodle-en-centos-7/

Medina, F.(2014). Instalación y configuración de Moodle 2.7 en Centos 7.0 con SELinux habilitado. México.Recuperado de: https:// es.slideshare.net/pacomedina/instalacin-y-configuracin-de-moodle-27-en-centos-7-con-selinux-habilitado

Upadhyay, R.(2014). Unixmen. India. How To Install Moodle 3.0 In Centos 7.0. Recuperado de: https://www.unixmen.com/ install-moodle-3-0-centos-7/

Cabrera, M. Como instalar Joomla en Linux en Linux Centos 7.0 paso a paso. Video Juegos y OpenSource. Recuperado de: http://drivemeca.blogspot.com/2016/04/como-instalar-joomla-en-linux-centos-7.html

Molina, F. y Ortega, E. (2014). Servicios en red. Madrid, España: RA-MA Editorial

Gestión de usuarios, grupos y permisos Samba. Recuperado de:

Jorba, E (2010). Introducción al sistema operativo GNU/Linux. España, Cataluña recuperado de http://openaccess.uoc.edu/webapps/ o2/bitstream/10609/61286/1/Administraci%C3%B3n%20 de%20sistemas%20GNU_Linux_M%C3%B3dulo1_ Introducci%C3%B3n%20al%20sistema%20operativo%20 GNU_Linux.pdf

Sanz, P. (2007). Directorios en Linux. España. Recuperado de http://www.uam.es/departamentos/ciencias/quimica/estruct/psm/documentacion/directorios-en-linux.pdf

Torres, J. (2011). El árbol de directorios de Linux. Recuperado de https://cursotecnicoredes2011.files.wordpress.com/2011/03/debian-tema-4-el-c3a1rbol-de-directorios.pdf

Lorandi, A. (2014). Breve historia de las distribuciones de Linux. México. Recuperado de https://www.uv.mx/personal/alorandi/files/2010/06/Breve-Historia-de-las-Distribuciones-Linux.pdf

Acerca de los autores

Jairo Vladimir Hidalgo Guijarro

Es magíster en Redes de Comunicaciones por la Universidad Católica, en Quito. Es ingeniero en Informática; ha publicado varios libros y artículos científicos en revistas de alto impacto sobre temas de seguridad informática; participó como ponente en el "3rd International Conference on Intelligent Human Systems Integration: Integrating People and Intelligent Systems" (IHSI 2020), realizado en la Universidad de Modena y Reggio Emilia, en Italia. Actualmente se desempeña como docente titular en la Universidad Politécnica Estatal del Carchi.

Georgina Guadalupe Arcos Ponce

Es ingeniera en Sistemas Computacionales por la Universidad Técnica del Norte, en Ibarra; tiene un diploma superior en Currículo por Competencias por la Universidad Técnica de Ambato; y tiene dos maestrías, una en Gerencia Informática por la Pontificia Universidad Católica del Ecuador, y otra en Desarrollo Integral de Destinos Turísticos por la Universidad de Las Palmas de Gran Canarias. Es autora y coautora de artículos científicos y libros. Desde el 2007 se desempeña como docente en la Universidad

Politécnica Estatal del Carchi, en donde, actualmente es directora de la carrera de Computación.

Jeffery Alex Naranjo Cedeño

Es ingeniero en Informática y Ciencias de la Computación por la Universidad Tecnológica Equinoccial, en Quito; tiene una maestría en Sistemas y Servicios en la Sociedad de la Información por la Universidad de Valencia, España. Desde el 2015 se desempeña como docente en la Universidad Politécnica Estatal del Carchi, en donde, además, es coordinador del Laboratorio de Fabricación Digital FABLAB.

Ha publicado varios artículos científicos en revistas especializadas y libros de investigación en el área de computación.

Educamos para
transformar el mundo

Este libro constituye un aporte esencial para estudiantes, docentes, investigadores y público en general que desee profundizar conocimientos de administración del Sistema Operativo Linux Centos en su versión 7.0. Se trata de una investigación minuciosa que permite conocer la distribución de dicho sistema operativo, es decir, sus versiones y fechas de lanzamiento, su estructura jerárquica y sus principales directorios y sistemas de archivos.

La lectura de este libro permitirá conocer la instalación y configuración de una máquina virtual paso a paso; que en este caso es Virtual Box, la cual, posteriormente, se alojará en el sistema operativo Linux Centos. Del mismo modo, el lector accederá a la creación de perfiles por medio de comandos de usuarios, carpetas y directorios, asignación de roles, permisos, personalización del sistema, interfaz y protocolos.

A partir del segundo capítulo, el libro ofrece un aspecto de suma importancia: el lector encontrará temas concomitantes y que tienen estricta relación con Linux y software libre, como son los de red plataforma web de tipo educativo virtual, con servidor Proxy y transferencias de archivos de monitoreo en servidores de escritorio remoto por medio de gestión de contenidos VPN.

Pero lo más interesante de todo el libro es, sin lugar a dudad, el hecho de que sus autores presentan todos los temas a manera de guía práctica, indicando la instalación y configuración, además de la gestión y administración. Esto le permitirá al usuario desarrollar la habilidad de autoaprendizaje.

Finalmente, el libro cuenta con un glosario de los términos y comandos más frecuentes que se utilizan, lo que le permitirá interactuar de manera fácil con los usuarios y profesionales de Linux.

M.Sc. Jhony Enríquez Herrera
Investigador Especialista en sistemas operativos.

ISBN: 978-9942-914-80-4