Índice de contenido

Información de Derechos reservados de esta publicación.

Tema 1. Aspectos Generales de GNU/Linux

1.1 Sistema Operativo

Un sistema operativo es el encargado de llevar a cabo todas las gestiones sobre los recursos de una computadora, es decir, un conjunto de programas de computadora destinado a permitir una administración eficaz de sus recursos. Comienza a trabajar cuando se enciende el computador, y gestiona el hardware de la máquina desde los niveles más básicos, permitiendo también la interacción con el usuario.

1.1.1 Función de un Sistema Operativo

Los sistemas operativos simplifican el manejo de la computadora, desempeñan una serie de funciones básicas esenciales para la gestión del equipo. Entre las más destacables, cada una ejercida por un componente interno (módulo en núcleos monolíticos y servidor en micronúcleos), podemos reseñar las siguientes:

- Proporcionar más comodidad en el uso de un computador.
- Gestionar de manera eficiente los recursos del equipo, ejecutando servicios para los procesos (programas)
- Brindar una interfaz al usuario, ejecutando instrucciones (comandos).
- Permitir que los cambios debidos al desarrollo del propio SO se puedan realizar sin interferir con los servicios que ya se prestaban (evolutividad).

1.2 UNIX

Unix es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969 por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Ken Thompson, Dennis Ritchie y Douglas McIlroy

Durante fines de la década de 1970 y principios de la década de 1980, la influencia de Unix en círculos académicos indujo a su adopción en masa (principalmente la variante BSD, que había surgido en la Universidad de California, Berkeley) en varias compañías que se iniciaban por aquel entonces, siendo la más destacada Sun Microsystems. Hoy en día, junto a los sistemas Unix certificados, también se pueden encontrar sistemas similares a Unix, como Linux y los derivados de BSD.

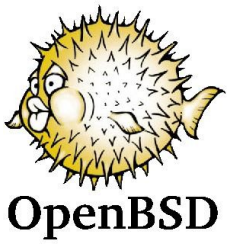
1.3 BSD

BSD son las iniciales de Berkeley Software Distribution (en español, Distribución de Software Berkeley) y se utiliza para identificar un sistema operativo derivado del sistema Unix nacido a partir de los aportes realizados a ese sistema por la Universidad de California en Berkeley.

En los primeros años del sistema Unix sus creadores, los Laboratorios Bell de la compañía AT&T, autorizaron a la Universidad de California en Berkeley y a otras universidades a utilizar el código fuente y adaptarlo a sus necesidades. Durante la década de los setenta y los ochenta Berkeley utilizó el sistema para sus investigaciones en materia de sistemas operativos. Cuando AT&T retiró el permiso de uso a la universidad por motivos comerciales, la universidad promovió la creación de una versión inspirada en el sistema Unix utilizando las aportaciones que ellos habían realizado, permitiendo luego su distribución con fines académicos y al cabo de algún tiempo reduciendo al mínimo las restricciones referente a su copia, distribución o modificación.

Algunos sistemas operativos descendientes del sistema desarrollado por Berkeley son Solaris, FreeBSD, NetBSD, OpenBSD y Mac OS X. BSD también ha hecho grandes contribuciones en el campo de los sistemas operativos en general, como por ejemplo:

- El manejo de memoria virtual paginado por demanda
- El control de trabajos
- El Fast FileSystem
- El protocolo TCP/IP
- El editor de texto vi

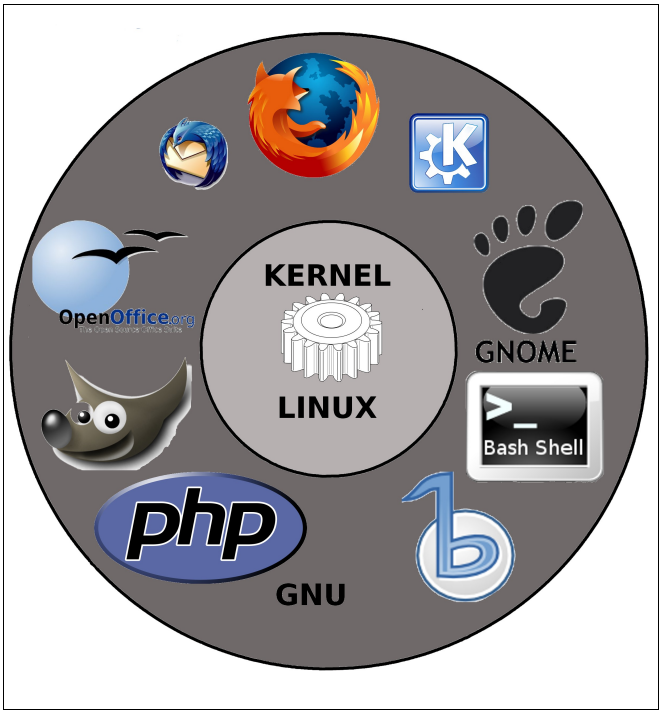


1.4 GNU/Linux

Linux es un sistema operativo tipo Unix que se distribuye bajo la Licencia Pública General de GNU (GPL) , es decir que es software libre. Su nombre proviene del Núcleo de Linux, desarrollado en 1991 por Linus Torvalds en conjunto con las aplicaciones de sistema creadas por el proyecto GNU liderado por Richard Stallman

GNU:- Representado por aplicaciones Open Source como Firefox, Gnome KDE,Thunderbird,The GIMP y OpenOffice

Kernel Linux.- Representado en Forma de Engrane, el cual esta constituido por aproximadamente 10, 000 lineas de codigo en lenguaje C



1.4.1 El Proyecto GNU

El proyecto GNU nació el 27 de septiembre de 1983 por la persona más relevante del movimiento del software libre en la actualidad, nos referimos a Richard Stallman.

El proyecto GNU fue diseñado con el objetivo de crear un sistema operativo completamente libre así como también para ser totalmente compatible con UNIX (*sistema operativo desarrollado en los* laboratorios *Bell por Dennis Ritchie*).

Para asegurar que el software GNU permaneciera libre para que todos los usuarios pudieran "ejecutarlo, copiarlo, modificarlo y distribuirlo", el proyecto debía ser liberado bajo una licencia diseñada para garantizar esos derechos al tiempo que evitase restricciones posteriores de los mismos. La idea se conoce como la Licencia General Pública de GNU (GPL).

En 1985, Stallman creó la Free Software Foundation para proveer soportes logísticos, legales y financieros al proyecto GNU. La FSF también contrató programadores para contribuir a GNU, aunque una porción sustancial del desarrollo fue (y continúa siendo) producida por voluntarios. A medida que GNU ganaba renombre, negocios interesados comenzaron a contribuir al desarrollo o comercialización de productos GNU y el correspondiente soporte técnico. El más prominente y exitoso de ellos fue Cygnus Solutions, ahora parte de Red Hat.

1.4.1.1 Etimologia

GNU es un acrónimo recursivo que significa GNU No es Unix (GNU is Not Unix). En español, se recomienda pronunciarlo ñu como el antílope africano, por ello, el término mayoritariamente se deletrea (G-N-U) para su mejor comprensión.

1.4.1.2 Free Software Foundation

La Fundación para el Software Libre (Free Software Foundation) es una organización creada en Octubre de 1985 por Richard Matthew Stallman y otros entusiastas del Software Libre con el propósito de difundir este movimiento.

"La Fundación para el Software Libre (FSF) está dedicada a eliminar las restricciones sobre la copia, redistribución, entendimiento, y modificación de programas de computadoras. Con este objeto, promociona el desarrollo y uso del software libre en todas las áreas de la computación, pero muy particularmente, ayudando a desarrollar el sistema operativo GNU.

1.4.1.3 Licencia GPL

La Licencia Pública General de GNU o más conocida por su acronimo en inglés (General Public License) , esta es una licencia creada por la Free Software Foundation a mediados de los 80, y está orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

1.4.4 Licencia LGPL

La Licencia Pública General Reducida de GNU (Lesser General Public License) es una licencia de software creada por la Free Software Foundation. Los contratos de licencia de la mayor parte del software están diseñados para jugar con su libertad de compartir y modificar dicho software. En contraste, la "GNU General Public License" pretende garantizar su libertad de compartir y modificar el software "libre", esto es para asegurar que el software es libre para todos sus usuarios. Esta licencia pública general se aplica a la mayoría del software de la "FSF" o "Free Software Foundation" (Fundación para el Software Libre) y a cualquier otro programa de software cuyos autores así lo establecen. Algunos otros programas de software de la Free Software Foundation están cubiertos por la "LGPL Lesser General Public License" (Licencia pública general reducida), la cual puede aplicar a sus programas también.

Esta licencia se aplica a cualquier programa o trabajo que contenga una nota puesta por el propietario de los derechos del trabajo estableciendo que su trabajo puede ser distribuido bajo los términos de esta "GPL General Public License". El "Programa", utilizado en lo subsecuente, se refiere a cualquier programa o trabajo original, y el "trabajo basado en el Programa" significa ya sea el Programa o cualquier trabajo derivado del mismo bajo la ley de derechos de autor: es decir, un trabajo que contenga el Programa o alguna porción de él, ya sea íntegra o con modificaciones o traducciones a otros idiomas.

Otras actividades que no sean copia, distribución o modificación si están cubiertas en esta licencia y están fuera de su alcance. El acto de ejecutar el programa no está restringido, y la salida de información del programa está cubierta sólo si su contenido constituye un trabajo basado en el Programa (es independiente de si fue resultado de ejecutar el programa). Si esto es cierto o no depende de la función del programa.

El proyecto OpenOffice.org de Sun Microsystems emplea la LGPL.

1.4.2 El Proyecto Linux

La historia de Linux está fuertemente vinculada a la del proyecto GNU. El proyecto GNU, iniciado en 1983, tiene como objetivo el desarrollo de un sistema Unix completo compuesto enteramente de software libre. Hacia 1991, cuando la primera versión del núcleo Linux fue liberada, el proyecto GNU había producido varios de los componentes del sistema operativo, incluyendo un intérprete de comandos, una biblioteca C y un compilador, pero aún no contaba con el núcleo que permitiera completar el sistema operativo.

Entonces, el núcleo creado por Linus Torvalds, quien se encontraba por entonces estudiando en la Universidad de Helsinki, llenó el hueco final que el sistema operativo GNU exigía. Subsecuentemente, miles de programadores voluntarios alrededor del mundo han participado en el proyecto, mejorándolo continuamente y agregando mas lineas al código original.

Linux se refiere estrictamente al núcleo Linux, pero es comúnmente utilizado para describir al sistema operativo tipo Unix, que utiliza primordialmente filosofía y metodologías libres (también conocido como GNU/Linux) y que está formado mediante la combinación del núcleo Linux con las bibliotecas y herramientas del proyecto GNU y de muchos otros proyectos/grupos de software (libre o no libre).

Linux es usado ampliamente en servidores y supercomputadoras y cuenta con el respaldo de corporaciones como Dell, Hewlett-Packard, IBM, Novell, Oracle, Red Hat y Sun Microsystems.

Las variantes de estos sistemas Linux se denominan "distribuciones". Algunas son gratuitas y otras de subscripcion, algunas insertan software no libre y otras solo software libre.

Algunas de las distribuciones mas populares son:

	CentOS (Community ENTerprise Operating System) es un clon a nivel binario de la distribución Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser bajado y usado por el público, pero no es mantenido ni asistido por Red Hat. CentOS usa yum para bajar e instalar las actualizaciones, herramienta también utilizada por Fedora
	Red Hat es una empresa dedicada al software libre, y ademas es un importante proveedor, distribuidor y promotor de Linux. Red Hat fue fundada en 1995 y tiene su sede en Raleigh, Carolina del Norte con oficinas en todo el mundo. La compañía es mejor conocida por su sistema operativo Red Hat Enterprise Linux (RHEL), y más recientemente, a través de la adquisición de la empresa de código abierto JBoss que es un servidor de aplicaciones.
	Fedora es una distribución Linux patrocinada oficialmente por Red Hat. El Proyecto Fedora Linux desarrollaba paquetes extra para viejas distribuciones de Red Hat Linux (RHL 8, RHL 9, FC 1, FC 2), antes de convertirse en parte del Proyecto Fedora. Cuando la distribución Red Hat Linux quedó entre Red Hat Enterprise Linux y el Proyecto Fedora existente, los usuarios domésticos y de pequeñas empresas tuvieron incertidumbre acerca de qué hacer; Red Hat Professional Workstation se creó en este mismo momento con la intención de llenar el nicho que Red Hat Linux había ocupado una vez, pero con un futuro incierto. Esta opción cayó rápidamente para aquellos que no eran usuarios de Red Hat Linux en favor del Proyecto Fedora. Recientemente, la comunidad Fedora ha prosperado, y la distribución Fedora tiene la reputación de ser una distribución completamente abierta enfocada en la innovación y abierta al trabajo en grupo con las comunidades de Linux

	Debian es una comunidad conformada por desarrolladores y usuarios, que pretende crear y mantener un sistema operativo GNU basado en software libre pre compilado y empaquetado, en un formato sencillo para múltiples arquitecturas y en varios núcleos. Debian nace como una apuesta por separar en sus versiones el software libre del software no libre. El modelo de desarrollo del proyecto es ajeno a motivos empresariales o comerciales, siendo llevado adelante por los propios usuarios, aunque cuenta con el apoyo de varias empresas en forma de infraestructuras. Debian no vende directamente su software, lo pone a disposición de cualquiera en Internet, aunque sí permite a personas o empresas distribuir comercialmente este software mientras se respete su licencia.
	Ubuntu es una distribución Linux que ofrece un sistema operativo enfocado a computadoras de escritorio aunque también proporciona soporte para servidores. Es una de las más importantes distribuciones de GNU/Linux a nivel mundial. Basada en Debian GNU/Linux, Ubuntu concentra su objetivo en la facilidad y libertad de uso, la facilidad de instalación y los lanzamientos regulares (cada 6 meses). Ubuntu es patrocinado por Canonical Ltd., una empresa privada fundada y financiada por el empresario sudafricano Mark Shuttleworth. El nombre de la distribución proviene del concepto zulú y xhosa de ubuntu, que significa "humanidad hacia otros" o "yo soy porque nosotros somos".
	OpenSuse es el nombre de la distribución y proyecto libre auspiciado por Novell y AMD para el desarrollo y mantenimiento de un sistema operativo basado en Linux. Luego de adquirir SUSE Linux en enero de 2004, Novell decidió lanzar SUSE Linux Professional como un proyecto completamente de código abierto, involucrando a la comunidad en el proceso de desarrollo. La versión inicial fue una versión beta de SUSE Linux 10.0

1.4.2.1 El Kernel Linux

Actualmente Linux es un núcleo monolítico híbrido. Los controladores de dispositivos y las extensiones del núcleo normalmente se ejecutan en un espacio privilegiado conocido como anillo 0, con acceso irrestricto al hardware, aunque algunos se ejecutan en espacio de usuario. A diferencia de los núcleos monolíticos tradicionales, los controladores de dispositivos y las extensiones al sistema operativo se pueden cargar y descargar fácilmente como módulos, mientras el sistema continúa funcionando sin interrupciones. También, a diferencia de los núcleos monolíticos tradicionales, los controladores pueden ser prevolcados (detenidos momentáneamente por actividades más importantes) bajo ciertas condiciones. Esta habilidad fue agregada para gestionar correctamente interrupciones de hardware, y para mejorar el soporte de Multiprocesamiento Simétrico.

Un sistema operativo con núcleo monolítico concentra todas las funcionalidades posibles (planificación, sistema de archivos, redes, controladores de dispositivos, gestión de memoria, etc) dentro de un gran programa. El mismo puede tener un tamaño considerable, y deberá ser recompilado por completo al añadir una nueva funcionalidad. Todos los componentes funcionales del núcleo tienen acceso a todas sus estructuras de datos internas y a sus rutinas. Un error en una rutina puede propagarse a todo el núcleo. Todos sus componentes se encuentran integrados en un único programa que ejecuta en un único espacio de direcciones. En este tipo de sistemas, todas las funciones que ofrece el sistema operativo se ejecutan en modo supervisor.

El hecho de que Linux no fuera desarrollado siguiendo el diseño de un micronúcleo (diseño que, en aquella época, era considerado el más apropiado para un núcleo por muchos teóricos informáticos) fue asunto de una famosa y acalorada discusión entre Linus Torvalds y Andy Tanenbaum.

A diferencia de los núcleos monolíticos tradicionales, los controladores de dispositivos son fácilmente configurables como módulos del núcleo cargables, y se pueden cargar o descargar mientras se está ejecutando el sistema.

1.5 ¿Que es el Software Libre u OpenSource?

Se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software; de modo más preciso, se refiere a cuatro libertades de los usuarios del software:

1. La libertad de usar el programa, con cualquier propósito
2. Estudiar el funcionamiento de la aplicación y adaptarlo a las necesidades
3. Distribuir copias, con lo que puede ayudar a otros.
4. Mejorar el programa y hacer públicas las mejoras, de modo que toda la comunidad se beneficie.

Otro de los requisitos fundamentales para considerar a una aplicación como Software Libre es el acceso al código fuente de la aplicación.

1.5.1 Que es el Freeware y Shareware

1.5.1.1 Freeware

El término en inglés freeware define un tipo de software que se distribuye sin costo y por tiempo ilimitado. A veces se incluye el código fuente, pero no es lo usual.

El freeware suele incluir una licencia de uso, que permite su redistribución pero con algunas restricciones, como no modificar la aplicación en sí, ni venderla, y dar cuenta de su autor. También puede desautorizar el uso en una compañía con fines comerciales o en una entidad gubernamental.

1.5.1.2 Shareware

Se denomina Shareware a una modalidad de distribución de software el cual permite al usuario evaluar de forma gratuita el producto, por un lapso de tiempo, aunque también las limitaciones pueden estar en algunas de las formas de uso o las capacidades finales.

Para adquirir una licencia de software que permite el uso del software de manera completa se requiere de un pago.

No debe confundirse el shareware con el sistema freeware que indica que un software es totalmente gratuito, si bien es cierto que el primero se inspira y tiene sus raíces en el segundo. Tampoco debe confundirse el hecho de que un software sea Shareware o freeware con el hecho de que sea de código abierto, ya que esto último depende de la disponibilidad o no del código fuente.

1.5.1.3 Ventajas del OpenSource contra el Freware, Shareware y Software privativo

- FLEXIBILIDAD. Si el código fuente está disponible, los desarrolladores pueden aprender y modificar los programas a su antojo, adaptándolo para realizar tareas específicas. Además, se produce un flujo constante de ideas que mejora la calidad de los programas.
- FIABILIDAD Y SEGURIDAD. Con varios programadores a la vez mirándose el mismo trabajo, los errores se detectan y corrigen antes, por lo que el producto resultante es más fiable y eficaz que el comercial.

- RAPIDEZ DE DESARROLLO. Las actualizaciones y ajustes se realizan a través de una comunicación constante vía Internet. Menores tiempos de desarrollo debido a la amplia disponibilidad de herramientas y librerías.
- RELACIÓN CON EL USUARIO. El programador se acerca mucho más a las necesidad real de su cliente, y puede crear un producto específico para él.
- LIBRE. Es de libre distribución, cualquier persona puede regalarlo, venderlo o prestarlo.
- COMBATE EFECTIVAMENTE LA PIRATERÍA DE SOFTWARE.
- AHORRO EN LICENCIAS.-No se tienen que pagar ningún tipo de licencias para poder usarlo, por lo que hace al Software Libre una perfecta alternativa para el sector Educativo Publico de País

1.6 El Estándar POSIX

POSIX es el acrónimo de Portable Operating System Interface; la X viene de UNIX. El término POSIX fue sugerido por Richard Stallman en respuesta a la demanda de la IEEE, que buscaba un nombre fácil de recordar. Una traducción aproximada del acrónimo podría ser "Interfaz de Sistema Operativo Portátil basado en UNIX".

Estándar Posix es una familia de estándares de llamadas al sistema operativo definidos por el IEEE y especificados formalmente en el IEEE 1003. Persiguen generalizar las interfaces de los sistemas operativos (Linux o uNIX) para que una misma aplicación pueda ejecutarse en distintas plataformas (Arquitecturas). Estos estándares surgieron de un proyecto de normalización de las API y describen un conjunto de interfaces de aplicación adaptables a una gran variedad de implementaciones de sistemas operativos.

1.7 Linux Standard Base

La Base Estándar para Linux (Linux Standard Base, abreviado LSB), es un proyecto conjunto de varias Distribuciones de Linux bajo la estructura organizativa del Free Standards Group con el objeto de crear y normalizar la estructura interna de los sistemas operativos derivados de Linux. La LSB está basada en la Especificación POSIX, la Especificación Única de UNIX (Single UNIX Specification) y en varios otros estándares abiertos, aunque extiende éstos en ciertas áreas.

De acuerdo a la definición de la propia LSB:

El objetivo de la LSB es desarrollar y promover un conjunto de estándares que aumentarán la compatibilidad entre las distribuciones de Linux y permitirán que los programas de aplicación puedan ser ejecutados en cualquier sistema que se adhiera a ella. Además, la LSB ayudará a coordinar esfuerzos tendentes a reclutar productores y proveedores de programas que creen productos originales para Linux o adaptaciones de productos existentes.

Mediante un proceso de certificación es posible obtener la conformidad a la LSB de un producto. Dicha certificación la lleva a cabo el Open Group en colaboración con el Free Standards Group (Grupo de Estándares Libres).

Como ejemplo, la LSB especifica: librerías estándar, un conjunto de órdenes y utilerías que extienden el estándar POSIX, la estructura jerárquica del sistema de archivos, los niveles de ejecución, y varias extensiones al sistema gráfico X Window.

1.8 El Estándar FSH

El **File System Hierarchy Standard** (Estándar de Jerarquía de Sistema de Ficheros) define los directorios principales y sus contenidos en el sistema operativo GNU/Linux . Se diseñó originalmente en 1994 para estandarizar el sistema de archivos de las distribuciones GNU/Linux, la cual tiene su base en la organización de directorios de los sistemas Unix.

El proceso de desarrollo de una jerarquía de sistema de archivos estándar comenzó en agosto de 1993 con un

esfuerzo enfocado a reestructurar el archivo y la estructura Linux. El FSSTND (Estándar del Sistema de Archivos), un estándar de la jerarquía del sistema de archivos específico del sistema operativo Linux, fue liberado el 14 de febrero de 1994. Revisiones posteriores fueron liberadas el 9 de octubre de 1994 y el 28 de marzo de 1995.

A principios de 1996, el objetivo de desarrollar una versión más comprensiva del FSSTND para direccionar no sólo a Linux, sino a otros sistemas derivados de UNIX, fue adoptado con la ayuda de miembros de la comunidad de desarrollo de BSD. Por consiguiente, un concentrado esfuerzo fue realizado para centrarse en hechos que fueran generales para los sistemas derivados de UNIX. En reconocimiento a esta amplitud del alcance, el nombre del estándar fue cambiado Estándar de Jerarquía del Sistema de Archivos, o FHS para abreviar.

El FHS es mantenido por el Grupo de Estándares Libres (Free Standards Group), una organización no lucrativa que consiste en los principales vendedores de software y hardware, tales como: HP, Red Hat, IBM y Dell.

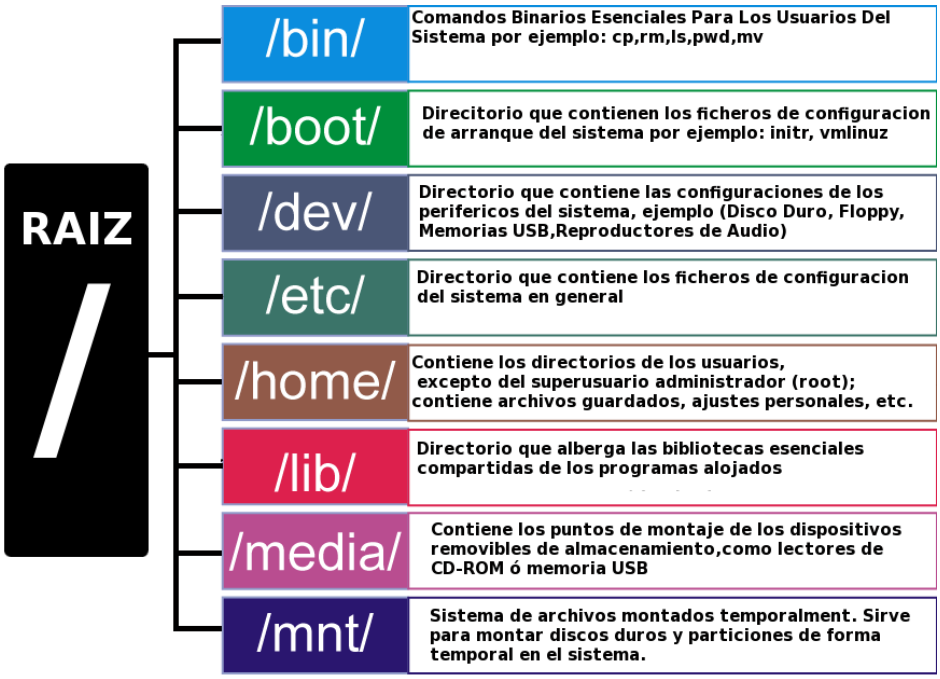
De todos modos, la gran mayoría de las distribuciones Linux, incluyendo aquellas desarrolladas por los miembros del Grupo de Estándares Libres (Free Standars Group), no siguen este estándar propuesto. En particular, caminos (path), expresamente creados por los redactores del FHS, como por ejemplo /srv/, no es usado extensamente. Algunos sistemas Linux rechazan el FHS en favor de un enfoque diferente, como es el caso de GoboLinux.

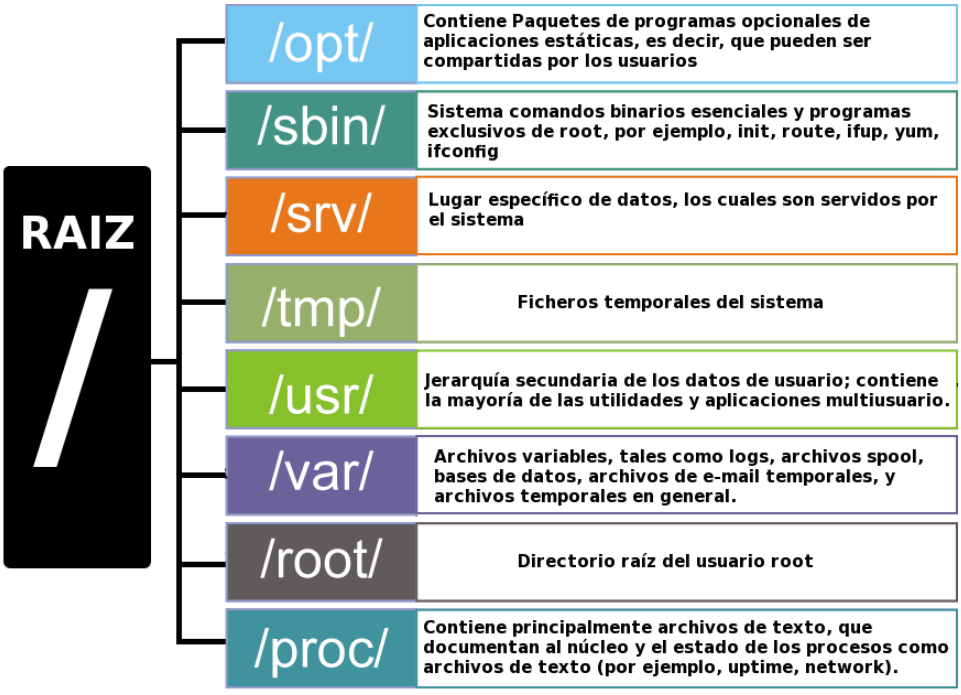
Desde que FHS comenzó como una iniciativa Linux, otros sistemas operativos derivados de UNIX, generalmente la han ignorado en favor de sus propios sistemas, los cuales a veces varían ampliamente. Por ejemplo, Mac OSX usa nombre como /Library, /Applications/, y /Users/ junto con la jerarquía de directorios tradicional de UNIX.

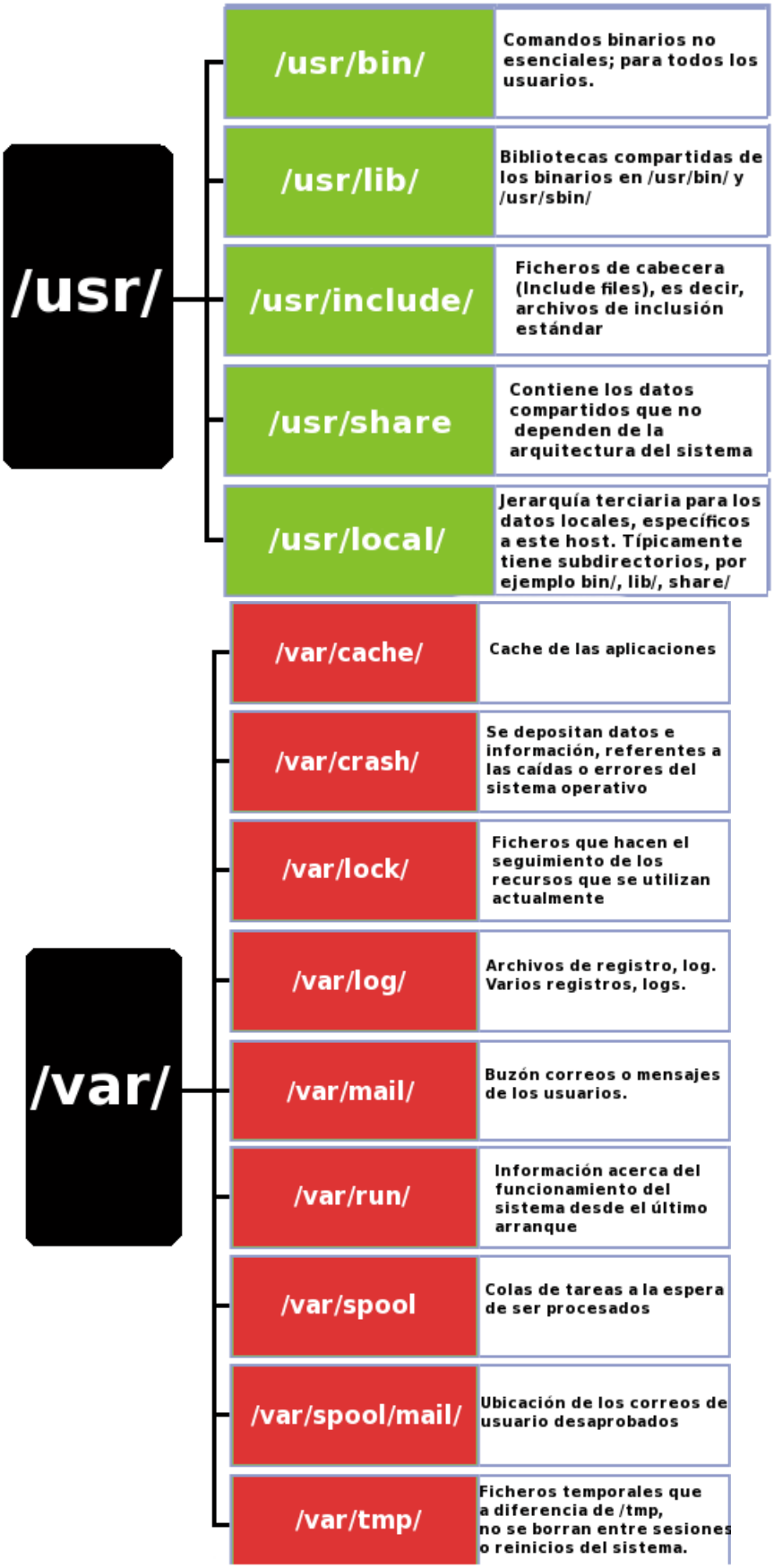
1.8.1 Estructura de los Directorios en Linux

En el sistema de ficheros de Linux, existen varias subjerarquías de directorios que poseen múltiples y diferentes funciones de almacenamiento y organización en todo el sistema. Estos directorios pueden clasificarse en:

- Estáticos: Contiene archivos que no cambian sin la intervención del administrador (root), sin embargo, pueden ser leídos por cualquier otro usuario. (/bin, /sbin, /opt, /boot, /usr/bin...)
- Dinámicos: Contiene archivos que son cambiantes, y pueden leerse y escribirse (algunos sólo por su respectivo usuario y el root).Para estos directorios, es recomendable una copia de seguridad con frecuencia, o mejor aún, deberían ser montados en una partición aparte en el mismo disco, como por ejemplo, montar el directorio /home en otra partición del mismo disco, independiente de la partición principal del sistema; de esta forma, puede repararse el sistema sin afectar o borrar los documentos de los usuarios. (/var/mail, /var/spool, /var/run, /var/lock, /home...)
- Compartidos: Contiene archivos que se pueden encontrar en un ordenador y utilizarse en otro, o incluso compartirse entre usuarios.
- Restringidos: Contiene ficheros que no se pueden compartir, solo son modificables por el administrador. (/etc, /boot, /var/run, /var/lock)


RAIZ
/
/bin/
Comandos Binarios Esenciales Para Los Usuarios Del Sistema por ejemplo: cp,rm,ls,pwd,mv
/boot/
Direcitorio que contienen los ficheros de configuracion de arranque del sistema por ejemplo: initr, vmlinuz
/dev/
Directorio que contiene las configuraciones de los perifericos del sistema, ejemplo (Disco Duro, Floppy, Memorias USB,Reproductores de Audio)
/etc/
Directorio que contiene los ficheros de configuracion del sistema en general
/home/
Contiene los directorios de los usuarios, excepto del superusuario administrador (root); contiene archivos guardados, ajustes personales, etc.
/lib/
Directorio que alberga las bibliotecas esenciales compartidas de los programas alojados
/media/
Contiene los puntos de montaje de los dispositivos removibles de almacenamiento,como lectores de CD-ROM ó memoria USB
/mnt/
Sistema de archivos montados temporalment. Sirve para montar discos duros y particiones de forma temporal en el sistema.


RAIZ
/
/opt/
Contiene Paquetes de programas opcionales de aplicaciones estáticas, es decir, que pueden ser compartidas por los usuarios
/sbin/
Sistema comandos binarios esenciales y programas exclusivos de root, por ejemplo, init, route, ifup, yum, ifconfig
/srv/
Lugar específico de datos, los cuales son servidos por el sistema
/tmp/
Ficheros temporales del sistema
/usr/
Jerarquía secundaria de los datos de usuario; contiene la mayoría de las utilidades y aplicaciones multiusuario.
/var/
Archivos variables, tales como logs, archivos spool, bases de datos, archivos de e-mail temporales, y archivos temporales en general.
/root/
Directorio raíz del usuario root
/proc/
Contiene principalmente archivos de texto, que documentan al núcleo y el estado de los procesos como archivos de texto (por ejemplo, uptime, network).


/usr/
/usr/bin/
Comandos binarios no esenciales; para todos los usuarios.
/usr/lib/
Bibliotecas compartidas de los binarios en /usr/bin/ y /usr/sbin/
/usr/include/
Ficheros de cabecera (Include files), es decir, archivos de inclusión estándar
/usr/share
Contiene los datos compartidos que no dependen de la arquitectura del sistema
/usr/local/
Jerarquía terciaria para los datos locales, específicos a este host. Típicamente tiene subdirectorios, por ejemplo bin/, lib/, share/
/var/
/var/cache/
Cache de las aplicaciones
/var/crash/
Se depositan datos e información, referentes a las caídas o errores del sistema operativo
/var/lock/
Ficheros que hacen el seguimiento de los recursos que se utilizan actualmente
/var/log/
Archivos de registro, log. Varios registros, logs.
/var/mail/
Buzón correos o mensajes de los usuarios.
/var/run/
Información acerca del funcionamiento del sistema desde el último arranque
/var/spool
Colas de tareas a la espera de ser procesados
/var/spool/mail/
Ubicación de los correos de usuario desaprobados
/var/tmp/
Ficheros temporales que a diferencia de /tmp, no se borran entre sesiones o reinicios del sistema.

1.9 ¿Que es Live CD?

Un Live CD o Live DVD, más genéricamente Live Distro, es un sistema operativo (normalmente acompañado de un conjunto de aplicaciones) almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de ficheros.

Algunos Live CD incluyen una herramienta que permite instalarlos en el disco duro. Otra característica es que por lo general no se efectúan cambios en la computadora utilizada, aunque algunos pueden almacenar preferencias si así se desea.

Para usar un Live CD es necesario obtener uno (muchos de ellos distribuyen libremente una imagen ISO que puede bajarse de Internet y grabarse en disco) y configurar la computadora para que arranque desde la unidad lectora, reiniciando luego la computadora con el disco en la lectora, con lo que el Live CD se iniciará automáticamente.

1.9.1 Características

La mayoría usa un sistema operativo basado en el núcleo Linux, pero también se usan otros sistemas como BeOS, FreeBSD, Minix, Solaris, OS/2 o incluso Microsoft Windows (sin embargo, distribuir un Live CD de éste último es ilegal).

El primer Live CD Linux fue Yggdrasil Linux en 1995,aunque fue poco exitosa. Posteriormente surgió DemoLinux (año 2000).

El auge de esta modalidad de Linux se inició alrededor del año 2003 con la distribución alemana de Knoppix, basada, a su vez, en la distribución de software Debian. Una de las mejoras de este método fue la compresión cloop, esto permitió sobrepasar los 650-700 MB del CD (se usaba el driver loop) y lograr introducir hasta 2 GB.

Uno de los mayores inconvenientes de este sistema es el requerimiento de una gran cantidad de memoria RAM (256 son más que suficientes y hay distribuciones que funcionan perfectamente en 128), una parte para su uso habitual y otra para funcionar como el disco virtual del sistema. En el arranque, se le pueden dar distintos parámetros para adaptar el sistema al computador, como la resolución de pantalla o para activar o desactivar la búsqueda automática de determinado hardware.

1.10 Identificando los escritorios en linux

El escritorio Linux, refiere al uso que se le da al sistema operativo Linux, al ser instalado en una computadora personal. El termino esta destinado a clarificar el uso personal del computador de otros roles, como por ejemplo, usar Linux en un servidor. Los dos roles son similares en el núcleo, porque los dos están basados en el Kernel Linux. El escritorio linux generalmente tendrá instalado por defecto paquetes destinados al "usuario final". Algunas distribuciones Linux se han centrado específicamente en el rol de escritorio. Otras incluyen un conjunto de todas las aplicaciones para la plataforma. En ese caso, el usuario puede seleccionar entre "escritorio" o "servidor" al momento de ser instalado el sistema operativo.

A continuación hablaremos de los dos proyectos de escritorio Linux mas importantes

1.10.1 Gnome

GNOME es un entorno de escritorio para sistemas operativos de tipo Unix bajo tecnología X Window. Forma parte oficial del proyecto GNU. Nació como una alternativa a KDE.

Se encuentra disponible actualmente en 48 idiomas en su última versión

1.10.1.1 Objetivo

El Proyecto GNOME pone un gran énfasis en la simplicidad, usabilidad y en hacer que las cosas funcionen. Otros objetivos del proyecto son:

- La libertad para crear un entorno de escritorio que siempre tendrá el código fuente disponible para reutilizarse bajo una licencia de software libre.
- El aseguramiento de la accesibilidad, de modo que pueda ser utilizado por cualquiera, sin importar sus conocimientos técnicos y discapacidad física.
- Hacer que este disponible en muchos idiomas. En el momento está siendo traducido a más de 100 idiomas.
- Un ciclo regular de liberaciones y una estructura de comunidad disciplinada.

1.10.1.2 Historia

El proyecto GNOME (GNU Network Object Model Environment) surgió en agosto de 1997 como proyecto liderado por los mexicanos Miguel de Icaza y Federico Mena para crear un entorno de escritorio completamente libre para sistemas operativos libres, en especial para GNU/Linux. Desde el principio, el objetivo principal de GNOME ha sido proporcionar un conjunto de aplicaciones amigables y un escritorio fácil de utilizar. GNOME también es una palabra del idioma inglés que significa gnomo.

En esos momentos existía otro proyecto anterior con los mismos objetivos, pero con diferentes medios: KDE. Los primeros desarrolladores de GNOME criticaban a dicho proyecto por basarse en la biblioteca de controles gráficos Qt, cuya licencia (QPL), aunque libre, no era compatible inicialmente con la licencia GPL de la FSF.

Años más tarde los problemas de licencia de Qt se han resuelto y estas críticas han cesado. Sin embargo, los dos proyectos siguen rumbos tecnológicos distintos y se hacen una competencia amigable.

Como con la mayoría de los programas GNU, GNOME ha sido diseñado para ejecutarse en toda la gama de sistemas operativos de tipo Unix con X Window, y especialmente pensado para GNU/Linux. Desde sus inicios se ha utilizado la biblioteca de controles gráficos GTK, originalmente desarrollada para el programa The GIMP.

A medida que el proyecto ha ido progresando en los últimos años, los objetivos del mismo se han extendido para tratar una serie de problemas en la infraestructura Unix existente.

Actualmente el proyecto evoluciona bajo amparo de la Fundación GNOME.

Captura de Gnome 2.24

1.10.2 KDE

De acuerdo con su página web, KDE es un entorno de escritorio contemporáneo para estaciones de trabajo Unix. KDE llena la necesidad de un escritorio amigable para estaciones de trabajo Unix, similar a los escritorios de MacOS o Windows

La “K”, originariamente, representaba la palabra “Kool” , pero su significado fue abandonado más tarde. Actualmente significa simplemente “K”, la letra inmediatamente anterior a la «L» (inicial de Linux) en el alfabeto.

1.10.2.1 Objetivo

KDE se basa en el principio de la personalización. Todos los componentes de KDE pueden ser configurados en mayor o menor medida por el usuario. Las opciones más comunes son accesibles en su mayoría desde menús y diálogos de configuración. Los usuarios avanzados pueden optar por editar los archivos de configuración manualmente, obteniendo en algunos casos un mayor control sobre el comportamiento del sistema.

La apariencia de KDE es configurable en varios niveles. Tanto el gestor de ventanas (llamado Kwin) como los controles (botones, menús, etc.) utilizan "estilos" intercambiables, que definen cada aspecto de su apariencia. Es por este motivo que KDE no mantiene una única apariencia entre versiones, sino que se opta por aquella más ampliamente aceptada en el momento de cada nuevo lanzamiento.

La intención del proyecto KDE es la de crear un entorno de escritorio que no se comporte de un modo predefinido, sino que permita al usuario adecuar el sistema a su gusto y comodidad. Esto no impide que KDE resulte fácil de usar para nuevos usuarios, detalle al que no se resta importancia.

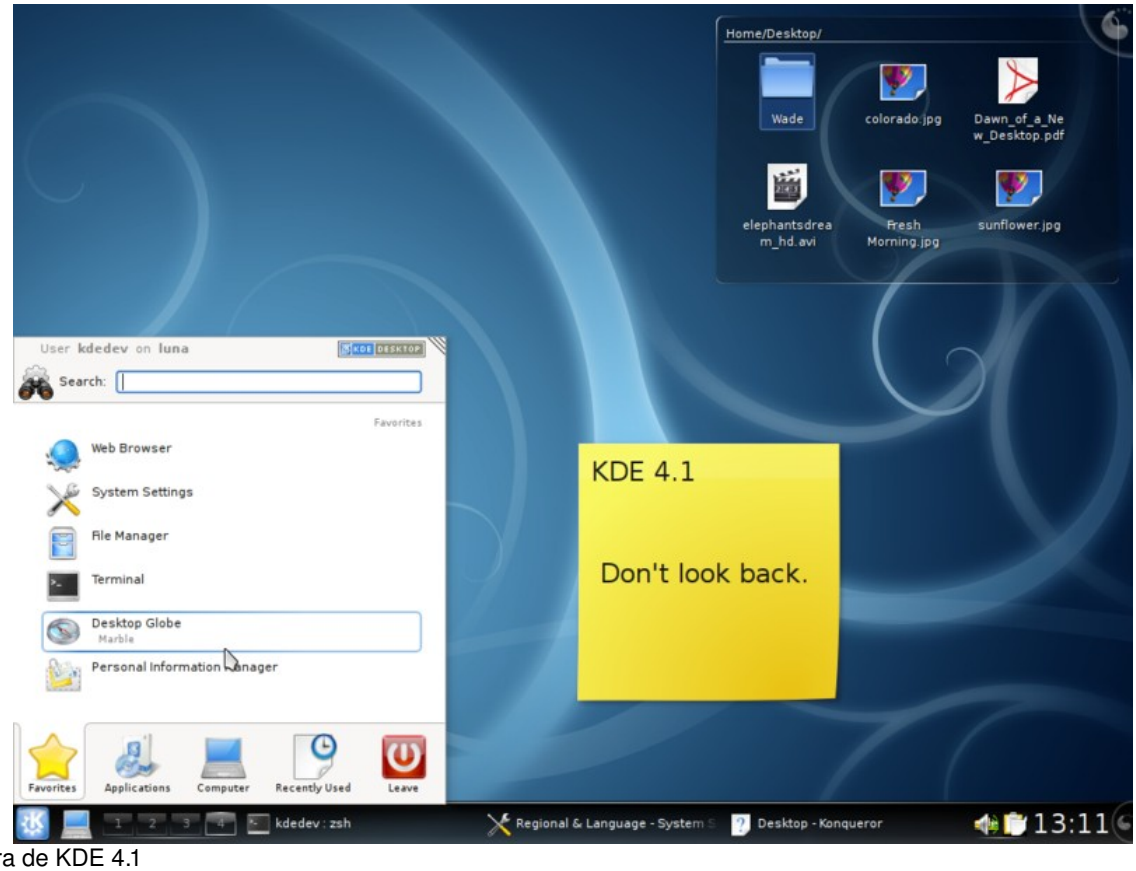
Algunas personas externas al proyecto a menudo critican su similitud con los escritorios Windows y su falta de innovación. Esta observación, sin embargo, recae sobre la selección de parámetros predefinidos del sistema, a menudo orientada a facilitar la integración de nuevos usuarios, acostumbrados en su mayoría a trabajar con Windows. Pese a todo esta critica no tiene fundamento alguno, ya que debido a que KDE tiene una alta capacidad de configuración se pueden realizar efectos de escritorio muy innovadores (inclusive algunos son comparables con Compiz o Beryl).

1.10.2.2 Historia

El proyecto fue iniciado en octubre de 1996 por el programador alemán Matthias Ettrich, quien buscaba crear una interfaz gráfica unificada para sistemas Unix. En sus inicios imitó a CDE (Common Desktop Environment), un entorno de escritorio utilizado por varios Unix.

Dos factores llevaron a la creación del proyecto alternativo GNOME en 1997: la elección de la biblioteca Qt, que por aquel entonces poseía una licencia incompatible con la GPL de GNU, aunque libre: la QPL, y en menor medida la importancia del lenguaje C++ para el desarrollo de KDE. La rivalidad actual entre ambos proyectos se considera beneficiosa generalmente y existe, de hecho, una constante cooperación e inspiración mutua.

- KDE 1: Al año siguiente, se publicó KDE 1.0. Esta versión contenía un panel (barra de tareas y lanzador de aplicaciones), un escritorio sobre el cual dejar iconos, un administrador de archivos (Kfm) y un gran número de utilidades.
- KDE 2: KDE 2.0, lanzado en el año 2000, fue reescrito casi por completo. Esta versión incluía Konqueror (un navegador web y gestor de archivos) además de muchas nuevas tecnologías con el objetivo de mejorar la integración entre aplicaciones. En esta versión mejoró parcialmente el aspecto visual.
- KDE 3: KDE 3.0 fue publicado en el año 2002, y es la evolución de KDE 2. El aspecto de la interfaz no varió hasta KDE 3.1, en el que consta una importante mejora referente al tema visual: Keramik es incluido como nuevo tema por omisión junto con el conjunto de iconos Crystal GT y el antialisado de fuentes. En KDE 3.2 Crystal GT fue reemplazado por Crystal SVG. En KDE 3.4 Keramik fue reemplazado por Plastik.



Captura de KDE 4.1

1.13 XFCE

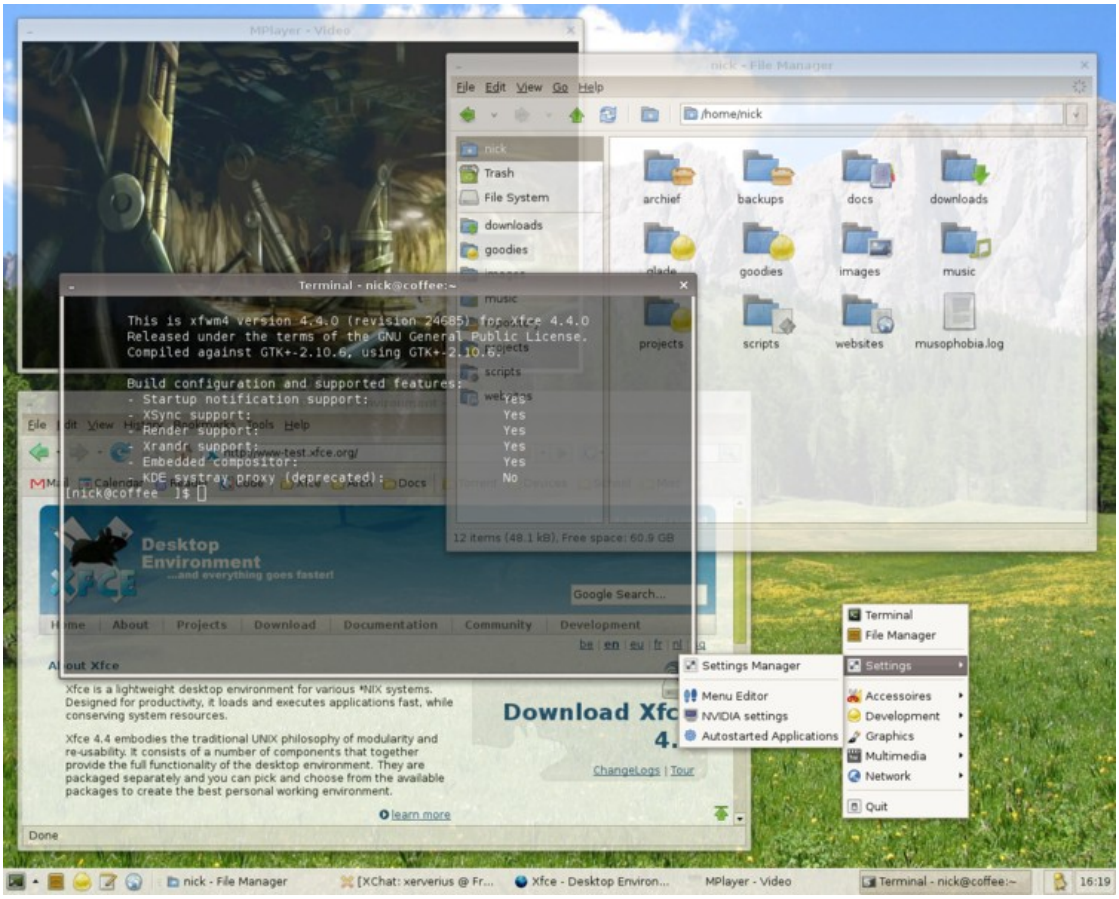
Xfce (éxfeis) es un entorno de escritorio ligero para sistemas tipo Unix como Linux, BSD, Solaris y derivados. Se configura íntegramente con el ratón o mouse. Su creador, Olivier Fourdan, dice de él: “Diseñado para la productividad, las aplicaciones se cargan y se ejecutan rápidamente, mientras conserva recursos de sistema”

Xfce también provee el marco de trabajo para el desarrollo de aplicaciones. Además de Xfce mismo, hay otros programas que también utilizan las bibliotecas de Xfce, como el editor de texto Mousepad, el reproductor multimedia Xfmedia o el emulador de consola Terminal.

Xfce está basado en la biblioteca GTK+ 2.x y utiliza el gestor de ventanas Xfwm. Xfce se parecía en sus inicios al entorno de escritorio CDE, pero fue alejándose notablemente debido a que fue reprogramado nuevamente desde cero (ya lo había hecho entre las versiones 2.x y 3.x), y a diferencia de sus anteriores versiones, ahora cuenta con un sistema modular pudiendo gestionar un sistema de tipo multihead de manera bastante sencilla, y sigue todos los estándares establecidos por Freedesktop.org.

El nombre Xfce originalmente provenía de XForms Common Enviroment, pero debido a los grandes cambios en el código, ya no usa el kit de herramientas de XForms, como originalmente lo hacía. El nombre sobrevivió, pero ya no se indica como XFce sino Xfce. Los desarrolladores están de acuerdo en que el nombre carece de significado actualmente, aunque se le suele desglosar como X Free Choresterol Environment (entorno X libre de colesterol) en referencia al poco consumo de memoria que realiza y a la velocidad con que se ejecuta al no tener elementos superfluos a diferencia de otros entornos de escritorio más grandes.

Thunar es el nuevo gestor de archivos predeterminado para Xfce desde la versión 4.4. Es similar a Nautilus y está diseñado para una máxima velocidad y un mínimo consumo de memoria. Xfce también posee un gestor de archivos comprimidos llamado Xarchiver.



Captura de XFCE 4.4

1.14 Enlightenment

Enlightenment, también conocido simplemente como E, es un gestor de ventanas ligero para UNIX y GNU/Linux. Uno de sus objetivos es llegar a ser un entorno de escritorio completo. Es muy configurable y muy atractivo visualmente. Durante un tiempo fue el gestor de ventanas de GNOME.

La última versión estable es la 0.16.8.6 (también llamada DR16). El siguiente lanzamiento importante será la versión 0.17 (DR17) que está actualmente en fase de desarrollo y se basa en las nuevas Enlightenment Foundation Libraries (EFL). DR17 no está basado en DR16 sino que ha sido reescrito totalmente.

1.14.1 Características actuales de la versión 0.17

DR17 está en fase desarrollo en este momento, pero ciertas características del núcleo ya están disponibles:

- Soporte de temas mediante un sistema de menús y una interfaz de cambio de temas en línea de comandos.
- La parrilla de escritorios virtuales.
- Diseño modular - puede cargar módulos externos desde un paquete separado de 'e-módulos'. Los módulos actuales incluyen un paginador de escritorios, 'iBar', un lanzador de aplicaciones animado, un módulo de sombreado de ventanas, notas de escritorio, un reloj (analógico o digital) y un monitor de carga de la batería.
- Fondos de escritorio animados, ítems de menú, ítems de iBar y widgets de escritorio son posibles.
- Ajustes de sombreado de ventanas, iconizado, maximizado y pegado.
- Combinaciones de teclas personalizables disponibles.
- Soporte para internacionalización.

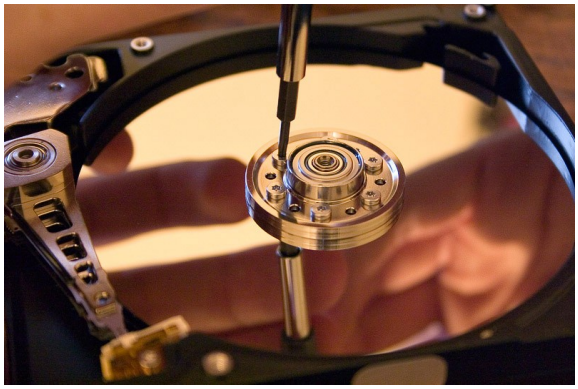
Captura de Enlightenment 0.17

Índice de contenido

Información de Derechos reservados de esta publicación.

Tema 2. Consideraciones Previas a la Instalación

2.1 Discos Duros



Un disco duro es un dispositivo de almacenamiento masivo de datos que a su vez también puede tener instalado algún Sistema Operativo, así mismo funge como memoria no volátil, es decir, cuando por alguna razón se interrumpe la energía eléctrica de nuestra casa u oficina la información anidada en el mismo se almacena de manera correcta, salvo algunas excepciones, como por ejemplo cuando se trabaja en tiempo real con el disco duro y no se guardan con anticipación dichos cambios.

Un ejemplo de memoria volátil es la memoria RAM (Random Access Memory), ya que este tipo de memoria solo almacena la información de manera temporal y es borrada nuevamente cuando se interrumpe la energía eléctrica de la computadora.

Un disco duro (Hard Disk) emplea un sistema de grabación magnética el cual es aplicado a una una serie de platos metálicos apilados girando a gran velocidad. Sobre estos platos se sitúan los cabezales encargados de leer o escribir los impulsos magnéticos.

Existen distintos tipos de interfaces y entre las mas comunes se encuentran las siguientes: Integrated Drive Electronics (**IDE**, también llamado **ATA**) , **SCSI** generalmente usado en servidores, **SATA**, este último estandarizado en el año 2004 y los mas recientes, los discos duros SAS , de los cuales hablaremos mas adelante.

2.1.1 Tipos de Discos Duros

Como anteriormente mencionamos, existen 4 principales tipos de discos duros:

1. Discos Duros IDE-ATA o PATA
2. Discos Duros SATA
3. Discos Duros SCSI
4. Discos Duros SAS

A continuación daremos una breve explicación sobre cada uno de ellos.

2.1.1.1 Discos Duros IDE-ATA

Los discos duros con esta denominación hacen uso de una interfaz llamada IDE(Integrated Device Electronics) ATA(Advanced Technology Attachment) que es la encargada de comunicar al Disco Duro con la tarjeta madre.

El estándar IDE-ATA fue diseñado originalmente para conectar discos duros; sin embargo, se desarrolló una extensión llamada ATAPI que permite interconectar otros periféricos de almacenamiento como unidades de CD-ROM o unidades de DVD-ROM en una interfaz IDE-ATA.

Habitualmente, un disco duro IDE-ATA puede estar configurado de 3 maneras diferentes, las cuales son:

- **Maestro o master.-** Los discos duros con esta configuración indican a la tarjeta madre que el debe ser el primero en ser cargado.

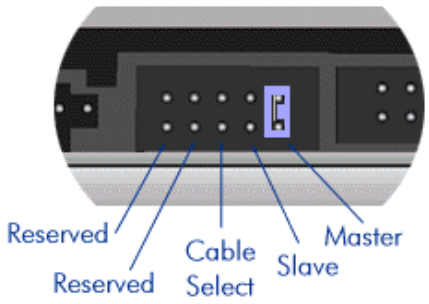
- **Esclavo o slave.-** Los discos duros con este tipo de configuración no son tomados en cuenta al momento de arrancar el sistema por lo que el disco duro maestro puede disponer de los demás discos duros configurados como discos slave
- **Selección por cable o cable select.-** El dispositivo será maestro o esclavo en función de su posición en el cable. Si hay otro dispositivo, también debe estar configurado como cable select. Si el dispositivo es el único en el cable, debe estar situado en la posición de maestro. Para distinguir el conector en el que se conectará el primer bus Ide (Ide 1) se utilizan colores distintos.

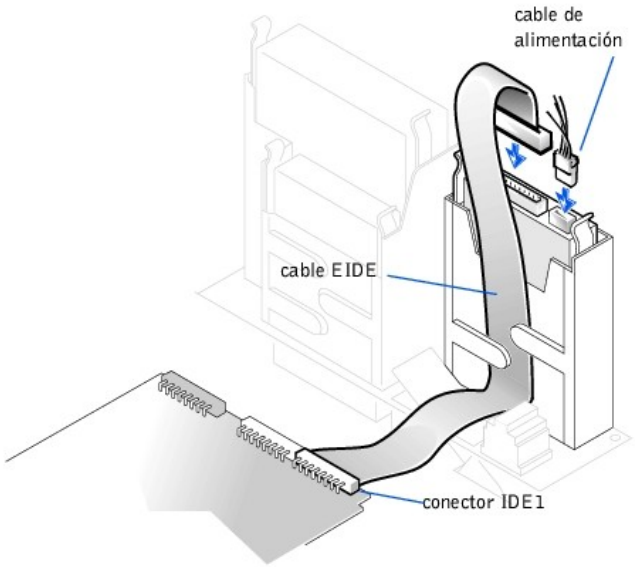
Este diseño IDE-ATA (dos dispositivos a un bus) tiene el inconveniente de que mientras se accede a un dispositivo el otro dispositivo del mismo conector IDE no se puede usar.

Este inconveniente está resuelto en discos duros como los SATA y en SCSI, que pueden usar dos dispositivos por canal.

Los discos IDE están mucho más extendidos que los SCSI debido a su precio mucho más bajo. El rendimiento de IDE es menor que SCSI pero se están reduciendo las diferencias.

A continuación veremos un diagrama de como tiene que ser conectado un disco duro IDE-ATA así como la localización de los pines que nos proporciona la opción de trabajar con las tres configuraciones posibles para un disco duro IDE-ATA:





2.1.1.2 Discos Duros SATA

Los discos duros con esta denominación hacen uso de una interfaz llamada Serial Advanced Technology Attachment que es la encargada de comunicar al Disco Duro con la tarjeta madre.

Estos discos duros sustituyen a los tradicionales IDE-ATA, ademas de que proporciona mayores velocidades, mejor aprovechamiento cuando hay varios discos, mayor longitud del cable de transmisión de datos y capacidad para conectar discos en caliente (con la computadora encendida).

El estándar Serial ATA se basa en una comunicación en serie. Se utiliza una ruta de datos para transmitir los datos y otra ruta para transmitir las confirmaciones de recepción. En cada una de estas rutas, los datos se transmiten mediante el modo de transmisión LVDS (Señal diferencial de bajo voltaje) que consiste en transferir una señal a un hilo y su contrapartida a un segundo hilo para permitir que el destinatario recree la señal por diferencia. Los datos de control se transmiten por la misma ruta que los datos mediante una secuencia específica de bits que los distingue.

Por lo tanto, la comunicación requiere de dos rutas de transmisión, cada una de las cuales está compuesta por dos hilos, con un total de cuatro hilos utilizados para la transmisión.

2.1.1.2.1 Conectores de Serial ATA

El cable utilizado por el estándar ATA Serial es un cable redondeado que contiene 7 hilos con un conector de 8 mm en su extremo:

Tres hilos tienen conexión a tierra y dos pares se utilizan para la transmisión de datos.

El conector de la fuente de alimentación también es diferente: comprende 15 clavijas que alimentan al periférico con una potencia de 3,3 V, 5 V o 12 V y tiene una apariencia similar al conector de datos:

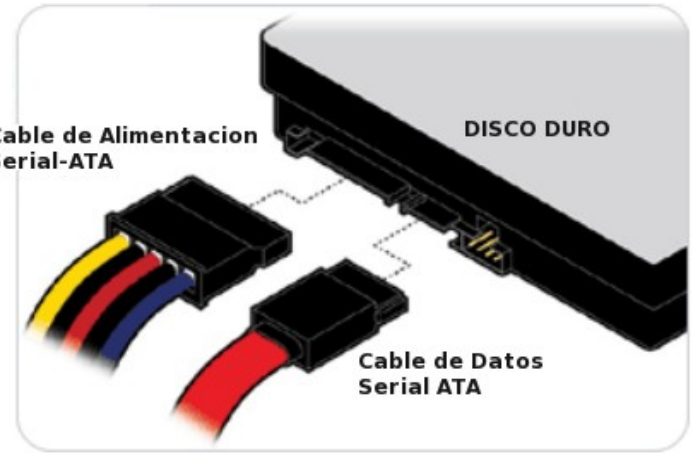
2.1.1.2.2 Características

El estándar Serial ATA brinda una velocidad de 187,5 MB/s (1,5 Gb/s) y cada octeto se transmite con un bit de arranque y un bit de parada, con una velocidad efectiva teórica de 150 MB/s (1,2 Gb/s). El estándar Serial ATA II debe contribuir a alcanzar 375 MB/s (3 Gb/s), es decir, una velocidad efectiva teórica de 300 MB/s, y finalmente 750 MB/s (6 Gb/s), es decir, una velocidad efectiva teórica de 600 MB/s.

Los cables del estándar Serial ATA pueden medir hasta 1 metro de longitud (en comparación con los 45 cm que miden los cables IDE). Además, la baja cantidad de hilos en una envoltura redonda permite una mayor flexibilidad y una mejor circulación del aire dentro de la carcasa que la de los cables IDE (incluso si existieran los cables IDE redondeados). A diferencia de los periféricos del estándar ATA, los del Serial ATA se encuentran solos en cada cable y ya no es necesario diferenciar los discos duros master de los discos duros slave.

Otra de la ventajas con este tipo de disco es que permite la conexión en caliente o en pocas palabras, mientras el equipo esta encendido

A continuación observaremos un diagrama de un disco duro Serial-ATA



2.1.1.3 Discos Duros SCSI

El estándar SCSI (Small Computers System Interface) es una interfaz que se utiliza para permitir la conexión de distintos tipos de periféricos a un ordenador mediante una tarjeta denominada adaptador SCSI o controlador SCSI generalmente mediante un conector PCI.

El número de periféricos que se pueden conectar depende del ancho del bus SCSI. Con un bus de 8 bits, se pueden conectar 8 unidades físicas y con uno de 16 bits, 16 unidades.

2.1.1.3.1 Direccionamiento de los Periféricos

Los periféricos se direccionan mediante números de identificación. El primer número es el ID, número que designa al controlador que se encuentra dentro de cada periférico (definido a través de los caballetes posicionados en cada periférico SCSI o por el software). El periférico puede tener hasta 8 unidades lógicas (por ejemplo, una unidad de CD-ROM con varios cajones). Las unidades lógicas se identifican mediante un LUN (Número de unidad lógica). Por último, un ordenador puede contener diversas tarjetas SCSI y, por lo tanto, a cada una le corresponde un número diferente.

2.1.1.3.2 SCSI asimétrico y diferencial

Existen dos tipos de bus SCSI:

- el bus asimétrico, conocido como SE (por Single-Ended o Terminación única), basado en una arquitectura paralela en la que cada canal circula en un alambre, sensible a las interferencias. Los cables SCSI en modo SE poseen 8 alambres para una transmisión de 8 bits (que se denominan limitados) o 16 alambres para cables de 16 bits (conocidos como extendidos). Este es el tipo de bus SCSI más común.

- el bus diferencial transporta señales a un par de alambres. La información se codifica por diferencia entre los dos alambres (cada uno transmite el voltaje opuesto) para desplazar las interrupciones electromagnéticas, lo que permite obtener una distancia de cableado considerable (alrededor de 25 metros). En general, existen dos modos: el modo LVD (Voltaje bajo diferencial), basado en señales de 3,3 V y el modo HVD (Voltaje Alto Diferencial), que utiliza señales de 5 V. Los periféricos que utilizan este tipo de transmisión son cada vez más raros y por lo general llevan la palabra "DIFF".

Los conectores para las dos categorías de periféricos son los mismos, pero las señales eléctricas son diferentes. Por lo tanto, los periféricos necesitan ser identificados (mediante los símbolos creados para tal fin) para no dañarlos.

2.1.1.3.3 Estándares SCSI

Los estándares SCSI definen los parámetros eléctricos de las interfaces de entrada/salida. El estándar SCSI-1 de 1986 definió los comandos estándar para el control de los periféricos SCSI en un bus con una frecuencia de 4,77 MHz con un ancho de 8 bits, lo que implicaba que era posible alcanzar velocidades de 5 MB/s.

Sin embargo, un gran número de dichos comandos eran opcionales, por lo que en 1994 se adoptó el estándar SCSI-2. Éste define 18 comandos, conocidos como CCS (Conjunto de comandos comunes). Se han definido varias versiones del estándar SCSI-2:

- El SCSI-2 extendido, basado en un bus de 16 bits (en lugar de 8), ofrece una velocidad de 10 MB/s
- El SCSI-2 rápido es un modo sincrónico rápido que permite un aumento de 5 a 10 MB/s para el estándar SCSI y de 10 a 20 MB/s para el SCSI-2 extendido (denominado SCSI-2 extendido rápido).
- Los modos Rápido-20 y Rápido-40 duplican y cuadriplican dichas velocidades respectivamente.

El estándar SCSI-3 incluye nuevos comandos y permite la unión de 32 periféricos, así como una velocidad máxima de 320 MB/s (en modo Ultra-320).

El siguiente cuadro resume las características de los diversos estándares SCSI:

Estándar	Ancho del bus	Velocidad del bus	Ancho de banda	Conector
SCSI-1 (*Fast-5 SCSI*)	8 bits	4,77 MHz	5 MB/seg	50 clavijas (bus simétrico o diferencial)
SCSI-2 – Fast-10 SCSI	8 bits	10 MHz	10 MB/seg	50 clavijas (bus simétrico o diferencial)
SCSI-2 - Extendido	16 bits	10 MHz	20 MB/seg	50 clavijas (bus simétrico o diferencial)
SCSI-2 - 32 bits rápido extendido	32 bits	10 MHz	40 MB/seg	68 clavijas (bus simétrico o diferencial)
SCSI-2 – Ultra SCSI-2 (Fast-20 SCSI)	8 bits	20 MHz	20 MB/seg	50 clavijas (bus simétrico o diferencial)
SCSI-2 - SCSI-2 ultra extendido	16 bits	20 MHz	40 MB/seg	
SCSI-3 – Ultra-2 SCSI (Fast-40 SCSI)	8 bits	40 MHz	40 MB/seg	
SCSI-3 - Ultra-2 SCSI-2 extendido	16 bits	40 MHz	80 MB/seg	68 clavijas (bus diferencial)
SCSI-3 – Ultra-160 (Ultra-3 SCSI o Fast-80 SCSI)	16 bits	80 MHz	160 MB/seg	68 clavijas (bus diferencial)
SCSI-3 – Ultra-320 (Ultra-4 SCSI o Fast-160 SCSI)	16 bits	80 MHz DDR	320 MB/seg	68 clavijas (bus diferencial)
SCSI-3 - Ultra-640 (Ultra-5 SCSI)	16	80 MHz QDR	640 MB/seg	68 clavijas (bus diferencial)

2.1.1.4 Discos Duros SAS

Serial Attached SCSI o SAS, es una interfaz de transferencia de datos en serie el cual es sucesor del disco dura SCSI, aunque sigue utilizando comandos SCSI para interaccionar con los dispositivos SAS. Aumenta la velocidad y permite la conexión y desconexión en caliente.

Una de las principales características es que aumenta la velocidad de transferencia al aumentar el número de dispositivos conectados, es decir, puede gestionar una tasa de transferencia constante para cada dispositivo conectado, además de terminar con la limitación de 16 dispositivos existente en SCSI, es por ello que se vaticina que la tecnología SAS irá reemplazando a su predecesora SCSI.

Además, el conector es el mismo que en el interfaz SATA y permite utilizar estos discos duros, para aplicaciones con menos necesidad de velocidad, ahorrando costos. Por lo tanto, los discos SATA pueden ser utilizados por controladoras SAS pero no a la inversa, una controladora SATA no reconoce discos SAS.

Está diseñado para permitir mayores tasas de transferencia y ser compatible con SATA (Serial ATA), y permite hasta 16384 dispositivos.

2.1.2 Zonas de un Disco Duro

Las principales partes que conforman un disco duro son:

- Las Pistas
- Los Sectores
- Los Cilindros
- Los Clusters

2.1.2.1 Pistas

Un pista o track se puede entender como una circunferencia del disco duro

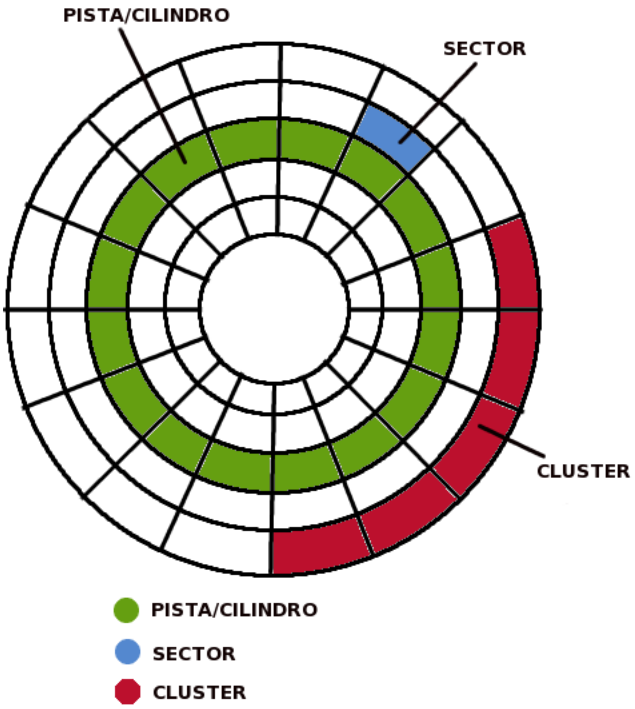
2.1.2.2 Sector

Un sector es cada una de las subdivisiones que conforman una pista, por lo regular el tamaño estándar de un sector es de 512 Bytes

2.1.2.3 Cilindro

Un cilindro esta conformado por la agrupación de varias pistas alineadas verticalmente, las cuales simulan un cilindro.

2.1.2.4 Cluster



Un cluster es una trozo de longitud de pista, comúnmente conformado por varios sectores

2.1.3 Estructura Lógica Del Disco Duro

La estructura lógica de un disco duro esta compuesta principalmente por

- El Master Boot Record
- Las particiones del Disco

2.1.3.1 Master Boot Record (MBR)

El Master Boot Record es el sector de arranque que contiene la tabla de particiones.

El Sector de Arranque o a veces también llamado bloque de arranque es un sector del disco duro que contiene el código de arranque de un Sistema Operativo, el Sector de Arranque por lo general esta localizado en el primer cilindro de la primera cabeza del disco duro en el primer sector (Cylinder, Head, Sector ---> 0,0,1) y es el encargado de inicializar el BIOS (Basic Input-Output System) de la computadora o servidor para preguntar si existe un sistema operativo existente en el sistema

Una vez que el BIOS verifica si existe un Sistema Operativo Instalado en el sistema , pasa el control de nuevo al MBR , el cual cual se definen las particiones primarias del Disco Duro. La tabla de particiones es la encargada de almacenar toda la información referente a las distintas particiones existentes del disco duro como son:

- El Tamaño de la partición
- El Formato de la particiones
- El Sector de Inicio de la partición
- Si es arrancable o boteable la partición

En la practica, el Master Boot Record es de 512 bytes.

2.1.3.2 Particiones Del Disco Duro

Las particiones de un disco duro pueden ser considerados como los trozos en los cuales esta dividido el disco duro. La finalidad de particionar un disco duro radica en la funcionalidad de tener varios sistemas operativos instalados en un mismo disco duro, claro esta que cada sistema operativo trabaja con su respectivo sistema de archivos, termino del que hablaremos en el siguiente tema.

Un disco duro solo puede soportar dos tipos de particiones:

2.1.3.2.1 Particiones Primarias

Es la primera y la mas importante, cualquier disco duro que se vaya a usar para almacenar un sistema operativo, forzosamente debe tener una partición de este tipo, pues son estas las encargadas de arrancar el sistema operativo, así como de almacenar el MBR y las tablas de particiones.

2.1.3.2.2 Particiones Extendida

Es otro tipo de partición que actúa como una partición primaria; sirve para contener infinidad de unidades lógicas en su interior. Fue ideada para romper la limitación de 4 particiones primarias en un solo disco físico. Solo puede existir una partición de este tipo por disco, y solo sirve para contener particiones lógicas. Por lo tanto, es el único tipo de partición que no soporta un sistema de archivos directamente.

2.1.3.2.2.1 Particiones Lógicas

Ocupa un trozo de partición extendida o la totalidad de la misma, la cual se ha formateado con un tipo específico de sistema de archivos (ext3, HPFS, NTFS) en al cual se instalara algún sistema operativo

2.2 Sistemas de Ficheros

Piense en un sistema de ficheros como el molde de una estructura metálica y al sistema operativo como el perfil que se acoplara al molde que la contendrá

Un sistema de ficheros se encarga de estructurar, gestionar y administrar eficientemente la información guardada en una unidad de almacenamiento masivo de datos como puede ser un disco duro, esta información puede ser consultada por un usuario de forma textual o de forma gráfica mediante la utilización de algún gestor de ficheros, que por lo regular son instalados

estructuran la información guardada en una unidad de almacenamiento (normalmente un disco duro) de una computadora, que luego será representada ya sea textual o gráficamente utilizando un gestor de archivos. La mayoría de los sistemas operativos poseen su propio sistema de archivos.

Un Sistema de Ficheros es un componente importante de un Sistema Operativo y suele contener:

- **Métodos de acceso** relacionados con la manera de acceder a los datos almacenados en archivos.
- **Administración de archivos** referida a la provisión de mecanismos para que los archivos sean almacenados, referenciados, compartidos y asegurados.
- **Administración del almacenamiento auxiliar** para la asignación de espacio a los archivos en los dispositivos de almacenamiento secundario.
- **Integridad del archivo** para garantizar la integridad de la información del archivo.

Sistemas Operativos como Linux hacen uso de los sistemas de ficheros como ext2, ext3 y swap, otros sistemas como por ejemplo Windows usan como sistema de ficheros los conocidos FAT y NTFS, por otra parte los sistemas operativos MacOS hacen uso del sistema de ficheros HFS.

La siguiente tabla nos dará una visión mas general sobre los sistemas de ficheros, así como de los sistemas operativos que hacen uso de las antes mencionadas.

Sistema Operativo	Sistema de Fichero Admitido
MS-DOS	**FAT16**
Windows 95	**FAT16**
Windows 98	**FAT16, FAT32**
Windows NT4	**FAT32 NTFS**
Windows 2000/XP	**FAT16, FAT32, NTFS**
Windows Vista	**NTFS**
Linux	**EXT2, EXT3, EXT4, ReiserFS,Swap**
MacOS	**HFS**
FreeBSD, OpenBSD	**UFS**
Sun Solaris	**UFS, ZFS**
IBM AIX	**JFS**

Como puede observarse, existen muchos sistemas de ficheros que pueden ser utilizados en los diferentes sistemas operativos, motivo por el cual explicaremos los detalles mas importantes de cada uno de esos sistemas de ficheros.

2.2.1 FAT16 (File Allocation Table)

FAT16 (Tabla de Asignación de Archivos) fue un sistema de ficheros desarrollado específicamente para el sistema operativo MS-DOS el cual pasaría luego a formar parte del sistemas de archivos que se implemento en los sistemas operativos Windows.

Este sistema de ficheros en realidad era un indice que creaba listas de contenidos en disco para grabar la ubicación de los archivos que éste contenía

Las implementaciones más extendidas de FAT tienen algunas desventajas. Cuando se borran y se escriben nuevos archivos tiende a dejar fragmentos dispersos de éstos por todo el disco duro, esto es debido a que los bloques que conformaban un archivo no siempre se almacenaban en el disco duro de forma contigua (la llamada fragmentacion de la información) y con el tiempo hacia que el proceso de lectura o escritura fuera cada vez más lento. La denominada desfragmentación es la solución a esto, pero es un proceso largo que debe repetirse regularmente para mantener el sistema de archivos en perfectas condiciones. FAT tampoco fue diseñado para ser redundante ante fallos. Inicialmente soportaba nombres cortos de ocho caracteres para el nombre así como tres para la extensión y por si fuera poco carecía de permisos de seguridad y con esto cualquier usuario podía acceder a cualquier archivo del sistema.

2.2.2 FAT32 (File Allocation Table)

FAT32 fue la respuesta para superar la barrera al limite de tamaño que ofrecía su predecesor, la FAT16, así mismo mantuvo la compatibilidad con el sistema operativo MS-DOS para luego ser implementado en la versión de Windows95.

Esta nueva FAT tenia como propósito implementar una nueva generación en sistemas de ficheros, motivo por el cual implemento direcciones de cluster de 32 bits aunque solo se ocuparan 28 de estos mismos.

En teoría, esto debería permitir aproximadamente 268.435.538 clusters, arrojando tamaños de almacenamiento cercanos a los dos terabytes. Sin embargo y debido a las limitaciones del software ScanDisk de Microsoft, esta ultima no permitía que la FAT32 creciera más allá de 4177920 clusters por partición (es decir, unos 124 gigabytes). Posteriormente, Windows 2000 y XP situaron el límite de FAT32 en los 32 gigabytes.

FAT32 apareció por primera vez en Windows 95 y era necesario reformatear el disco duro para implementar FAT32.

2.2.3 NTFS (New Technology File System)

El sistema de ficheros NTFS esta basada en una estructura llamada tabla maestra de ficheros, la cual puede contener información detallada y estructurada de los ficheros del mismo. Este sistema de ficheros ya permitía el uso de nombres mas largos, aunque a diferencia del sistema de ficheros FAT distingue entre letras mayúsculas y minúsculas

El rendimiento, así como el acceso a los archivos de una partición NTFS es mas rápido a comparación de una FAT, ya que esta implementada en un árbol binario de alto rendimiento para localizar a los archivos. En teoría, el tamaño límite de una partición es de 16 exabytes (17 mil millones de TB). Sin embargo, el límite físico de un disco es de 2TB.

NTFS es un sistema de ficheros desarrollado para los sistemas operativos Windows NT, Windows 2000, Windows 2003, Windows XP y Windows Vista y está basado en el sistema de ficheros HPFS de IBM/Microsoft usado en el sistema operativo OS/2, el cual también tiene ciertas influencias del formato de archivos HFS diseñado por Apple.

2.2.4 EXT2 (Second Extended Filesystem)

El sistema de ficheros EXT2 fue desarrollado originalmente por Remy Card quien es un programador y desarrollador de origen Frances el cual ha aportado mucha de su investigacion el proyecto GNU/Linux. Particularmente Remy Card desarrollo el sistema de ficheros ext2 para los sistemas operativos RedHat, Fedora y Debian,

Este sistema de ficheros tiene un tipo de tabla FAT de tamaño fijo, donde se almacenan los i-nodos. Los i-nodos son una versión muy mejorada de FAT, donde un puntero i-nodo almacena información del archivo (ruta o path, tamaño, ubicación física). En cuanto a la ubicación, es una referencia a un sector del disco donde están todos y cada una de las referencias a los bloques del archivo fragmentado. Estos bloques son de tamaño especificable cuando se crea el sistema de archivos, desde los 512 bytes hasta los 4 kB, lo cual asegura un buen aprovechamiento del espacio libre con archivos pequeños. Los límites son un máximo de 2 TB de archivo, y de 4 TB de partición.

2.2.5 EXT3 (Third Extended Filesystem)

La principal diferencia de EXT2 con EXT3 es que EXT3 dispone de un registro por diario o mayormente conocido como journaling

Así mismo EXT3 puede ser montado y usado como un sistema de archivos EXT2. Otra diferencia importante es que EXT3 utiliza un árbol binario balanceado (árbol AVL) e incorpora el asignador de bloques de disco.

Aunque su velocidad y escalabilidad es menor que sus competidores, como JFS, ReiserFS o XFS, tiene la ventaja de permitir actualizar de EXT2 a EXT3 sin perder los datos almacenados ni formatear el disco y un menor consumo de CPU.

El sistema de archivo EXT3 agrega a EXT2 lo siguiente:

- Registro por diario.
- Índices en árbol para directorios que ocupan múltiples bloques.
- Crecimiento en línea.

2.2.6 EXT4 (Fourth Extended Filesystem)

Este sistema de ficheros también cuenta con un registro por diario, y se espera este disponible en futuras versiones de Linux como Fedora 10, CentOs y Ubuntu 8.10

Las principales mejoras de este sistema de ficheros serán:

- Soporte de volúmenes de hasta 1024 PiB.
  PiB.-Pebibyte es la denominación de una Unidad de almacenamiento de información. Corresponde a 250 bytes, es decir, 1.125.899.906.842.624 bytes
- Soporte añadido de extent el cal

Actualmente, el ext4 es compatible con su anterior versión, el ext3, esto quiere decir que se puede montar como una partición ext3. También se pueden montar las particiones ext3 como ext4, aunque, si la partición ext4 usa *extent* (una de las mayores mejoras), la compatibilidad con la versión anterior, y por lo tanto, montar la partición como ext3, no es posible. La opción *extent* no es usada por defecto.

2.2.7 HPFS (High Performance File System*)*

Fue creado específicamente para el sistema operativo OS/2 para mejorar las limitaciones del sistema de archivos FAT. Fue escrito por Gordon Letwin y otros empleados de Microsoft, y agregado a OS/2 versión 1.2, en esa época OS/2 era todavía un desarrollo conjunto entre Microsoft e IBM.

Se caracteriza por permitir nombres largos, metadatos e información de seguridad, así como de autocomprobación e información estructural.

Otra de sus características es que, aunque poseía tabla de archivos como FAT, ésta se encontraba posicionada físicamente en el centro de la partición, de tal manera que redundaba en menores tiempos de acceso a la hora de leerla o escribirla.

2.2.8 ReiserFS

ReiserFS es un sistema de archivos de propósito general, diseñado e implementado por un equipo de la empresa Namesys, liderado por Hans Reiser. Actualmente es soportado por Linux y existen planes de futuro para incluirlo en otros sistemas operativos. También es soportado bajo windows de forma no oficial, aunque por el momento de manera inestable y rudimentaria. A partir de la versión 2.4.1 del núcleo de Linux, ReiserFS se convirtió en el primer sistema de ficheros con journal en ser incluido en el núcleo estándar. También es el sistema de archivos por defecto en varias distribuciones, como SuSE (excepto en openSuSE 10.2 que su formato por defecto es ext3), Xandros, Yoper, Linspire, Kurumin Linux, FTOSX, Libranet y Knoppix.

Con la excepción de actualizaciones de seguridad y parches críticos, Namesys ha cesado el desarrollo de ReiserFS (también llamado reiser3) para centrarse en Reiser4, el sucesor de este sistema de archivos.

ReiserFS ofrece funcionalidades que pocas veces se han visto en otros sistemas de archivos:

- Journaling. Esta es la mejora a la que se ha dado más publicidad, ya que previene el riesgo de corrupción del sistema de archivos.
- Reparticionamiento con el sistema de ficheros montado y desmontado. Podemos aumentar el tamaño del sistema de ficheros mientras lo tenemos montado y desmontado (online y offline). Para disminuirlo, únicamente se permite estando offline (desmontado). Namesys nos proporciona las herramientas para estas operaciones, e incluso, podemos usarlas bajo un gestor de volúmenes lógicos como LVM o EVMS.

- Tail packing, un esquema para reducir la fragmentación interna

Comparado con EXT2 y EXT3 en el uso de archivos menores de 4k, ReiserFS es normalmente más rápido en un factor de 10–15. Esto proporciona una elevada ganancia en las news, como por ejemplo Usenet, caches para servicios HTTP, agentes de correo y otras aplicaciones en las que el tiempo de acceso a ficheros pequeños debe ser lo más rápida posible.

Algunas de las desventajas de ReiserFS son:

Los usuarios que usen como sistema de ficheros ext2, deben formatear sus discos, aunque no así los que usen ext3.

- ReiserFS en versiones del kernel anteriores a la 2.4.10 se considera inestable y no se recomienda su uso, especialmente en conjunción con NFS
- Algunas operaciones sobre archivos no son síncronas bajo ReiserFS, lo que pueden causar comportamientos extraños en aplicaciones fuertemente basadas en locks de archivos.
- No se conoce una forma de desfragmentar un sistema de archivos ReiserFS, aparte de un volcado completo y su restauración.
- Tempranas implementaciones de ReiserFS (anteriores a la incluida en el kernel 2.6.2), eran susceptibles de problemas de escrituras fuera de orden, lo que provocaba que archivos siendo escritos durante una caída del sistema, ganaran un pico de bytes extras de basura en el siguiente montado del sistema de archivos. La implementación actual de journaling, es correcta en este aspecto, manteniendo el journaling ordenado, del estilo de ext3.

2.2.9 ZFS (Zettabyte File System)

Es un sistema de ficheros desarrollado por Sun Microsystems para su sistema operativo Solaris. El significado original era “Zettabyte File System”, pero ahora es un acrónimo recursivo.

El anuncio oficial de ZFS se produjo en Septiembre del 2004. El código fuente del producto final se integró en la rama principal de desarrollo de Solaris el 31 de octubre del 2005 y fue lanzado el 16 de noviembre de 2005 como parte del build 27 de OpenSolaris.

ZFS fue diseñado e implementado por un equipo de Sun liderado por Jeff Bonwick. ZFS destaca por su gran capacidad, integración de los conceptos anteriormente separados de sistema de ficheros y administrador de volúmenes en un solo producto, nueva estructura sobre el disco, sistemas de archivos ligeros, y una administración de espacios de almacenamiento sencilla.

Sun ha indicado que está investigando el port del producto a Linux, aunque no hay planes para llevarlo a HP-UX o AIX.

FreeBSD 7, a lanzarse a fines del 2007, también dará soporte a ZFS.

Recientemente, Apple ha confirmado que utilizará ZFS en la próxima versión Server de su sistema operativo Mac OS X 10.6 Snow Leopard.

2.2.10 XFS

XFS es un sistema de archivos de 64 bits con journaling de alto rendimiento creado por SGI (antiguamente Silicon Graphics Inc.) para su implementación de UNIX llamada IRIX. En mayo del 2000, SGI liberó XFS bajo una licencia de código abierto.

XFS se incorporó a Linux a partir de la versión 2.4.25, cuando Marcelo Tosatti (responsable de la rama 2.4) lo consideró lo suficientemente estable para incorporarlo en la rama principal de desarrollo del kernel. Los programas de instalación de las distribuciones de SuSE, Gentoo, Mandriva, Slackware, Fedora Core, Ubuntu y Debian ofrecen XFS como un sistema de archivos más. En FreeBSD el soporte para solo-lectura de XFS se añadió a partir de Diciembre de 2005 y en Junio de 2006 un soporte experimental de escritura fue incorporado a FreeBSD-7.0-CURRENT.

2.2.11 JFS (Journaling File System)

Es un sistema de archivos con respaldo de transacciones desarrollado por IBM y usado en sus servidores. Fue diseñado con la idea de conseguir "servidores de alto rendimiento y servidores de archivos de altas prestaciones, asociados a e-business". Según se lee en la documentación y el código fuente, va a pasar un tiempo antes de que la adaptación a Linux este finalizada e incluida en la distribución estándar del kernel. JFS utiliza un método interesante para organizar los bloques vacíos, estructurándolos en un árbol y usa una técnica especial para agrupar bloques lógicos vacíos.

JFS fue desarrollado para AIX. La primera versión para Linux fue distribuida en el verano de 2000. La versión 1.0.0 salió a la luz en el año 2001. JFS está diseñado para cumplir las exigencias del entorno de un servidor de alto rendimiento en el que sólo cuenta el funcionamiento. Al ser un sistema de ficheros de 64 bits, JFS soporta ficheros grandes y particiones LFS (del inglés Large File Support), lo cual es una ventaja más para los entornos de servidor.

También está disponible para las últimas versiones de OS/2 y eComstation

Las principales ventajas de JFS son:

- Eficiente respaldo de transacciones (Journaling).

JFS, al igual que ReiserFS, sigue el principio de metadata only. En vez de una completa comprobación sólo se tienen en cuenta las modificaciones en los metadatos provocadas por las actividades del sistema. Esto ahorra una gran cantidad de tiempo en la fase de recuperación del sistema tras una caída. Las actividades simultáneas que requieren más entradas de protocolo se pueden unir en un grupo, en el que la pérdida de rendimiento del sistema de ficheros se reduce en gran medida mediante múltiples procesos de escritura.

- Eficiente administración de directorios.

JFS abarca diversas estructuras de directorios. En pequeños directorios se permite el almacenamiento directo del contenido del directorio en Inode. En directorios más grandes se utiliza Btrees, que facilitan considerablemente la administración del directorio.

- Mejor utilización de la memoria mediante adjudicación dinámica de Inodes.

Con ext2 debe dar por anticipado el grosor del Inode (la memoria ocupada por la información de administración). Con ello se limita la cantidad máxima de ficheros o directorios de su sistema de ficheros. JFS le ahorra esto, puesto que asigna memoria Inode de forma dinámica y la pone a su disposición cuando no se está utilizando.

2.3 Aplicaciones OpenSource para particionar discos duros

Existen aplicaciones libres como alternativas a las aplicaciones propietarias como es el caso del Partitioning Magic, a continuación se exponen 2 de las mejores:

2.3.1 Gparted

GParted es el editor de particiones de GNOME. Esta aplicación es usada para crear, eliminar, redimensionar, inspeccionar y copiar particiones, como también sistemas de archivos. Esto es útil para crear espacio para nuevos sistemas operativos, reorganizar el uso del disco y crear imágenes de un disco en una partición.

La aplicación utiliza la librería libparted para detectar y manipular dispositivos y tablas de partición, mientras varias herramientas de sistema de archivos dan mantenimiento a sistemas de archivos no incluidos en libparted. Está escrito en C++ y utiliza gtkmm como herramienta gráfica. Este acercamento es para mantener la interfaz gráfica de usuario lo más simple posible, conforme con las Human Interface Guidelines.

2.3.1.1 Gparted LiveCD

Se encuentra disponible en LiveCD, basado en Slackware y construido sobre la última rama estable núcleo de Linux (2.6). LiveCD es actualizado con cada lanzamiento de GParted. El LiveCD de Ubuntu incluye esta aplicación entre sus utilidades. También se encuentra disponible en versión LiveUSB.

Cuando se carga LiveCD, se inicia una mini-distribución que contiene las siguientes aplicaciones:

- Escritorio Xfce
- Thunar como gestor de archivos
- Una aplicación para capturas de pantallas (por medio de Thunar se pueden guardan en un pendrive)
- Documentento de ayuda
- GParted
- Xfree86

2.3.1.2 Capacidades y limitaciones

GParted no puede incrementar el tamaño de las particiones sin existir un espacio vacío después de dicha partición, es decir, si existen dos particiones juntas no se podrá aumentar el tamaño de una en detrimento de la otra; pero esto es más bien una limitación técnica. En esta tabla se muestran las capacidades de GParted, de acuerdo con cada sistema de archivos.

	Detectar	Leer	Crear	Aumentar	Encoger	Mover	Copiar	Revisar
EXT2	SI	SI	SI	SI	SI	SI	SI	SI
EXT3	SI	SI	SI	SI	SI	SI	SI	SI
FAT16	SI	SI	SI	SI	SI	SI	SI	SI
FAT32	SI	SI	SI	SI	SI	SI	SI	SI
HFS	SI	SI	SI	NO	SI	SI	SI	NO
HFS+	SI	SI	NO	NO	SI	SI	SI	NO
JFS	SI	SI	SI	SI	NO	SI	SI	NO
SWAP	SI	NO	SI	SI	SI	SI	SI	NO
NTFS	SI	SI	SI	SI	SI	SI	SI	SI
ReiserFS	SI	SI	SI	SI	SI	SI	SI	SI
Reiser4	SI	SI	SI	NO	NO	SI	SI	SI
UFS	SI	NO	NO	NO	NO	SI	SI	NO
XFS	SI	SI	SI	SI	PARCIAL	SI	SI	SI

Si usted desea probar esta aplicación, la puede descargar del siguiente portal web

Fuente: http://gparted.sourceforge.net/

2.3.2 Parted Magic

Parte Magic es un LiveCD que incluye una distribución Linux a medida para poder operar directamente con ella sin necesidad de ser instalada en el disco duro. No estamos hablando solo de un particionador de discos mas. En este LiveCD podemos encontrar varias herramientas entre ellas un editor de particiones llamado VisParted basado en el genuino Gparted con la que podremos crear, redimensionar y borrar nuestras particiones del disco duro.

Parted Magic soporta los siguientes sistemas de archivos: ext2, ext3, ext4, fat16, fat32, hfs, hfs+, jfs, linux-swap, ntfs, reiserfs, reiser4 y xfs.

Si usted desea probar esta aplicación, la puede descargar del siguiente portal web

2.3.3 QtParted

QtParted es una aplicación para Linux que es usada para crear, eliminar, redimensionar o administrar particiones del disco duro. Utiliza la librería GNU Parted y fue construida con el Qt toolkit. Como GNU Parted, tiene soporte inherente para redimensionar particiones NTFS, usando la utilidad ntfsresize. Se incluye predeterminadamente en varias distribuciones como Kubuntu.

El equipo QtParted no provee soporte para usar su aplicación en un Live CD, a diferencia de GParted. Sin embargo, QtParted está incluido en el Ark Linux Live (el equipo de Ark Linux actualmente mantiene este programa), en Knoppix, en el Live CD de Kubuntu, en MEPIS, en Nimblex y en el Trinity Rescue Kit.

Fuente: http://qtparted.sourceforge.net/

Índice de contenido

Información de Derechos reservados de esta publicación.

Autor del manual: Javier Eduardo Duarte

Tema 1. Instalación del Sistema Operativo CentOS

1.1 Instalación de CentOS 5

La instalación de los sistemas Linux basados en Red Hat© se puede realizar a través de los siguientes medios:

- CD-ROM / DVD-ROM
- Disco Duro
- USB
- Red
  - HTTP / FTP / NFS

La instalación del sistema operativo a través de los CD's o DVD no es muy difícil, solo se necesita tener este medio de instalación e insertarlo en la lectora de CD-ROM / DVD-ROM y seguir las instrucciones. En la sección “Medios de instalación” se explica como realizar la instalación del sistema operativos cuando no se cuenta con un CD/DVD de instalación.

En la figura se muestra la ventana de inicio, en la cual se muestra las opciones que se pueden ejecutar antes de iniciar la instalación, estas opciones son conocidas como “Parámetros de kernel”. Para iniciar la instalación basta presionar la tecla **ENTER**.

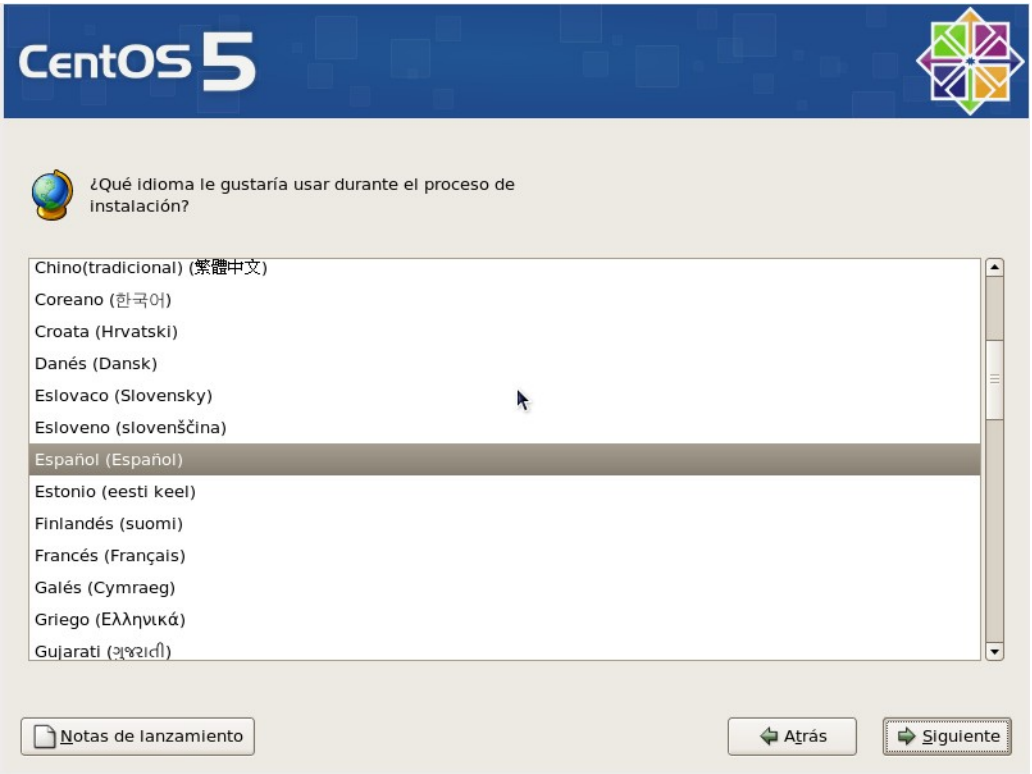
Antes de iniciar la instalación se recomienda que analice la integridad del medio de instalación para verificar que no este dañado, mal grabado o rayoneado, esto con el fin de evitar errores al instalar el sistema operativo. En la siguiente figura se muestra el asistente para verificar el medio de instalación. Para omitir esta prueba seleccione Skip.

Las versiones Linux basadas en Red Hat cuentan con un asistente gráfico llamado Anaconda, el cual es el instalador para sistemas operativos basados en Red Hat Linux como Fedora y Centos ademas facilita la instalación y configuración del sistema operativo.

En la siguiente hoja se muestra la pantalla del instalador gráfico Anaconda, solo tendrá que teclear "Next" para proseguir con la instalación.

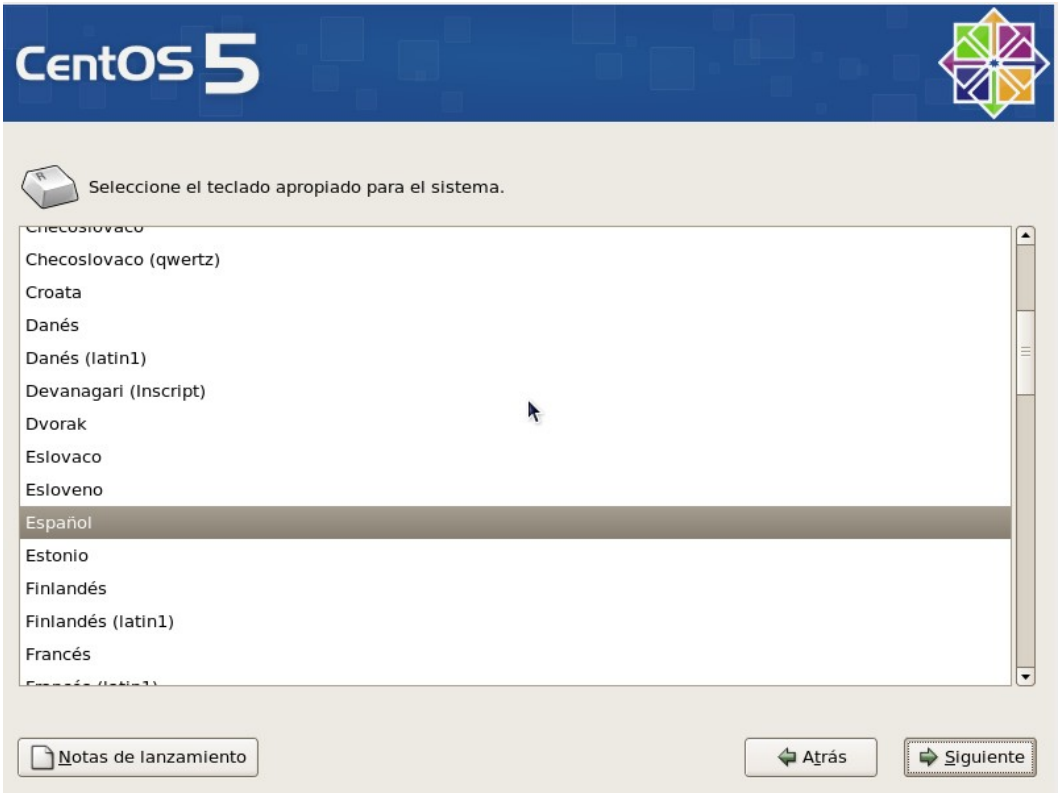
1.1.1 Configuración del idioma

Seleccioné el idioma predeterminado que tendrá el sistema operativo como se muestra en la figura . Se sugiere que el idioma predeterminado sea español.



1.1.2 Configuración del teclado

Seleccione el teclado como se muestra en la figura. Para el idioma Español existe diferentes distribuciones de teclado, las cuales varían por la ubicación de los signos de puntuación. Para conocer la distribución del teclado solo es necesario conocer la ubicación del carácter **"@"**, para la distribución español el "@" se encuentra en tecla "2", para la distribución latinoamericana la "@" se encuentra en tecla "Q".



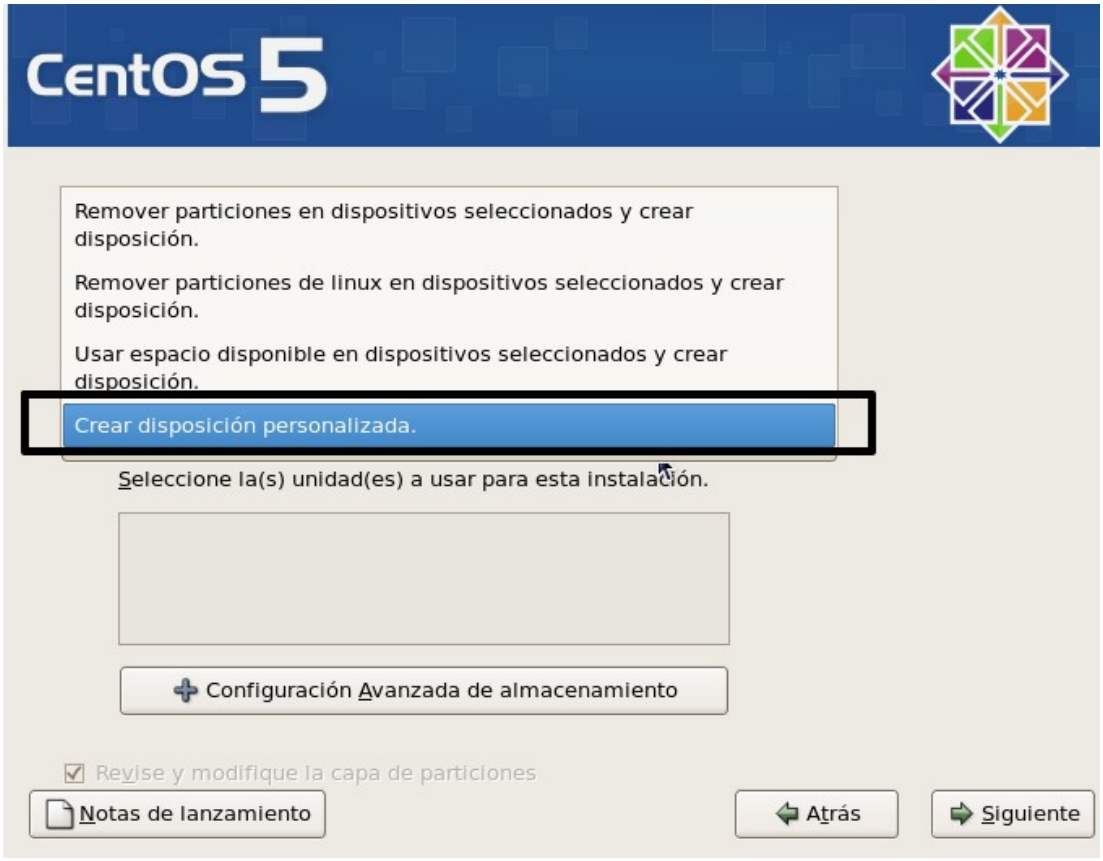
1.1.3 Particionando el Disco Duro

Antes de comenzar la instalación, el asistente solicitará partición del disco duro en la cual se instalará el sistema operativo. Las operaciones que se pueden realizar son las siguientes:

- Remover particiones en dispositivos seleccionados y crear disposición. Esta opción borra todos los sistemas operativos instalados así como sus datos del disco dura e instala el sistema operativo Linux en todo el disco duro.
- Remover particiones de Linux en dispositivos seleccionados y crear disposición. Esta opción borra todas las particiones Linux instaladas en disco duro e instala la nueva versión Linux.
- Usar espacio disponible en dispositivos seleccionados y crear disposición. Esta opción instala Linux en el espacio libre en el disco duro.
- Crear disposición personalizada. Esta opción permite particionar el disco duro de forma manual.

Se recomienda utilizar la ultima opción:

“Crear disposición personalizada”



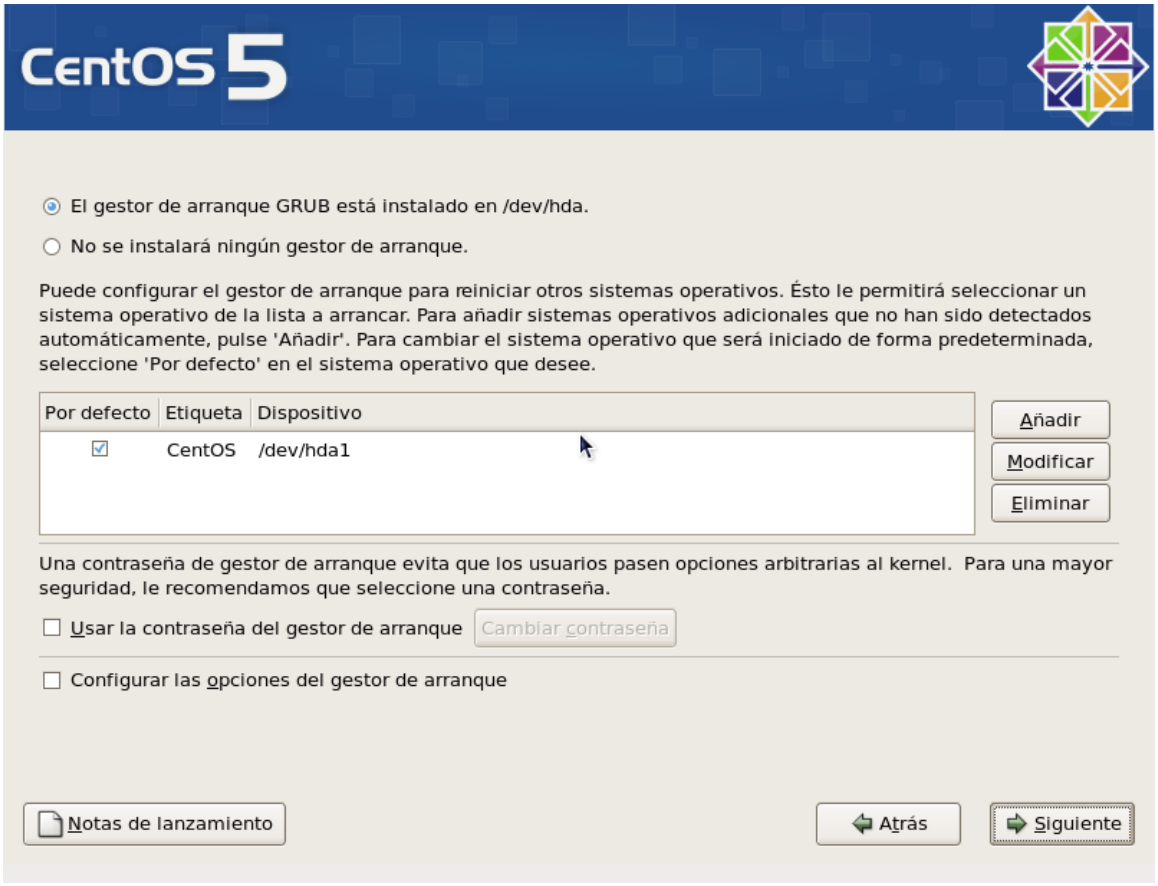
Al seleccionar la opción personalizada, se mostrara una herramienta para particionar el disco duro.

Para crea una partición, presione el botón **"nuevo"**, se mostrara una ventana de dialogo en la cual se presentan las siguientes opciones ():

- Punto de montaje. Define el sistema de archivos que se instalará en esta partición.
- Tipo de sistema de archivos. Define el tipo de sistema de archivo a utilizar en la partición.
- Unidades admisibles. Muestra los discos duros que serán afectados por la operación los cuales se puede realizar la operación.
- Tamaño. Define el tamaño en Megabytes (Mb) de la partición
- Opciones de tamaño adicionales:
  - Tamaño fijo. Si esta opción esta activa, toma el cantidad definida en el campo anterior y lo tomo como el tamaño fijo para la partición.
  - Completar todo el espacio hasta. Si esta opción esta activa, toma el cantidad definida en el campo tamaño y crea la partición hasta la cantidad definida
  - Completar hasta el tamaño permitido. Si esta opción esta activa, la partición se crea con el espacio libre en el disco duro.
- Forzar a primaria. Esta opción permite que la partición se cree como primaria.

1.1.4 Gestor de arranque

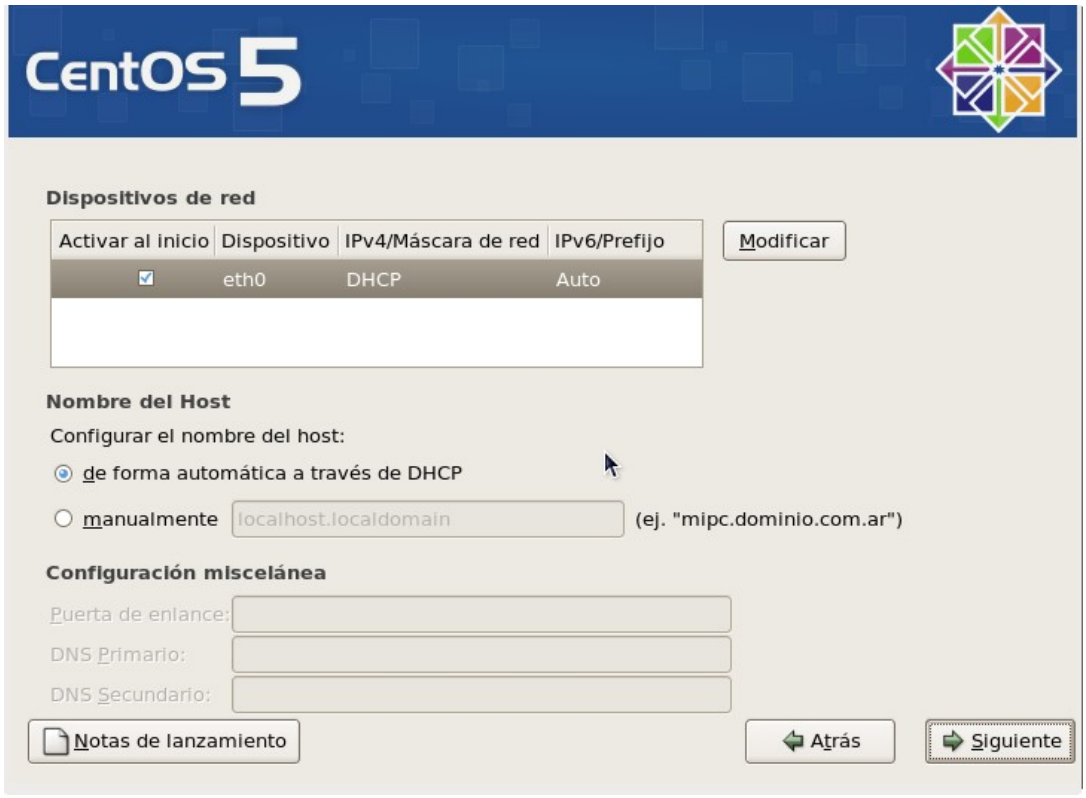
El gestor de arranque es la aplicación que permite seleccionar entre múltiples sistemas instalados en el misma computadora. En los sistemas Linux, el gestor de arranque predeterminado y popular es el **GRUB** (***GR**and **U**nified **B**ootloader)*. La instalación del Grub se realiza en el primer sector del disco duro conocido como el Master Boot Record (MBR). Si se tiene instalado otro gestor de arranque de un sistema operativo diferente, se puede omitir la instalación del Grub para no modificar el MBR.



Se recomienda poner una contraseña al gestor de arranque, para evitar que otro tipo usuarios puedan introducir parámetros de kernel y en administradores de sistema, tomando el control total del equipo.

1.1.5 Configuración de la tarjeta de red

Gran parte de los sistemas Linux reconoce la mayoría de las tarjetas de red comerciales instaladas en el equipo, como se muestra en la figura (), el asistente de instalación permite configurar los parámetros de Red estos dispositivos de forma manual o de forma automática por medio de un servidor DHCP , así como definir que dispositivos de red van a arrancar con el sistema operativo.

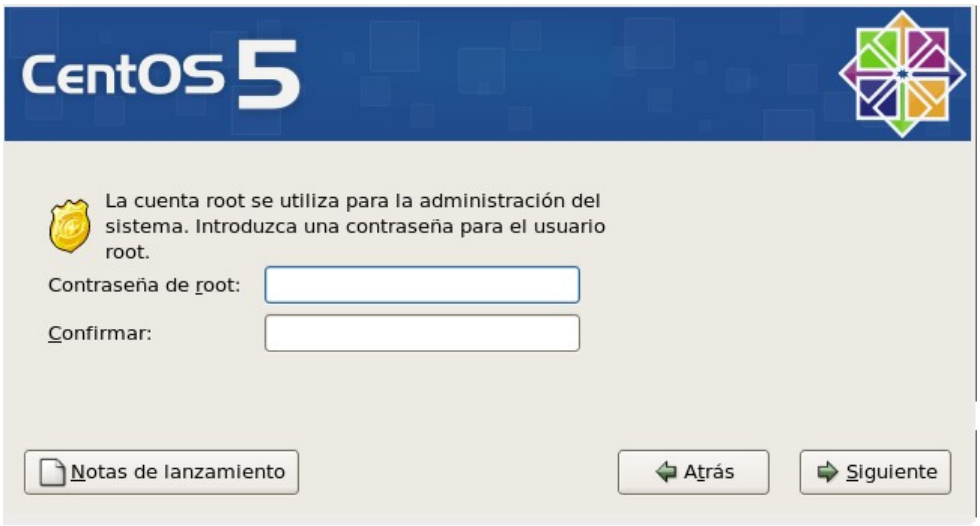


1.1.6 Configuración de la zona horaria

Se recomienda seleccionar la ubicación en la cual se encuentra la computadora para configurar la zona horaria, esto con el fin de tener sincronizada y al tiempo la hora del equipo. El tiempo universal coordinado (UTC) es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo teniendo como ventaja su precisión al poseer reloj atómicos que permite calcular el tiempo

1.1.7 Contraseña del Administrador

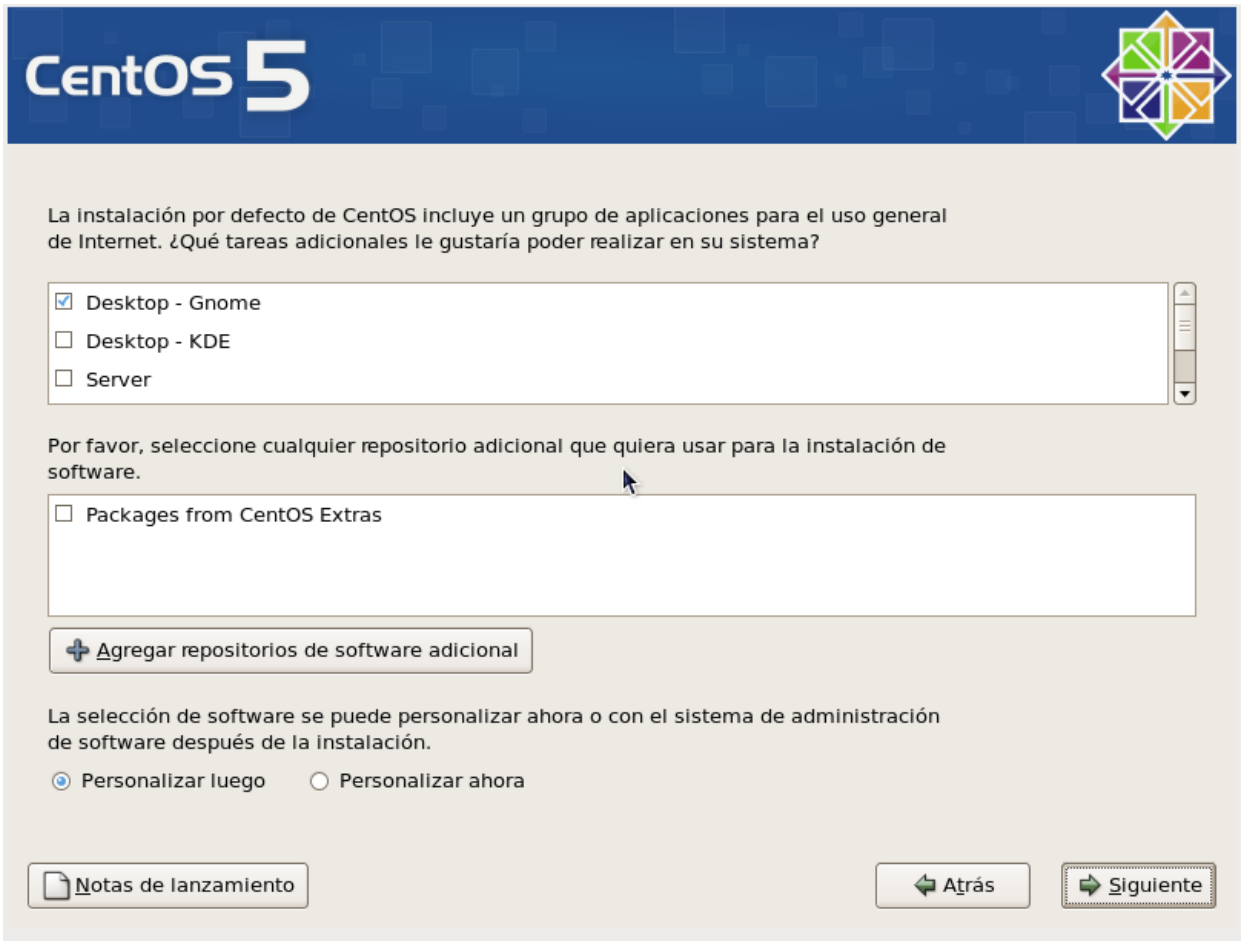
El asistente de instalación solicita la contraseña de root (administrador) como se muestra en la siguiente figura, se recomienda que esta contraseña contenga caracteres alfanuméricos.



1.1.8 Selección de paquetes

Los sistemas Linux basados en Red Hat ponen en categorías las aplicaciones disponibles que se deseen instalar. Esta categorías se dividen en:

- Desktop – GNOME. Escritorio predeterminado se caracteriza por su diseño ergonómico y fácil de usar contiene las aplicaciones mas utilizadas por los usuarios, como editores y procesadores de texto, visualizadores de pdf, programas de procesamiento de imágenes, juegos entre otros.
- Desktop – KDE. Escritorio alternativo caracterizado por ser mas visual y estético, también ofrece las aplicaciones mas utilizadas.
- Servidores. Ofrece los servidores mas utilizado en ambiente en producción, como servidores Web, Correo, DNS, entre otros.
- Clúster. Herramientas y sistemas requeridos para la implementación de arreglos de servidores de alto desempeño o de alta disponibilidad, según los requerimientos de nuestro entorno.
- Clúster de Almacenamiento. Herramientas y sistemas requeridos para el manejo de arreglos de dispositivos de almacenamiento distribuidos.



Al terminar la configuración, el asistente comprobará las dependencias entre los paquetes para poder realizar la instalación del sistema operativo, este proceso puede variar dependiendo del numero las aplicaciones seleccionadas y de la capacidad del sistema operativo.

Índice de contenido

Información de Derechos reservados de esta publicación.

Tema 3. Manejo del editor de textos VI

3.1 Acerca de VI

La historia de este poderoso editor de textos se centra en William Nelson Joy o mayormente conocido como Bill Joy (Cofundador de la empresa Sun Microsystems), el cual comenzó el desarrollo de **VI** tomando como base dos editores de textos: **"ed"** y **"ex"** . Dichos editores de textos eran para ese entonces los mayormente utilizados en equipos UNIX pero debido a su gran deficiencia y complejidad dejaron de ser utilizados.

El editor de textos **VI** ha sido uno de los editores de textos mayormente implementado a lo largo de la historia de los sistemas operativos UNIX, es por ello que ha logrado establecerse como el editor de textos estándar de sistemas operativos como el mismo UNIX, Linux y BSD

Así mismo existen alternativas mucho mas atractivas y estéticas a **VI**, como pueden ser **EMACS**, **gEdit** y **nano**, mas sin embargo y debido a que VI a logrado permanecer por tantos años como el editor de textos predefinido de UNIX este ha llegado a consolidarse de una manera impresionante, un ejemplo claro de esto es que en donde quiera que tengan un equipo con UNIX, Linux o BSD siempre encontraras instalado el editor de textos **VI** cosa que no te garantizan editores de texto como **EMACS**, **gEdit** o **nano**.

Otro de los puntos fuertes de VI es el hecho de que este no da formato al texto pues no centra ni justifica párrafos pero permite mover, copiar, eliminar o insertar caracteres por medio del búfer permaneciendo la información ahí hasta que los cambios en el archivo se hayan guardado o bien hasta que termine la ejecución de la aplicación sin haber guardado las modificaciones.

Existe una versión mejorada de **VI** la cual es conocida como **VIM**, la diferencia radica en el uso de colores para diferenciar los diferentes tipos de sentencias implementadas en los diferentes archivos de configuración de Linux lo cual resulta muy practico para los administradores de sistemas.

3.2 Modos de Operación de VI

3.2.1 Modo Comandos

Como su nombre lo indica permite indicar comandos que ejecuten una acción específica, como búsquedas, copiar, pegar, eliminar líneas, mover el cursor, posicionarse en partes del archivo, etc. Varios comados están disponibles directamente, con solo apretar una o dos teclas, y otros están disponibles en el modo **última línea** que se accede a ella presionando la tecla dos puntos **':'** y en seguida se indica la acción o comando a ejecutar. Para salir del modo de última línea se presiona ESC.

3.2.2 Modo Inserción

En este modo es cuando se está realmente en el archivo, cuando se puede escribirlo y editarlo. Estando en el modo de inserción, para regresar al modo de comandos se presiona la tecla ESC.

3.3 Tutorial básico de VI

Antes de comenzar con el tutorial básico de VI le recomendamos primero crear un archivo vació. Dentro de el ejecutaremos todos los comandos básicos de VI, para ello haremos uso del comando touch

```
[root@ localhost ]# touch prueba.txt
```

3.3.1 Abrir

Ubique la ruta en la cual creo el archivo vacío prueba.txt y seguido de ello teclee el siguiente comando en una terminal de BASH

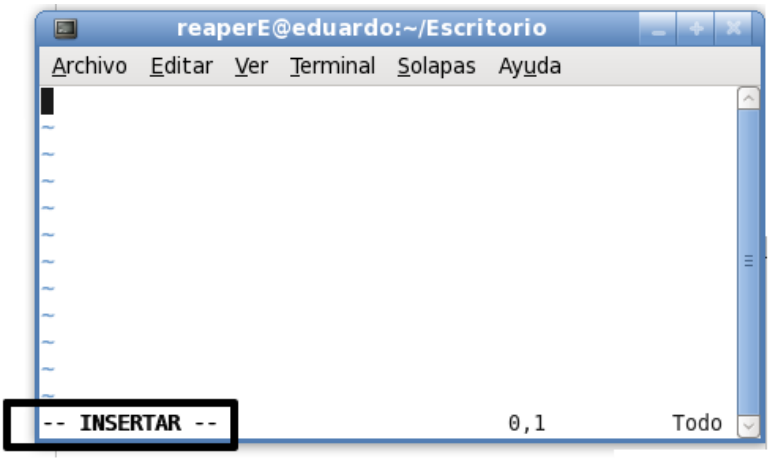
```
[root@ localhost ]#  vi prueba.tx

~
~
"prueba.txt" 0L, 0C
```

El siguiente paso sera añadir a nuestro archivo de texto algún contenido.

3.3.2 Editar

Para poder llevar a cabo esta operación primero se tendrá que abrir el archivo “prueba.txt” y posteriormente deberá teclear el botón “Insert”, esta acción nos pasara al modo inserción de Vi

posterior a ello deberá observar la palabra “INSERTAR” en la parte inferior de su izquierda de la terminal de BASH como a continuación se muestra.



Añada el siguiente texto al archivo "prueba.txt".

Curso:Instalación de Servidores Linux Asico

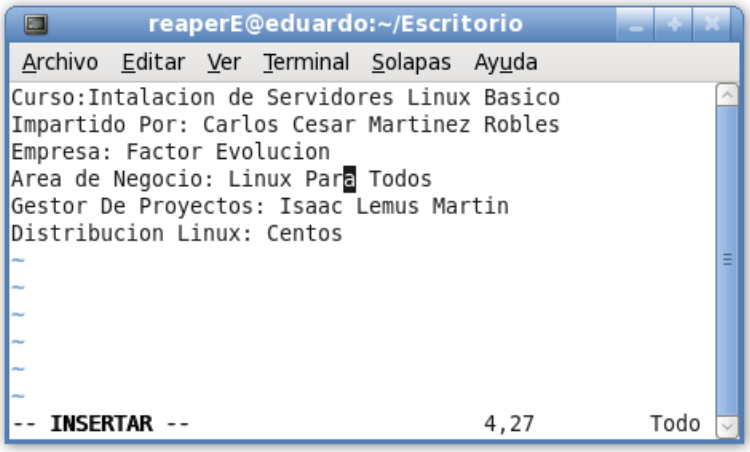
Impartido Por: Carlos Cesar Martinez Robles

Empresa: Factor Evolucion

Área de Negocio: Linux Para Todos

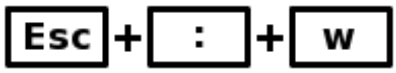
Gestor De Proyectos: Isaac Lemus Martín

Distribución Linux: Centos



3.3.3 Guardar

Para guardar los cambios hechos al archivo solo tendrá que teclear los botones:



La tecla **"Esc"** nos permite cambiar entre el modo inserción y el modo comandos, un ejemplo del modo de comandos es guardar, copiar, buscar, reemplazar y salir, en este caso la letra **"w"** indica que deben ser guardados los cambios hechos al archivo.

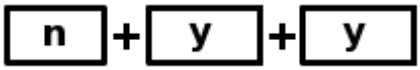
Si deseamos editar de nuevo el archivo "prueba.txt" deberá teclear nuevamente el botón:

Esto para cambiarnos del modo comandos al modo inserción

3.3.4 Copiar

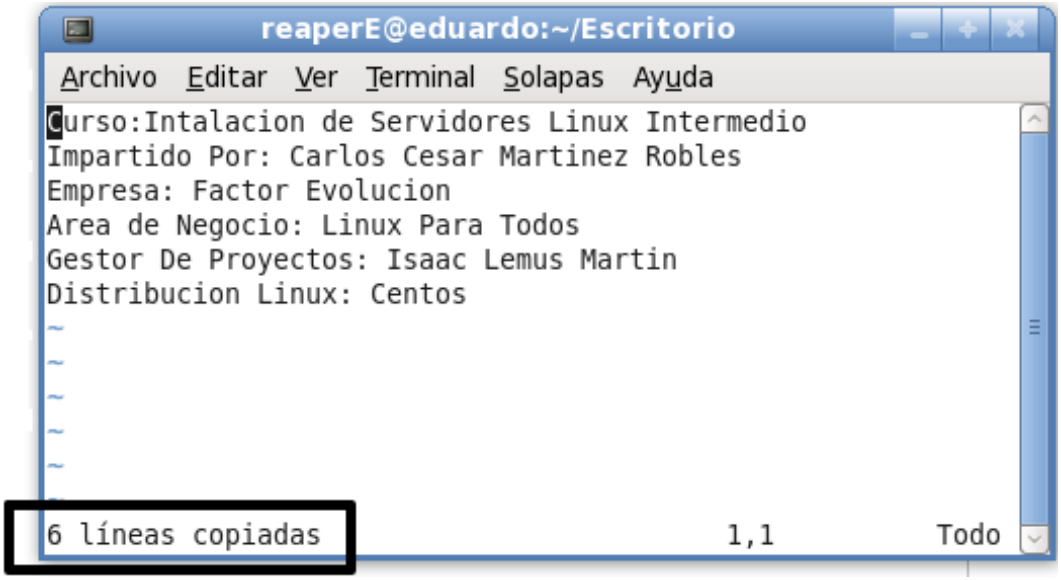
Como siguiente ejemplo copiaremos el párrafo completo que introducimos anteriormente, para ello tenemos que cambiarnos al modo de comandos de VI lo cual podemos conseguir tecleando el botón **"Esc"**

Una vez ubicados en el modo de comandos teclee la siguiente combinación de teclas:



La letra **“n”** indica el numero de lineas que deseamos copiar a partir de donde esta el cursor.

En este caso sustituiremos la letra **“n”** por el numero **'6'** ya que son **'6'** el numero de lineas que conforman nuestro párrafo así como también ubicar el cursor en la primera linea del párrafo. Si todo fue bien ejecutado debemos observar el siguiente mensaje en la esquina inferior izquierda de la pantalla:

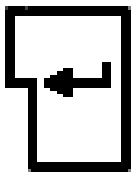


Algunas opciones mas acerca del copiado de texto pueden ser consultadas en el tema **“Referencia Rápida de Comandos de Vi”**

3.3.5 Pegar

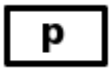
Para pegar el párrafo que acabamos de copiar primero y antes que nada debemos teclear el botón

esto para cambiarnos del modo de comandos de Vi al modo de inserción, esto con el fin de situarnos en la ultima linea del párrafo y con ello poder dar un espacio de separación entre el párrafo original y el párrafo copiado. Para dar el espacio de separación solo basta con teclear la tecla de “Enter”.

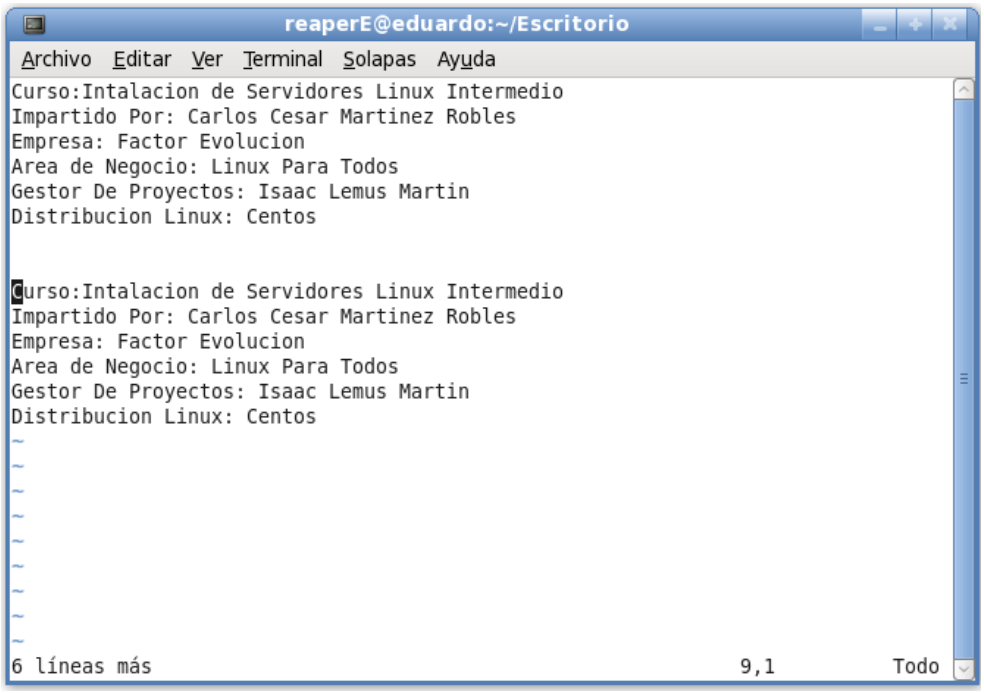


Y una vez mas regresar al modo de comando de Vi tecleando la tecla **“Esc”**

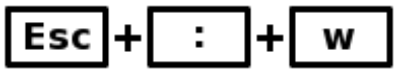
Para pegar el texto solo basta teclear la tecla **“p”**



Debe quedar como se muestra a continuación



Para guardar los cambios hechos al archivo solo tendrá que teclear los botones:



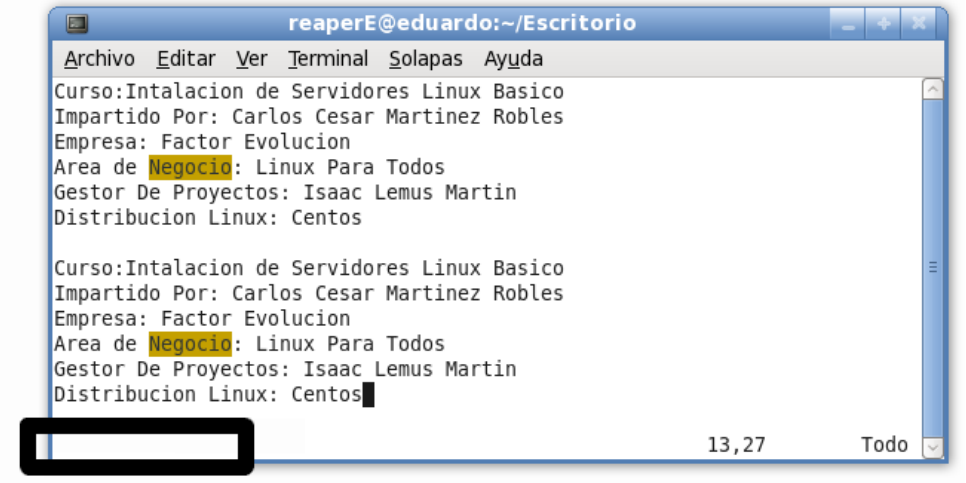
Recuerde que la tecla **“Esc”** nos permite cambiarnos del modo inserción al modo de comandos.

3.3.6 Buscar

La siguiente función sera la de buscar una palabra y acto seguido remplazarla por otra.

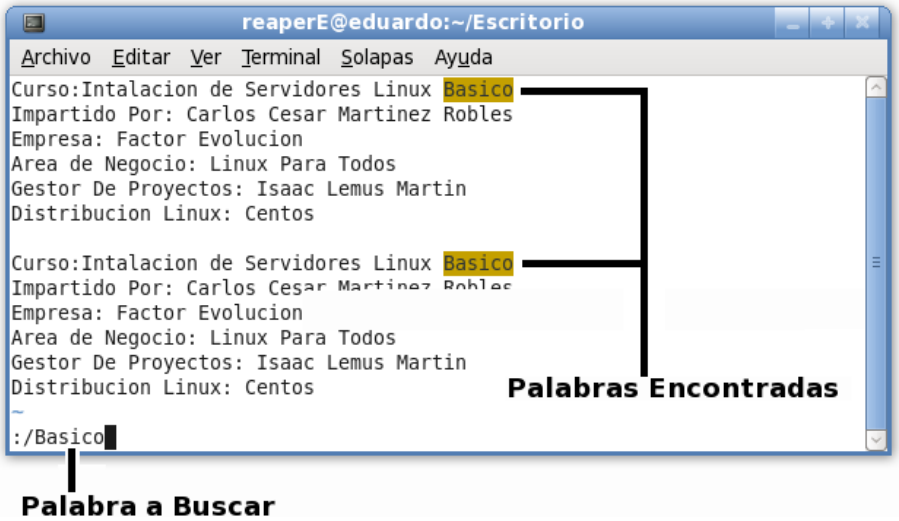
Para ello debemos entrar al modo de comandos de VI, si no recuerda como hacerlo no se preocupe, solo debe teclear el botón

como podemos observar la palabra “INSERTAR” ya no esta visible, esto indica que ya estamos dentro del modo de comandos de VI



Para comenzar la búsqueda de cualquier palabra solo tiene que teclear la siguiente combinación de botones:

La frase “palabraABuscar” debe reemplazarla por la palabra que usted esta buscando, como ejemplo nosotros buscaremos la palabra “Básico” dentro de todo el fichero.



Como podemos observar, VI nos remarco con un color diferente todas las palabras que este encontró relacionadas a la palabra **“Básico”.** Para navegar entre todas las búsquedas realizadas con la palabra **“Básico”** solo tiene que teclear (en modo de comandos) la tecla **“n”**

n

3.3.7 Reemplazar

Como siguiente paso, reemplazaremos la palabra “Básico” por “Intermedio”.

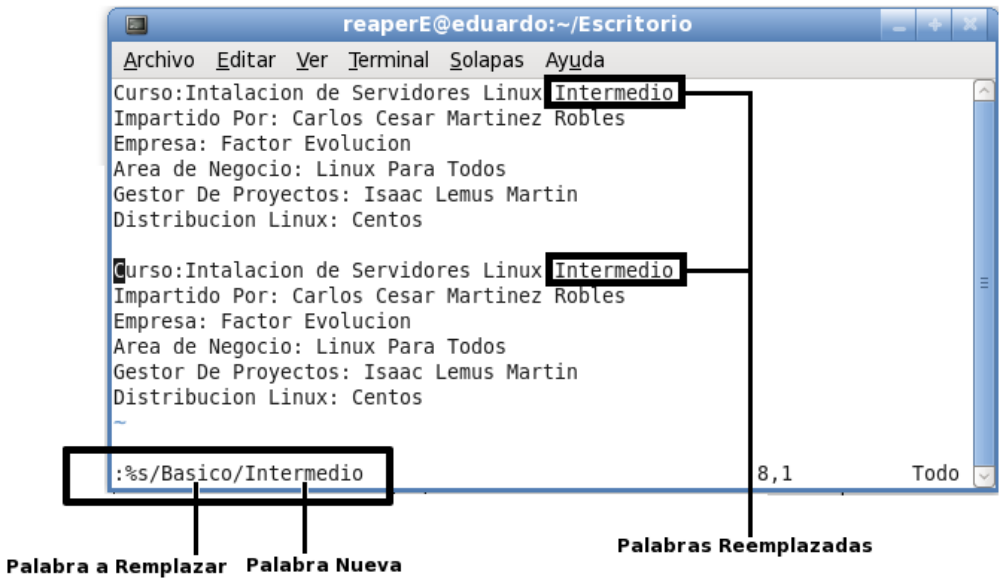
Para esto debemos estar en modo de comandos, y luego de ello teclear la siguiente sintaxis:

: + % + s + / + PalabraARemplazar + / + NuevaPalabra

Siguiendo la sintaxis anterior nosotros deberíamos teclear lo siguiente:

:%s/Basico/Intermedio

Y nos tendría que arrojar los siguientes resultados:



3.3.8 Cerrando el VI

Por ultimo solo nos resta guardar y cerrar el archivo , para ello tenemos que cambiarnos al modo de comandos de VI, por lo que tenemos que teclear el botón **“Esc”**

Esc

después solo habrá que teclear la combinación de teclas **“:wq”**

: + w + q

las letra **“w”** denota write o en español, guardar, la letra **“q”** denota quit o traducido en español, cerrar.

Para finalizar, sólo recordar que la documentación de **vitutor** es todo un libro en sí mismo, y que lo puedes completar con todos los recursos disponibles en la Red. Y para recordar toda la tabla de comandos existentes, lo mejor es practicar usando el editor, que (como me sucedió a mí) seguramente se acabará convirtiendo en una herramienta imprescindible para usted.

Así mismo, usted puede practicar usando el tutorial **vitutor** el cual puede lanzar escribiendo en una terminal de BASH lo siguiente:

```
[root@ localhost ]# vitutor
```

3.4 Referencia rápida de comandos

3.4.1 Ejecutando Vi y comandos para archivos

vi archivoNuevo	Abre o crea un archivo
vi /rutaDelArchivo/archivo	Abre o crea un archivo en la carpeta indicada
vi -r	Muestra archivos rescatados
vi -r archivo	Recupera archivos cerrados inadecuadamente
vi archivo1 archivo2	Abre múltiples archivos
vi **+n** archivo	Abre el archivo y posiciona el cursor en la linea **“n”**
vi **+/palabra** archivo	Abre el archivo y posiciona el cursor en la linea donde encuentra la **palabra**
:w	Guarda el archivo actual

3.4.2 Terminando y cerrando archivos

:q	Cierra el archivo actual
:q!	Cierra el archivo actual e ignora los cambios hechos al mismo
:wq	Guarda el archivo actual y cierra el mismo
:wq **archivo3**	Guarda el archivo actual, cierra el mismo y ademas lo renombra con el nombre de **“archivo3”**
:x	Guarda el archivo actual y cierra el mismo

3.4.3 Estableciendo opciones del archivo

:set	Muestra las opciones con las que fue generado el archivo
:set all	Muestra el menú de opciones que pueden ser implementadas al archivo
:set **opcionDelMenu**	Implementa al archivo alguna de las opciones del menú referente al comando anterior
:set **no[opcionDelMenu]**	Deshabilita alguna de las opciones implementadas al archivo
:set un	Habilita la numeración de las lineas en Vi
:set noun	Deshabilita la numeración de las lineas en Vi

3.4.4 Modificando el contenido del archivo

x	Borra el carácter en donde se encuentra ubicado el puntero
X	Borra el carácter antes del puntero
nx	Borra **n** cantidad de caracteres
dd	Borra una linea completa
ndd	Borra **n** lineas completas
dw	Borra la palabra donde se encuentra posicionado el puntero
ndw	Borra **n** cantidad de palabras
D	Borra desde la ubicación del puntero hasta el final de la linea
dL	Borra desde la ubicación del puntero hasta el final de la pantalla
dG	Borra desde la ubicación del puntero hasta el final del archivo
cw	Reemplaza la palabra en la cual se situá el puntero por un nuevo texto
J	Concatena la linea actual con la siguiente
~	Cambia de mayúscula a minúscula el carácter actual
u	Regresa a un estado antes el archivo
U	Regresa a un estado antes la línea actual
.	Repite el ultimo cambio de texto
>>	Mueve la línea actual a la derecha un tabulador
<<	Mueve la línea actual a la izquierda un tabulador

3.4.5 Búsqueda y remplazo de texto [En modo comandos de Vi]

/palabraABuscar	Hace una búsqueda de adelante hacia a tras del documento de la palabra especificada
?palabraABuscar	Hace una búsqueda de tras hacia adelante del documento de la palabra especificada
n	Se mueve de adelante hacia a tras de la siguiente ocurrencia de la palabra buscada
N	Se mueve de atrás hacia adelante de la siguiente ocurrencia de la palabra buscada
:s/actual/futuro	Sustituye la palabra **'actual'** por la palabra **'futuro'** en la línea actual
:s/actual/futuro/g	Sustituye todas las palabras **'actual'** por la palabra **'futuro'** en la línea actual
:%s/actual/futuro/g	Sustituye todas las palabras **'actual'** por la palabra **'futuro'** en todo el archivo
:s/actual/futuro/g/c	Sustituye todas las palabras **'actual'** por la palabra **'futuro'** en todo el archivo y ademas pide confirmación para efectuar los cambios

3.4.6 Copiando y pegando texto

y	Copia la linea en la cual se encuentra ubicado el puntero
yy	Copia la linea en la cual se encuentra ubicado el puntero
nyy	Copia n numero de lineas tomando como referencia la ubicación donde se encuentra ubicado el puntero
yw	Copia la palabra actual
pp	Pega después del cursor
P	Pega antes del cursor

Índice de contenido

Información de Derechos reservados de esta publicación.

Tema 6. Estados de Ejecución y Secuencias de Arranque

6.1 El Proceso de arranque

El proceso de arranque de un sistema operativo Linux se inicializa de la siguiente manera:

Cuando usted enciende su servidor o su computadora personal, esta hace que el BIOS de su equipo inicie las operaciones relacionadas con el arranque. El **BIOS** (Basic Input Output System) es un pequeño programa escrito en lenguaje ensamblador cuya función es cargar el sistema operativo en la memoria RAM (Random Access Memory), una vez que el BIOS carga el sistema operativo en RAM este inicia un proceso llamado **POST** (Power On Self Test) el cual es un proceso de diagnostico y verificación de los componentes de entrada y salida de un servidor o computadora y se encarga de configurar y diagnosticar el estado del hardware, una vez verificado el hardware se inicia la fase de arranque del sistema **(bootstrapping)** el cual cede el control al **GRUB** (Grand Unified Bootloader), el GRUB es un gestor de arranque que hace uso de un menú gráfico que permite elegir el Sistema Operativo que se desea arrancar; Así mismo, el GRUB realiza las siguientes tareas:

1. Cargar el kernel en memoria.
2. Cargar el sistema de ficheros virtual **initrd** el cual es usado tipicamente para hacer los arreglos necesarios antes de que el sistema de ficheros raíz pueda ser montado
3. Pasarle los argumentos **runlevel** e **init** al kernel
4. Comenzar la ejecución del **kernel**

Al terminar de ejecutar todas las tareas anteriores el GRUB le cede el control total del arranque al kernel y este a su vez se encarga de realizar la llamada a la función **starup** la cual tiene como función detectar el tipo de CPU con el que el equipo cuenta así como de lo principal del sistema operativo, como el manejo de memoria, planificador de tareas, entradas y salidas, comunicación interprocesos, y demás sistemas de control, a partir de este momento se ejecuta el proceso **INIT.**

6.2 El Proceso INIT

INIT es el primer proceso en ejecutarse despues de la carga del kernel de linux e implementa dos modelos bajo los cuales puede trabajar, estos son

1. SystemV
2. BSD

Estos modelos son arrancados por un programa (script) de arranque que establece como deben inicializarse los diferentes servicios, programas o registros que sean necesarios para que el sistema funcione como el administrador lo requiere.

Explicaremos brevemente como es que trabajan estos modelos

6.2.1 SystemV

Es un modelo usado para controlar el inicio y apagado del sistema y fue originalmente desarrollado por la compañía estadounidense de telecomunicaciones AT&T.

SystemV fue una de las versiones del sistema operativo Unix que se encargaba de controlar el arranque de los programas en el instante de inicio del equipo. Este modelo es considerado por muchos como facil, potente y flexible en comparacion con el sistema de inicio **BSD**

Existen cuatro versiones release de SystemV (**SVR**) , las cuales son:

1. SVR1.-Primera version de SystemV lanzada en 1984, incluia el editor de textos Vi
2. SVR2.-Incluye mejoras con respecto al nucleo el cual esta implementado como memoria virtual paginada, el sistema operativo Apple esta basado en este modelo.
3. SVR3.-Incluye mejoras en el sistema de ficheros asi como una nueva API de red, el sistema operativo AIX de IBM hace uso de este modelo
4. SVR4.- Fue la versión más popular de SVR asi como la fuente de varias características comunes del sistema operativo Unix, como el script /**etc/init.d**

6.2.1.1 Niveles de Ejecucion

Los niveles de ejecucion en SystemV describen ciertos estados del equipo los cuales se caracterizan por ejecutar ciertos procesos. En general existen 8 niveles de ejecucion los cuales van del 0 al 6 y S o s, que son alias del mismo nivel de ejecucion, de estos ochos niveles, tres son considerados reservados, estos son:

0.- Halt

1.-Single user mode

6.-Reboot

Aparte de los niveles de ejecucion 0,1 y 6 todos los sistemas operativos Linux tratan a los niveles de ejecucion un poco diferente. El denominador comun de todas las distribuciones linux es el fichero

```
/etc/inittab
```

el cual define lo que hace cada nivel de ejecucion.

A continuacion un ejemplo de cuantos niveles de ejecucion tienen cada una de las distribuciones mas importantes de linux, asi como del sistema operativo solaris y AIX

Sistema Operativo	Niveles de ejecucion por default
AIX	2
debian	2
gentoo linux	3

Sistema Operativo	Niveles de ejecucion por default
Mandriva	5
redhat.	3 o 5
fedora	3 o 5
slackware linux	3
suse A NOVELL BUSINESS	5
ubuntu	2
solaris	2

En la mayoria de los sistemas operativos linux los usuarios pueden saber bajo que nivel de ejecucion estan trabajando tecleando en una consola y como root lo siguiente:

```
[root@localhost ]$ runlevel
N 5
```

Existen tambien los ficheros llamados **rcN.d** en donde la letra **N** representa cada uno de los niveles de ejecucion en los que trabaja **init.d,** la funcion de estos ficheros se explicara mas a detalle en el siguiente tema.

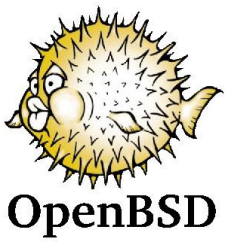
6.2.2 BSD

El modelo BSD init se ejecuta mediante el script de inicializacion situado en la ruta

```
/etc/rc
```

Algunos de los sistemas operativos que se basan en este modelo son los basados en BSD como:

- FreeBSD
- NetBSD
- OpenBSD
- DragonFlyBSD
- DesktopBSD
- PCBSD



6.3 El fichero init.d

En este fichero se encuentran todos los scripts encargados de levantar cada uno de los servicios del servidor.

La ubicación de este fichero esta localizada en:

Algunos de los servicios que podemos encontrar en el fichero init.d son los referentes a:

- Servidor Web Apache ---->httpd
- Servidor Samba -----> smb
- Servidor de Correo --->sendmail
- Servidor DHCP ---->dhcpd
- Servidor DNS ---->named
- Manejador de Base de Datos MySQL ---->mysqld

```
[root@localhost ~]# cd /etc/rc.d/init.d/
[root@localhost init.d]# ls -l
total 428
-rwxr-xr-x 1 root root  2974 jun 23  10:18 dhcpd
                  .
                  .
                  .
-rwxr-xr-x 1 root root  3099 feb 25  2008 httpd
-rwxr-xr-x 1 root root  4239 mar  3  2008 mysqld
                  .
                  .
                  .
-rwxr-xr-- 1 root root  6154 ago  6 05:05 named
-rwxr-xr-x 1 root root  1745 sep 18 10:26 smb
-rwxr-xr-x 1 root root  4112 mar 29  2008 sendmail
```

6.4 El fichero rcN.d

rcN.d es un conjunto de directorios que representan cada uno de los niveles de ejecucion del sistema operativo. Estos directorios a su vez contienen un conjunto de enlaces simbolicos a los scripts del directorio **/etc/rc.d/init.d**

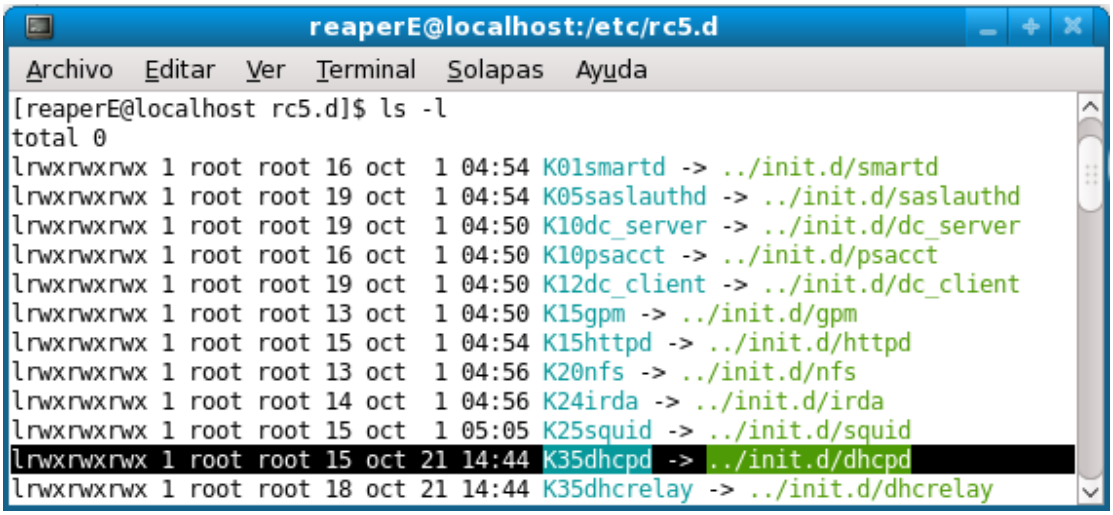
La funcion que desempeñan estos directorios es organizar la manera en como los servicios de un servidor son levantados, como por ejemplo, imaginemos que tenemos instalado un servidor Web apache, y que lo tenemos configurado para que trabaje en los niveles de ejecucion 3 y 5 , por ende deberiamos poder observar dichos enlaces simbolicos en las rutas

- /etc/rc.d/rc3.d
- /etc/rc.d/rc5.d

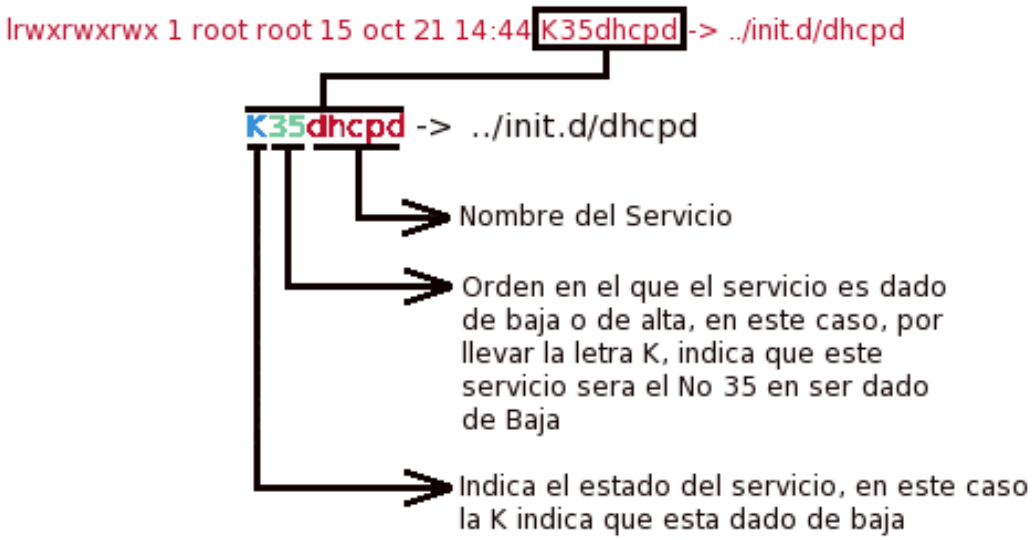
Otra de las caracteristicas de estos enlaces simbolicos es la sintaxis de sus propiedades. Esta sintaxis esta conformada por 3 parametros

1. El estado del servicio, los cuales son representados con dos variables:
    - La letra K.-Esta letra representa que el servicio esta dado de baja
    - La letra S.-Esta letra representa que el servicio esta dado de alta
2. El orden en el que es arrancado el servicio.- Este parametro indica el orden en el que los servicios deben ser dados de alta o de baja
3. El nombre del servicio

Un ejemplo de esto lo podemos observar de la siguiente tabla, la cual la tomamos de la ruta **/etc/rc.d/rc5.d**, lo cual indica que los scripts dentro de esta carpeta se ejecutan en el nivel de ejecucion 5



Los detalles del renglon subrayado se explican a continuacion:



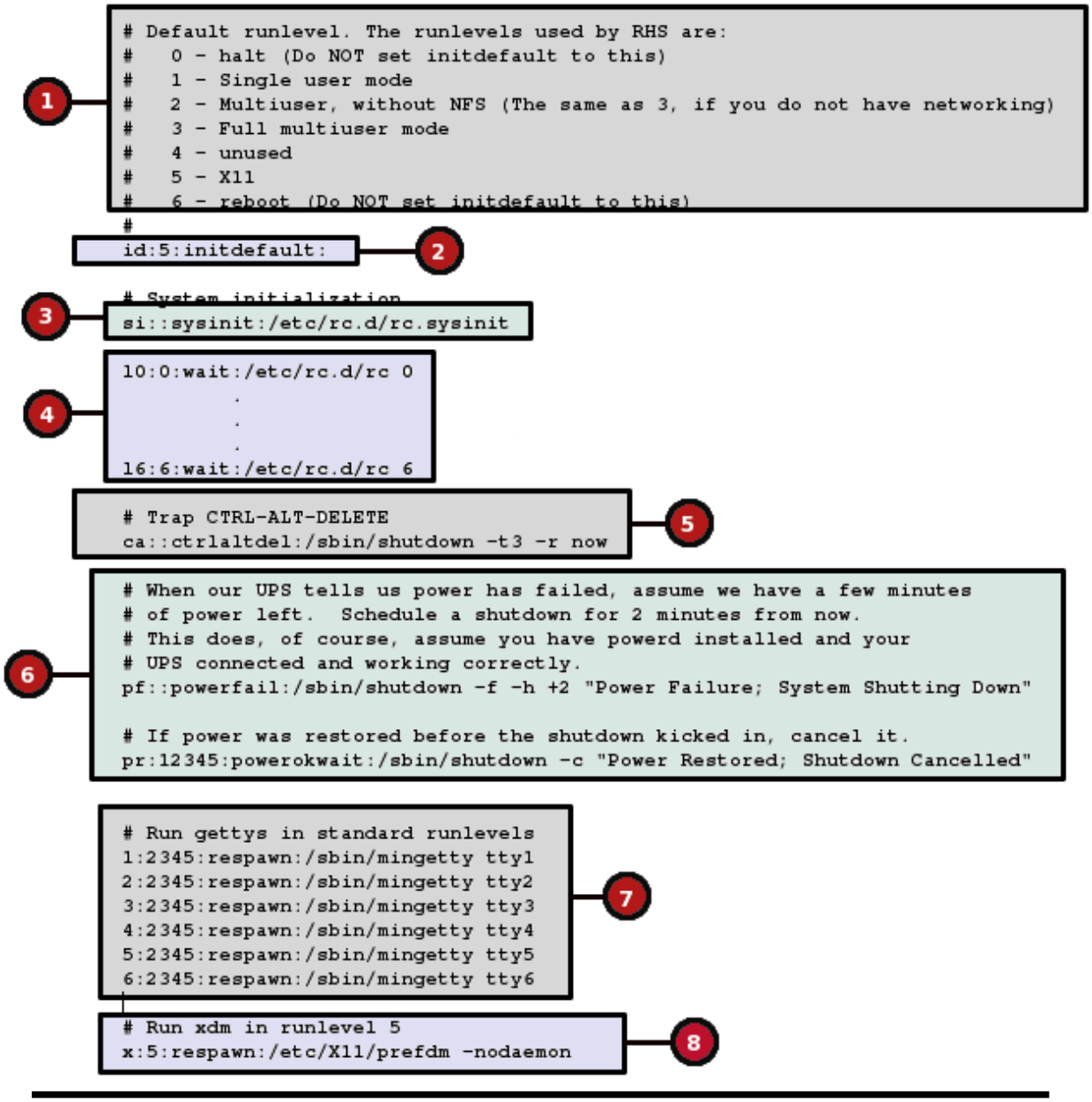
6.5 El fichero inittab

La ubicación de este fichero la podemos localizar en:

El fichero inittab describe que procesos se inician en la carga asi como los scripts de inicializacion del sistema, tambien distingue los multiples niveles de ejecucion bajo la cual trabaja el sistema operativo, recordemos que los niveles de ejecucion validos son 8, de los cuales tres son reservados y otro mas es alias de algun nivel en particular.

De acuerdo a lo mostrado en la siguiente imagen describiremos la funcion que desempeña cada linea.

Para ello usamos como ejemplo el fichero inittab del sistema operativo Centos version 5.2

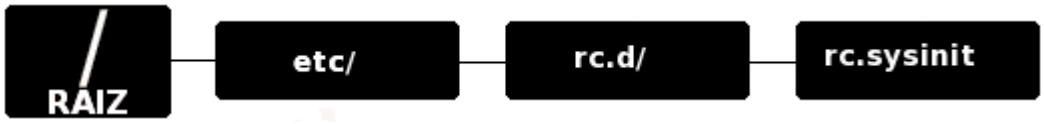


1. .- Este recuadro nos indica los diferentes niveles de ejecucion bajo los cuales trabaja CentOS 5.2
2. .-Este es el nivel de ejecucion en el cual arranca por defecto el equipo
3. .-Aqui se especifica que script de configuracion se debe cargar para el proceso de arranque del sistema
4. .-Aqui se especifican los scripts de arranque que el sistema utilizara para cada nivel de ejecucion o tambien llamados runlevels
5. .-Esta seccion controla el reseteo del sistema. Se puede comentar esta linea para que no pueda ser reseteado el sistema
6. .-Estas dos lineas estan relacionadas con las acciones que deben de seguirse en caso de una falla de voltaje y la segunda indica que debe hacerse cuando el voltaje ha sido restablecido.

7. Lineas encargadas de controlar los procesos getty
8. Esta linea arranca el entorno grafico del sistema, las cuales pueden ser GNOME o KDE

6.6 El fichero rc.sysinit

Este fichero esta localizado en la siguiente ruta

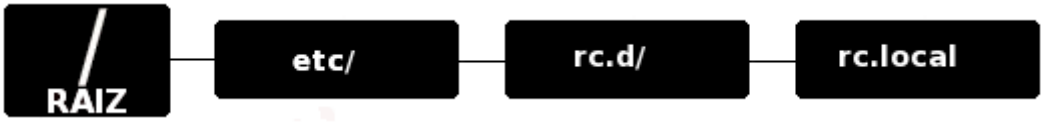


La funcion que desempeña este fichero es ejecutar una serie de scripts que inicializan tareas como:

- Configuracion de reloj del sistema
- Configuracion de los parametros del Kernel
- Levantamiento de dispositivos RAID y LVM
- Activacion y Actualizacion de cuotas en disco
- Activacion de la particion SWAP

6.7 El fichero rc.local

Este fichero esta localizado en la siguiente ruta



Este fichero es el utimo en ser ejecutado por el proceso **init.**

La funcion que tiene este script es agregar comandos que nos haga facil de realizar tareas necesarias como arrancar servicios especiales o inicializar dispositivos sin tener que escribir scripts complejos de inicializacion en el directorio /etc/rc.d/init.d ni creando enlaces simbolicos.

6.8 Niveles de Ejecucion

Los niveles de ejecucion o tambien llamados runlevels hacen referencia a los sistemas operativos Linux que implementan el estilo de sistema de arranque de iniciacion tipo UNIX System V del cual ya hemos hablando extensamente.

A lo largo de este tema mencionamos 8 niveles de ejecucion bajo los cuales trabajan algunos sistemas operativos linux, en especial los de la Familia Red Hat. A continuacion mencionaremos las caracteristicas de cada uno de ellos.

6.8.1 Nivel 0 –Parada Del Sistema

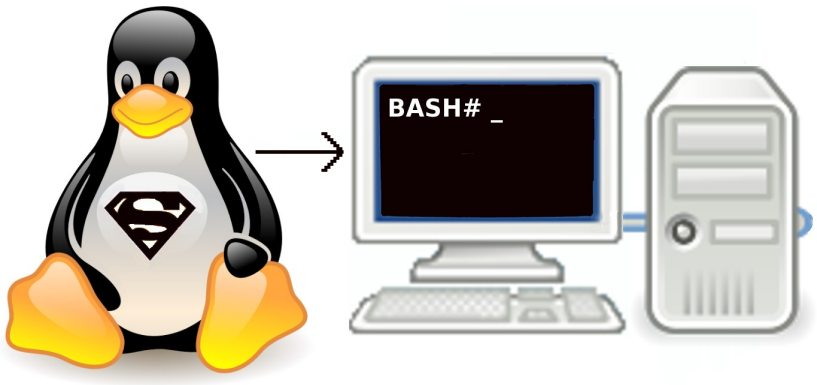
El nivel 0 es usado para especificarle al sistema que debe apagarse, la forma en que este lo hace es a travez del comando halt.

Al ejecutarse este comando se apagan todos los servicios que se encuentren activos

6.8.2 Nivel 1 o S -Monousuario o Single User

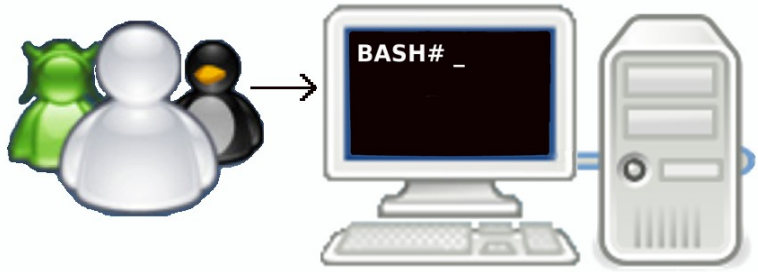
El nivel 1 o tambien llamado nivel Single (S) solo puede ser iniciado por el administrador del sistema (root), por lo que ningun usuario podra hacer eso de este nivel de ejecucion

En este nivel no se activan los servicios de Red, y tampoco se inician los procesos (daemons) de inicio por lo que permite reparar problemas o hacer pruebas al sistema.



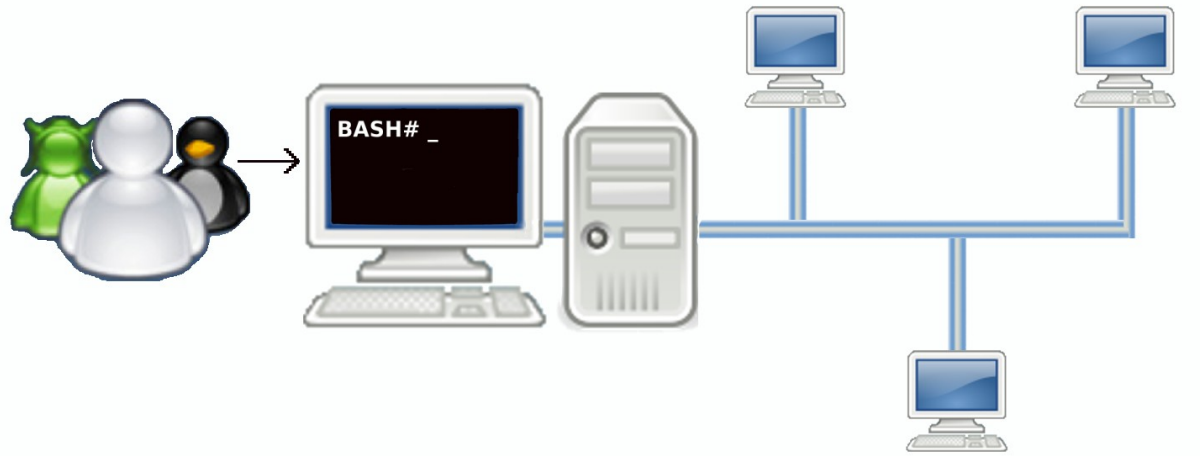
6.8.3 Nivel 2 -Multiusuario sin Red

Este nivel esta caracterizado por la capacidad de permitir que varios usuarios puedan entrar al sistema pero sin contar con soporte en red, esto quiere decir que no se puede contar con servidores como NFS o web.



6.8.4 Nivel 3 -Multiusuario con Red

Este sistema esta caracterizado por la capacidad de permitir a varios usuarios entrar al sistema, a diferencia del nivel de ejecucion 2, este si cuenta con soporte de red.

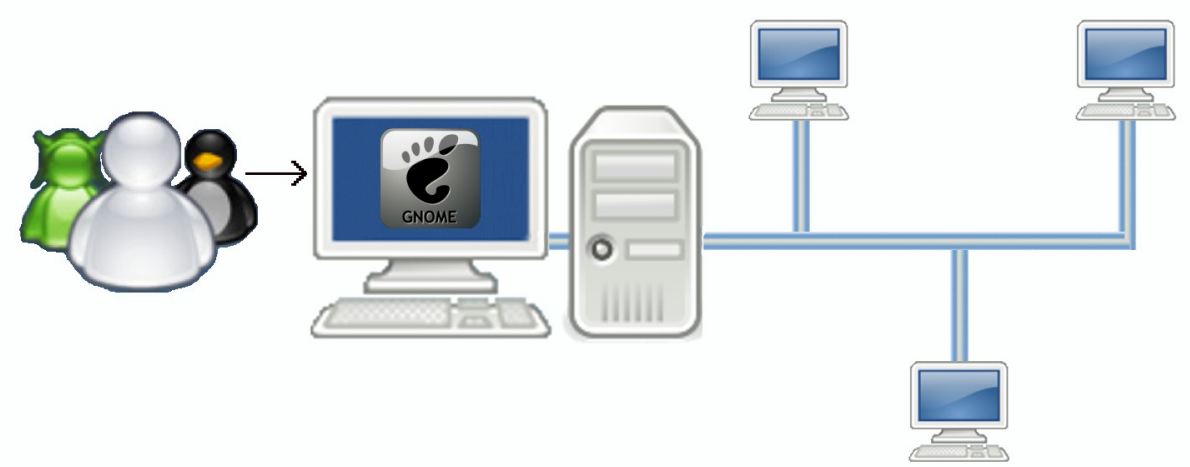


6.8.5 Nivel 4. -Sin Uso

Para la mayoria de las distribuciones linux este nivel de ejecucion no tiene asignada ninguna funcion, pero puede ser personalizado por el administrador para que cumpla con alguna funcion en especial

6.8.6 Nivel 5. -Multiusuario Grafico

Este nivel de ejecucion es identico al nivel 3, la unica diferencia es el alta de entornos graficos como GNOME o KDE para la administracion del sistema



6.8.7 Nivel 6. -Reinicio del Sistema

6.9 Comando chkconfig

Este comando es una herramienta util para levantar o desactivar servicios los cuales son aplicados durante el arranque del equipo asi como tambien conocer el estado de los servicios que se estan ejecutando.

- Para conocer el estado de los procesos que estan corriendo en su sistema puede ejecutar el siguiente comando

```
[root@localhost ~]#chkconfig  --list
```

- Para conocer el status de algun proceso en particular solo teclee esto

```
[root@localhost ~]#chkconfig --list httpd
httpd           0:desactivado   1:desactivado   2:desactivado
3:desactivado   4:desactivado   5:desactivado   6:desactivado
```

Lo cual nos mostrara bajo que niveles de ejecucion esta corriendo el proceso o servicio.

- Para levantar algun proceso o servicio durante el arranque del sistema solo teclee esto

```
[root@localhost ~]#chkconfig --level 35 httpd on
```

De esta manera estamos especificando el sistema que siempre que este inicie levante el servidor web apache en los niveles de ejecucion 3 y 5

- Para detener algun proceso o servicio durante el arranque del sistema solo teclee esto

```
[root@localhost ~]#chkconfig --level 35 httpd off
```

De esta manera estamos especificando el sistema que siempre que este inicie tenga detenido el servidor web apache en los niveles de ejecucion 3 y 5

6.10 Levantando, deteniendo y reiniciando servicios

Otra forma de levantar, detener o reiniciar servicios en caliente es mediante el uso del siguiente comando el cual hace uso del fichero init.d del cual hemos hablado anteriormente.

La estructura de la sintaxis para poder ocupar el comando es la siguiente:

```
[root@localhost ~]#/etc/init.d/nombreDelServicio  {start|stop|status|
restart|reload}
```

A manera de ejemplificar el uso del anterior comando haremos lo siguiente.

Supongamos que tenemos ya instalado y configurado un servidor web apache y lo unico que falta es levantar el servicio, para ello solo bastara teclear lo siguiente:

```
[root@localhost ~]#/etc/init.d/httpd start
```

Para detener este mismo servicio solo debemos cambiar la palabra **start** por **stop**

```
[root@localhost ~]#/etc/init.d/httpd stop
```

De igual manera si se quiere reiniciar el servicio solo debemos cambiar la palabra **stop** por **restart**

```
[root@localhost ~]#/etc/init.d/httpd restart
```

Otra manera de arrancar, detener o reiniciar servicios sin necesidad de teclear toda la ruta anterior es mediante el uso de un alias el cual tiene la siguiente sintaxis

```
[root@localhost ~]# service httpd {start|stop|status|restart|reload}
```

De igual forma solo debemos teclear start, stop o restar según sea el caso

Ejemplo

```
[root@localhost ~]#service httpd start
```

Índice de contenido

Información de Derechos reservados de esta publicación.

Tema 6. Comandos Linux Basicos

6.1 Informacion del Sistema

A continuacion daremos una serie de comandos utiles para conocer aspectos generales del sistema

6.1.1 arch

Este comando sirve para mostrarnos la arquitectura del procesador de nuestro sistema

```
[root@localhost ~]# arch
x86_64
```

6.1.2 uname [parametros]

La funcion de este comando es similar al anterior, la unica diferencia es que este nos arroja mas informacion del sistema de acuerdo al numero de parametros que le pasemos.

Los parametros que podemos usar son:

- a.- Imprime el nombre kernel,del equipo, version del kernel, fecha en que fue apagado el sistema por ultima vez, arquitectura del sistema
- s.-Imprime el nombre del kernel
- n.-Imprime el nombre del equipo
- r.-Imprime version del kernel
- i o p.-Imprime la arquitectura del equipo
- o.-Imprime el nombre del sistema operativo

Ejemplo:

```
[root@localhost ~]# uname -a
Linux localhost.localdomain 2.6.25-14.fc9.x86_64 #1 SMP Thu May 1 06:06:21
EDT 2008 x86_64 x86_64 x86_64 GNU/Linux
```

6.1.3 dmidecode

Lo que hace este comando es leer la información del BIOS directamente y regresar un listado muy completo de todo el hardware encontrado en el equipo. DMI es por Desktop Management interface y lee la información del llamado SMBIOS (System Management BIOS).

dmidecode por defecto ofrece un listado bastante largo y completo, asi que si deseas uno más corto o resumido, úsalo con *-q*.

Ejemplo:

```
[root@localhost ~]# dmidecode -q
BIOS Information
        Address: 0xF0000
        Runtime Size: 64 kB
        ROM Size: 512 kB
        Characteristics:
        PCI is supported
```

6.1.4 cat /proc/cpuinfo

Nos muestra la informacion referente al procesador del sistema

Ejemplo:

```
[root@localhost ~]# cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 15
model           : 107
model name      : AMD Athlon(tm) 64 X2 Dual Core Processor 4000+
stepping        : 1
cpu MHz         : 2009.260
cache size      : 512 KB
```

6.1.5 cat /proc/meminfo

Verifica el uso de la memoria

Ejemplo:

```
[root@localhost ~]# cat /proc/meminfo
MemTotal:      3030856 kB
MemFree:        571796 kB
Buffers:         88272 kB
Cached:        1393576 kB
SwapCached:          0 kB
```

6.1.6 cat /proc/swaps

Nos muestra el uso del espacio en memoria SWAP

Ejemplo:

```
[root@localhost ~]# cat /proc/swaps
Filename         Type            Size     Used    Priority
/dev/sda4        partition       2096472  0       -1
```

6.1.7 cat /proc/net/dev

Verifica adaptadores de red y sus estadisticas

Ejemplo:

```
[root@localhost ~]# cat /proc/net/dev
Inter-|   Receive                                                |  Transmit
 face |bytes    packets errs drop fifo frame compressed multicast|bytes
packets errs drop fifo colls carrier compressed
```

6.1.8 cat /proc/mounts

Nos muestra los sistemas de ficheros que se encuentran montados

Ejemplo:

```
[root@localhost ~]# cat /proc/mounts
rootfs / rootfs rw 0 0
/dev/root / ext3 rw,relatime,errors=continue,user_xattr,acl,data=ordered 0 0
/dev /dev tmpfs rw,relatime,mode=755 0 0
/proc /proc proc rw,relatime 0 0
/sys /sys sysfs rw,relatime 0 0
none /selinux selinuxfs rw,relatime 0 0
/proc/bus/usb /proc/bus/usb usbfs rw,relatime 0 0
devpts /dev/pts devpts rw,relatime,gid=5,mode=620 0 0
tmpfs /dev/shm tmpfs rw,relatime 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw,relatime 0 0
sunrpc /var/lib/nfs/rpc_pipefs rpc_pipefs rw,relatime 0 0
fusectl /sys/fs/fuse/connections fusectl rw,relatime 0 0
```

6.1.9 lspci -tv

Nos lista los dispositivos PCI con lo que dispone el equipo

Ejemplo:

```
[root@localhost ~]# lspci -tv
nVidia Corporation MCP61 Memory Controller
nVidia Corporation MCP61 LPC Bridge
nVidia Corporation MCP61 SMBus
nVidia Corporation MCP61 Memory Controller
nVidia Corporation MCP61 SMU
nVidia Corporation MCP61 USB Controller
nVidia Corporation MCP61 USB Controller
ADMtek NC100 Network Everywhere Fast Ethernet 10/100
nVidia Corporation MCP61 High Definition Audio
nVidia Corporation MCP61 IDE
nVidia Corporation MCP61 Ethernet
 nVidia Corporation MCP61 SATA Controller
nVidia Corporation GeForce 6100 nForce 405
Advanced Micro Devices [AMD] K8 [Athlon64/Opteron] HyperTransport Technology
Configuration
dvanced Micro Devices [AMD] K8 [Athlon64/Opteron] Address Map
Advanced Micro Devices [AMD] K8 [Athlon64/Opteron] DRAM Controller
Advanced Micro Devices [AMD] K8 [Athlon64/Opteron] Miscellaneous Control
```

6.1.10 lsusb -tv

Nos lista los dispositivos USB con lo que dispone el equipo

Ejemplo:

```
[root@localhost ~]# lspci -tv
Bus#  2
`-Dev#   1 Vendor 0x1d6b Product 0x0001
Bus#  1
`-Dev#   1 Vendor 0x1d6b Product 0x0002
```

6.1.11 date

Nos muestra la fecha que tiene registrado el sistema

Ejemplo:

```
[root@localhost ~]# date
mié oct 29 13:52:34 CST 2008
```

En caso de querer modificar la fecha solo se debe de seguir la siguiente sintaxis

```
date [MesDiaHoraMinutoAño.Segundos]
```

Ejemplo:

```
[root@localhost ~]# date 041217002007.00
```

6.1.12 dmesg

dmesg es principalmente usado para mostrar los mensajes que se mostraron en pantalla cuando se arranco el sistema. Se usa sobre todo para realizar depuraciones al sistema de como se están cargando los diversos módulos y componentes al arranque del sistema o ya en ejecución. Debido a lo extenso del sistema, es conveniente redireccionar la salida a un archivo lo cual se puede hacer de la siguiente manera

```
[root@localhost ~]# dmesg > mensajes.txt
```

6.1.13 w

Nos indica los usuarios que se encuentran en el sistema asi como lo que hacen en el

Ejemplo:

```
[root@localhost ~]# w
administrador@repoubuntu:~$ w
 11:32:50 up 12 days, 22:25,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
administ pts/0    192.168.1.77     11:32    0.00s  0.10s  0.00s w
```

6.1.14 df -h

Nos reporta el uso de espacio en los discos duros
Ejemplo

```
[root@localhost ~]# df -h
S.ficheros          Tamaño Usado  Disp Uso% Montado en
/dev/sda2              79G   45G   31G  60% /
tmpfs                 1,5G     0  1,5G   0% /dev/shm
```

6.1.15 ps -xa

Este comando lista los procesos que se estan ejecutando en el sistema

```
[root@localhost ~]# ps -xa
    S      0:00 /usr/libexec/gdm-session-worker
 2389 ?        S      0:03 /usr/libexec/gconfd-2 4
 2391 ?        S      0:00 /usr/bin/gnome-keyring-daemon -d --login
 2392 ?        Ssl    0:00 gnome-session
 2401 ?        S      0:00 dbus-launch --sh-syntax --exit-with-session
```

6.1.16 mkdir

Este comando sirve para crear una carpeta

Ejemplo:

```
[root@localhost ~]# mkdir Documentos
```

Tambien puede usarse en conjunto con el parametro **-p** para crear un arbol de carpetas

Ejemplo

```
[root@localhost ~]# mkdir -p empresaX/ventas/ricardo
```

6.1.17 touch

Sirve para generar archivos sin contenido

Ejemplo

```
[root@localhost ~]# touch datos1.txt
[root@localhost ~]# touch info.txt
[root@localhost ~]# touch direcciones.txt
[root@localhost ~]# touch contactos.txt
[root@localhost ~]# touch salarios.txt
```

6.1.18 cd

Comando que nos permite movernos entre directorios, su sintaxis es:

```
cd  [carpetaDondeQuieroMoverme]
```

Ejemplo:

```
[root@localhost ~]# cd Documentos
[root@localhost Documentos~]#
```

para regresar un nivel entre directorios es:

```
[root@localhost Documentos~]# cd ..
[root@localhost ~]#
```

6.1.19 cp

Comando que sirve para copiar archivos o carpetas, su sintaxis es

```
cp [parametros] [archivo/Directorio] [rutaDestino]
```

Los parametros son:

-R -Copia directorios recursivamente

-v -Muestra el estado de la copia

-f -Forza la copia sin pedirnos confirmacion

Ejemplo 1:

Copiando un archivo a una carpeta

```
[root@localhost ~]# cp archivosX.txt /home/carlos/pruebas
```

Ejemplo 2:

Copiando una carpeta a otra carpeta

```
[root@localhost ~]# cp -Rvf misArchivos /home/carlos/pruebas
```

6.1.20 mv

Comando que sirve para mover archivos o carpetas, su sintaxis es

```
mv [parametros][archivo/Directorio] [rutaDestino]
```

Los parametros son:

-v -Muestra el estado del proceso

-f -Forza el movimiento sin pedirnos confirmacion

Ejemplo 1:

Moviendo un archivo a una carpeta

```
[root@localhost ~]# mv archivosX.txt /home/carlos/pruebas
```

Ejemplo 2:

Moviendo un archivo a una carpeta

```
[root@localhost ~]# mv misArchivos /home/carlos/pruebas
```

6.1.21 rm

Comando que sirve para eliminar archivos o carpetas, su sintaxis es

```
rm [parametros] [archivo/Directorio]
```

Los parametros son:

-R -Borra directorios recursivamente

-v -Muestra el estado de la borrado

-f -Forza el borrado sin pedirnos confirmacion

Ejemplo 1:

```
[root@localhost ~]# rm archivosX.txt
```

Ejemplo2:

```
[root@localhost ~]# rm  -Rfv carpetaCompartida
```

6.1.22 ls

Lista los archivos que contiene una carpeta, su sintaxis es

```
ls [parametros]
```

Los parametros son:

-l -Muestra los detalles de archivos y carpetas

-a -Muestra los archivos o carpetas ocultas

Ejemplo:

```
[root@localhost ~]# ls -l
total 255344
drwx------ 2 reaperE reaperE      4096 oct 30 11:52 amsn_received
-rw-r--r-- 1 reaperE reaperE 256753963 oct 22 10:37 anterior.tar.gz
-rw-rw-r-- 1 reaperE reaperE     10475 oct 22 17:34 barra firefox.png
-rwxr-xr-x 1 reaperE reaperE     14395 oct  1 12:26 Configuracion MySql.sxw
drwxr-xr-x 2 reaperE reaperE      4096 oct  2 10:26 Descargas
drwxr-xr-x 2 reaperE reaperE      4096 oct 22 12:32 Documentacion RedHat
```

6.1.23 find

Busca archivos en una ruta especifica, su sintaxis es

```
find [ruta] [expresion]
```

Ejemplo1.- Buscar archivos y carpetas con el nombre “expedienteX” en todo el directorio Raiz

```
[root@localhost ~]# find / -name expedienteX
```

Ejemplo 2.-Buscar archivos y carpetas que le pertenezcan al usuario “cmartinez” en todo el directorio raiz

```
[root@localhost ~]# find / -user cmartinez
```

Ejemplo 3.-Buscar archivos con extension .bin dentro del directorio '/home/ilemus'

```
[root@localhost ~]# find /home/ilemus -name \*.bin
```

Ejemplo 4.-Buscar archivos binarios que no han sido usados en los ultimos 100 dias

```
[root@localhost ~]# find /usr/bin -type f -atime +100
```

Ejemplo5.-Buscar archivos binarios creados o modificados en los ultimos diez dias

```
[root@localhost ~]# find /usr/bin -type f -mtime -10
```

Ejemplo 6.-Mostrar archivos con la extension “.ps”

Hay que destacar que para hacer uso de este comando primero se tiene que ejecutar el comando **updatedb**

```
[root@localhost ~]# find / -user cmartinez
```

6.1.24 updatedb

Este comando sirve para actualizar la base de datos de nuestro sistema

6.1.25 mount

El comando mount nos sirve para montar desde particiones de disco, hasta dispositivos externos como cd's, dvd's, floopy drives, imagenes ISO, o dispositivos de almacenamiento masivo de datos.

La manera de usar este comando es la siguiente:

Ejemplo1. Montando un DVD

```
[root@localhost ~]# mount /dev/dvd /mnt/caspetaDeMontaje
```

Ejemplo 2. Montando en CD

```
[root@localhost ~]# mount /dev/cdrom /mnt/caspetaDeMontaje
```

Ejemplo 3. Montando un floppy drive

```
[root@localhost ~]# mount /dev/fd /mnt/caspetaDeMontaje
```

Ejemplo 4. Montando un dispositivo USB

```
[root@localhost ~]# mount /dev/usbdisk /mnt/caspetaDeMontaje
```

Ejemplo 5.- Montando una imagen ISO

```
[root@localhost ~]# mount -iso9660 -o loop fichero.iso /mnt/caspetaDeMontaje
```

Ejemplo 6.- Montando un sistema de ficheros de Windows

```
[root@localhost ~]# mount -t vfat /dev/particionWindows /mnt/caspetaDeMonta
```

Ejemplo 7.- Montando un sistema de ficheros de Linux

```
[root@localhost ~]# mount -t ext3 /dev/particionLinux /mnt/caspetaDeMontaje
```

6.2 Compresion de Archivos

6.2.1 tar

El comando tar es utilizado normalmente para empaquetar o desempaquetar archivos.

La sintaxis para el buen uso de este comando es:

```
[root@localhost ~]# tar [parametros] [fichero1] [fichero2]
```

Los parametros son:

c.- Crea un fichero tar

v. -Muestra el estado de la borrado

x.-Extrae los archivos (descomprime los ficheros que se encuentran dentro del archivo tar)

z.-Comprime el archivo tar con gzip

j.-Comprime el archivo tar bzip

f.-Al usar el parametro -c junto con este parametro se especifica que se utilizara el nombre del archivo especificado para la creacion del archivo tar

Ejemplo 1.- Empaquetar un archivo con TAR

```
[root@localhost ~]# tar -cvf archivo.tar directorioAComprimir
```

Ejemplo 2.-Desempaquetar ficheros TAR

```
[root@localhost ~]# tar -xvf archivo.tar
```

Ejemplo 3.-Comprimir una carpeta con TAR.GZ

```
[root@localhost ~]# tar -czvf archivo.tar.gz directorioAComprimir
```

Ejemplo4.-Descomprimir una carpeta TAR.GZ

```
[root@localhost ~]# tar -xzvf archivo.tar.gz
```

Ejemplo 5.-Comprimir una carpeta con TAR.BZ

```
[root@localhost ~]# tar -cjvf archivo.tar.bz directorioAComprimir
```

Ejemplo 6.-Descomprimir una carpeta TAR.BZ

```
[root@localhost ~]# tar -xvf archivo.tar.bz
```

6.2.2 zip

El comando zip es utilizado normalmente para comprimir paquetes.

La sintaxis para el buen uso de este comando es:

```
[root@localhost ~]# zip [parametros]
```

Ejemplo 1. Comprimiendo un archivo con ZIP

```
[root@localhost ~]# zip archivo.zip ficheros
```

Ejemplo 2.-Descomprimiendo un archivo ZIP

```
[root@localhost ~]# unzip archivo.zip
```

Índice de contenido

Información de Derechos reservados de esta publicación.

Tema 4a. Configuracion de los Parametros de Red

4a.1 Configuracion de interfaces de red

La configuración de la interfaz es importante en un servidor o equipo de escritorio. Los principales archivos de configuración son

/etc/hosts	Este archivo de configuración contiene los nombres de equipos dentro de una red local y se utilizar para resolver su nombre cuando no se tiene un servidor de DNS en la red local, también este archivo define la dirección de loopback que representa al propio equipo independientemente de la dirección IP que se le haya asignado.
/etc/resolv.conf	Este archivo especifica las direcciones IP de los servidores DNS
/etc/sysconfig/network	Este archivo de configuración es utilizado para definir las características de red deseadas
/etc/sysconfig/network-scripts/ifcfg-<interfaz>	Estos archivos de configuración son utilizados para especificar la configuración de la tarjeta de red.

4a.1.1 Configuracion del archivo /etc/hosts

Este archivo de texto asocia las direcciones IP con el nombre del equipo (hostname). Este archivo debe tener la siguiente forma:

Direccion IP	nombre.del.equipo	alias

Las modificaciones realizadas en este archivo de configuración son reflejados inmediatamente

Nota: Este archivo se encuentra la dirección de loopback (127.0.0.1), esta dirección es utilizada por varias aplicaciones para su funcionamientos, se recomienda que no modifique esta linea.

Ejemplo:

```
127.0.0.1          localhost.localdomain          localhost
192.168.1.10       mail.redfactor.net      mail
192.168.1.13       www.red.factor.net                www
207.249.0.40       www.linuxparatodos.net
```

4a.1.2 Configuracion del archivo /etc/resolv.conf

Este archivo de configuración contiene la direcciones IP de los servidores DNS. Sus parámetros de configuración son:

nameserver	Define las direcciones IP de los servidores de nombre en los cuales se deberán resolver las búsquedas. El archivos hosts solo permite hasta 3 servidores de nombre diferentes
domain	Define el nombre de dominio local en el cual pertenecen los equipos en una red local.
search	Este parámetro define la lista de búsqueda nombres de equiposes útil cuando se busca un equipo dentro de la red local por un nombre corto
sortlist	Este parámetro indica la preferencia de los nameserver definidos

4a.1.3 Configuracion del archivo /etc/resolv.conf

Los parámetros que utiliza este este archivo son:

NETWORKING	Los valores que admites son: ● yes Permite la configuración de los servicio de red. ● no No permite la configuración de los servicio de red.
FORWARD_IPV4	Habilita el reenvío de paquetes. Los valores que admite son yes o no.
HOSTNAME	Define el nombre del equipo, el cual debe de tener la forma del *Fully Qualified Domain Name* (*FQDN*). Por ejemplo: **equipo.ejemplo.net**
GATEWAY	Este parametro define la dirección IP del Gateway

4a.1.4 Configuración de la interfaz de red

El directorio de configuración de la interfaz de red se encuentra en:

/etc/sysconfig/network-scripts/

Dentro de este directorio se encuentran los archivos de configuración de los dispositivos, dependiendo del numero de interfaces de red instaladas en el computadora será el numero de archivos de configuración, el nombre de estos archivos depende del tipo de dispositivo

Ethernet	ifcfg-eth0, ifcfg-eth1, ..., ifcfg-eth**N**.
Wi-Fi	ifcfg-wlan0, ifcfg-wlan1, ..., Ifcfg-wlan**N**.
Modem	ifcfg-ppp0, ifcfg-ppp1, ..., ifcfg-ppp**N**.

en donde **N** representa el numero de interfaz a configurar.

Los parámetros que admiten los archivos de configuración de la interfaz de red Ethernet son los siguientes:

DEVICE	Define el nombre del dispositivo físico
BOOTPROTO	none No utiliza ningún protocolo de arranque. static Se define de forma manual los parámetros de red. dhcp Obtiene los parámetros de red por medio de un servidor de DHPC
IPADDR	Define la dirección IP asignada a ese dispositivo.
NETMASK	Define la mascara de red.
NETWORK	Define el segmento de red
HWADDR	Define el dirección MAC del dispositivo de red. Se recomienda que modificar el valor de este parámetro.
GATEWAY	Define la Dirección IP del Gateway en la red
ONBOOT	Establece si el dispositivo debe activarse con los servicios de red
DNS1, DNS2	Define la direcciones de los servidores DNS primario y secundario a utilizar.
DHCP_HOSTNAME	Esta opción establece un nombre al equipo. Utilice esta opción si el servidor DHCP requiere que el cliente especifique el nombre de su equipo antes de recibir una dirección IP.

Ejemplo del archivo de configuración.

```
DEVICE=eth0
BOOTPROTO=static
IPADDR=192.168.2.10
NETMASK=255.255.255.0
NETWORK=192.168.2.0
GATEWAY=192.168.2.254
DNS1=192.168.2.1
HWADDR= 00:1E:EC:6E:CD:51
```

Índice de contenido

Información de Derechos reservados de esta publicación.

Tema 4. Instalación y Configuración de un servidor DHCP

4.1 Introducción a DHCP

DHCP (Dinamic Host Control Protocol) es un protocolo de red utilizado para asignar una serie de configuraciones TCP/IP (dirección IP, nombre de la maquina,dominio al que pertenece, routeador, servidor DNS, gateway) a los equipos que forman parte de una red de área local LAN (Local Area Network).

El DHCP es un protocolo de tipo cliente/servidor que se comunica por el puerto 67 y 68 a través de UDP, generalmente un servidor DHCP posee una lista de direcciones IP dinámicas y las va asignando a las maquinas clientes conforme estas van estando disponibles.

Sin el uso de un servidor DHCP, cada dirección IP se tendría que configurar manualmente en cada equipo y, si el equipo se mueve a otra subred, la IP del equipo seria diferente a la establecida antes. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si el equipo es conectado en un lugar diferente de la red.

4.1.1 Funcionamiento de un DHCP

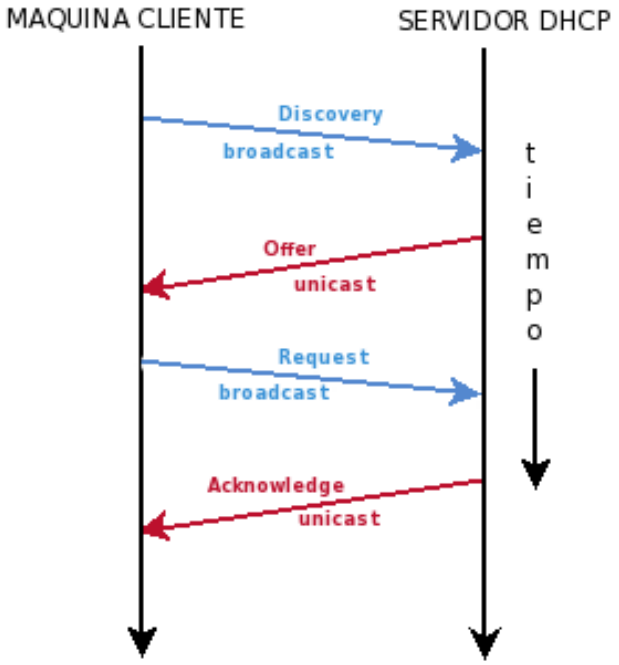
Antes que nada hay que tener en cuenta que nuestro servidor DHCP debe contar con una dirección IP fija, por lo tanto en nuestra red solo existirá un equipo que dispondrá de una IP fija, o sea, nuestro servidor DHCP.

El paso siguiente es cuando la maquina cliente se conecta a la red, en este fase, la maquina cliente hace uso del sistema básico de comunicación BOOTP**.** El **BOOTP** (**Boot**strap **P**rotocol) es un protocolo de red **UDP** utilizado para obtener la dirección IP automáticamente y usualmente es iniciado cuando se realiza en el proceso de boteo de una computadora o sistema operativo. Cuando la maquina cliente se inicia esta no cuenta con información sobre la configuración de red a la cual esta conectada, en este momento la maquina cliente inicia una técnica llamada transmisión la cual busca, encuentra y se comunica con el servidor DHCP solicitándole los parámetros de configuración de la red. Cuando el DHCP recibe el paquete de transmisión este contestará con otro paquete de transmisión que contiene toda la información solicitada por el maquina cliente.

Algunos de esos paquetes que se transmiten del cliente al servidor DHCP y viceversa son los siguientes:

- **DHCP Discovery.-**La maquina cliente enviá este paquete para ubicar los servidores DHCP disponibles en la red interna, una vez recibido este paquete, el servidor DHCP almacena la dirección Ethernet de quien genera la petición.
- **DHCP Offer.-** Respuesta del servidor DHCP al paquete DHCP Discover la cual contiene los parámetros de red interna.
- **DHCP Request.-**El cliente selecciona la configuración de los paquetes recibidos de DHCP Offer. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor

- **DHCP Acknowledge.-**Cuando el servidor DHCP recibe el mensaje DHCP Request del cliente, este inicia la fase final del proceso de configuración .Esta fase implica el reconocimiento DHCP Pack el envío de un paquete al cliente. En este punto, la configuración TCP/IP se ha completado. El servidor reconoce la solicitud y se lo enviá al cliente.
- **DHCP Release.-** La maquina cliente enviá una petición al servidor DHCP informándole sobre la liberación de su dirección IP
- DHCP Ack.-Respuesta del Servidor DHCP al la maquina cliente la cual enviá los parámetros de red como por ejemplo la dirección IP que le corresponde a la misma.
- **DHCP Inform.-**El cliente envía una petición al servidor de DHCP para solicitar más información que la que el servidor ha enviado con el DHCP Ask o para repetir los datos para un uso particular.
- DHCP Nak.- Respuesta del servidor DHCP a la maquina cliente la cual le indica que su dirección IP ha vencido o que su configuración es errónea
- DHCP Decline.- La maquina cliente le informa el servidor DHCP que la dirección IP ya esta en uso



Esquema de una sesion DHCP

4.1.2 Asignación de direcciones IP

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- **Asignación manual**: Asigna una dirección IP a un equipo determinado. Es mas frecuentemente utilizado cuando se desea controlar la asignación de direcciones IP a cada equipo y así evitar también , que se conecten equipos no identificados

- **Asignación automática**: Asigna una dirección IP de forma permanente a un equipo. Se suele utilizar cuando el número de equipos en la LAN no varía demasiado.

- **Asignación dinámica**: Este método hace uso de la reutilizacion de direcciones IP, técnica mediante la cual, el servidor dhcp reinicia las tarjetas de red cada cierto intervalo de tiempo, asignando una nueva dirección IP a los equipos.

4.2 Requerimientos para la Instalación de un DHCP

Procederemos a instalar nuestro servidor DHCP mediante la descarga de los siguientes paquetes por lo que se recomienda que dichas descargas se hagan como root.

Para ello teclearemos en consola lo siguiente:

```
[localhost@localdomain ~]# yum install -y dhcp
```

Una vez que se halla descargado e instalado el dhcp, este creara su fichero de configuración en la siguiente ubicación:

```
/etc/dhcpd.conf
```

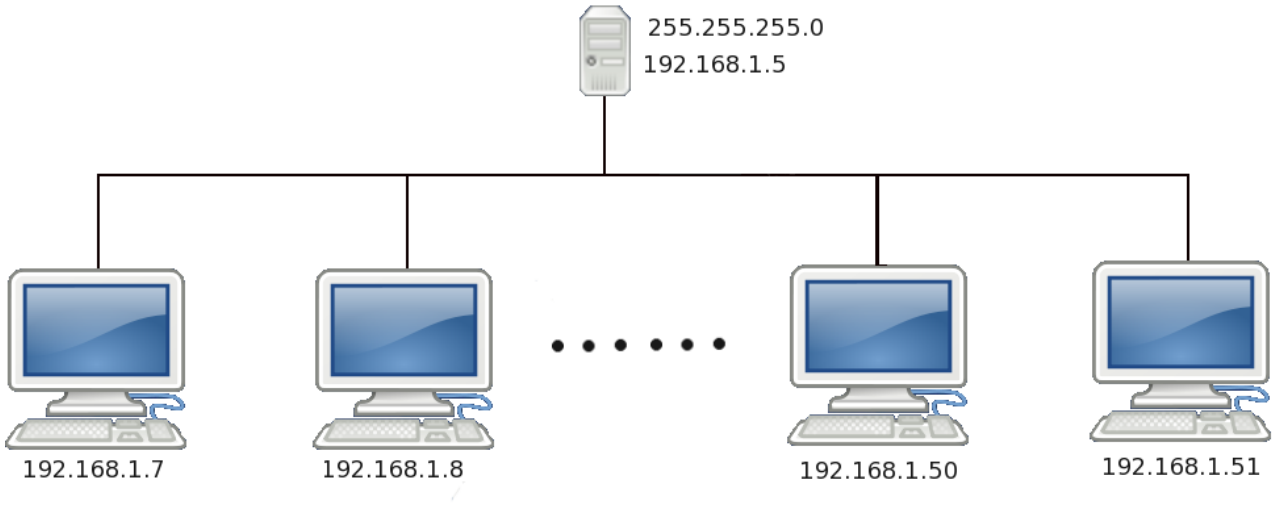
4.3 Configuración del fichero dhcpd.conf

El primer paso para configurar el servidor de DHCP sera editar el fichero dhcp.conf al cual le añadiremos la información de nuestra LAN. El archivo de configuración puede contener tabulaciones o líneas en blanco adicionales para facilitar el formato. Las palabras clave no distinguen entre mayúsculas y minúsculas. Las líneas que empiezan con el símbolo numeral (#) se consideran comentarios.

Consideremos el siguiente requerimiento:

Se requiere implementar un servidor DHCP que implemente los tres métodos de asignación de direcciones IP. El servidor DHCP contara con dos tarjetas de red, las cuales tendrán asignadas las direcciones **192.168.1.5** y **192.168.2.5** , el segmento de red sobre el cual actuara el servidor DHCP es el 1**92.168.1.0**, la submascara de red asignada sera la **255.255.255.0**, así mismo el servidor DHCP servirá como gateway el cual tendrá asignada la misma dirección IP que el DHCP (**192.168.1.5)**, la dirección de broadcast asignada sera la **192.168.1.255,** el rango de direcciones IP que asignara el servidor DHCP estará entre el rango de **192.168.1.7 á 192.168.1.100**

El diagrama de la red quedara de la siguiente manera



4.3.1 Parámetros de configuración

ignore/allow client-updates	Permite la actualización de las asignaciones de un cliente a requerimiento de este, o bien las asignaciones se actualizan cuando el servidor así lo requiera (***ignore***).
shared-network redLocal	Parámetro que describe las subredes que compartirán la misma red física las cuales se especifican dentro de esta declaración
subnet	Segmento de subred sobre el cual actuara el dhcp
netmask	Mascara de red de la subred
option routers	Parámetro que especifica mediante IP la ubicación del router
option subnet-mask	Mascara de red de la subred
option broadcast-address	Parámetro que especifica la IP de broadcast
option domain-name "tuDominio.com";	Parámetro que describe el nombre de tu dominio
option domain-name-servers	Parámetro que especifica mediante IP la ubicación del DNS
range	Rango sobre el cual el DHCP asignara direcciones IP
default-lease-time	Parámetro que indica el tiempo entre cada nueva asignación de IP a los equipos
max-lease-time	Parámetro que indica el tiempo de vigencia de la dirección IP para cada equipo
host nombreDeLaMaquina	Parámetro que describe el nombre del equipo
option host-name "nombreDeLaMaquina.tuDominio.com"	Parámetro que describe el nombre de la computadora y el nombre de dominio asociado a la misma
hardware ethernet	Parámetro que describe la dirección MAC asociada a la tarjeta ethernet del equipo
fixed-address	Parámetro que describe la dirección IP destinada a un equipo
authoritative	La configuración correcta para la red es la definida en el servidor DHCP. Poner este parámetro al comienzo del archivo de configuración supone que el servidor DHCP reasignará direcciones a los clientes mal configurados por el motivo que sea, incluida una configuración nueva del servidor.
not authoritative	La función de este parámetro es justo la contraria del anterior. Es decir: la configuración del servidor de DHCP no es concluyente y los clientes mal configurados que sean detectados por el servidor, seguirán con su configuración intacta.
ddns-domainname <*nombre*>	Mediante el uso de este parámetro, se añadirá ***<nombre>*** al final del nombre de la máquina cliente, para formar un nombre de dominio totalmente cualificado (*FQDN*).

ddns-hostname <nombre>	Por defecto, el servidor DHCP utiliza como nombre para la solicitud el nombre que el cliente tiene asignado a su máquina. Mediante este parámetro se asigna un nombre concreto a una máquina o a todas en general. Por ejemplo, para asignar un nombre a una dirección MAC concreta, utilizaremos el código siguiente:

```
host  "nada" {
        hardware ethernet 00:60:30:3f:2d:4a;
        ddns-hostname "nombre_del_host";
}
```

Y para asignar, por ejemplo, la dirección MAC como parte del nombre del maquina cliente, podemos usar lo siguiente:

```
ddns-hostname = binary-to-ascii (16,8, "-", substring (hardware, 1, 6));
```

ddns-updates <*on*|*off*>	Activa la actualización DNS mediante los valores asignados por DHCP.
group	Inicia la declaración de *Grupo*.
min-lease-time <*duración*>	Especifica la cantidad mínima de tiempo, en segundos, que será mantenida una asignación de direcciones.
one-lease-per-client <*on/off*>	Cuando la opción se iguala a *on* y un cliente solicita una asignación de dirección (DHCPREQUEST), el servidor libera de forma automática cualquier otra asignación asociada a dicho cliente. Con esto se supone que si el cliente solicita una nueva asignación es porque ha olvidado que tuviera alguna, luego tiene un sólo interfaz de red. No dándose esta situación entre los clientes no es muy aconsejable el uso de esta opción.
range *ip-menor ip-mayor*	n una declaración de subred, este parámetro define el rango de direcciones que serán asignadas. Pueden darse dos instrucciones range seguidas del modo: range 192.168.0.11 192.168.0.100; range 192.168.0.125 192.168.0.210;
server-identifier <*IP*>	Identifica la máquina donde se aloja el servidor de DHCP. Su uso se aplica cuando la máquina en cuestión tiene varias direcciones asignadas en un mismo interfaz de red.
server-name <*nombre*>	Nombre del servidor que será suministrado al cliente que solicita la asignación.

Editaremos el fichero /etc/dhcpd.conf de tres maneras diferentes, esto con el fin de ejemplificar los tres métodos de asignación de direcciones IP.

4.3.2 Asignación manual

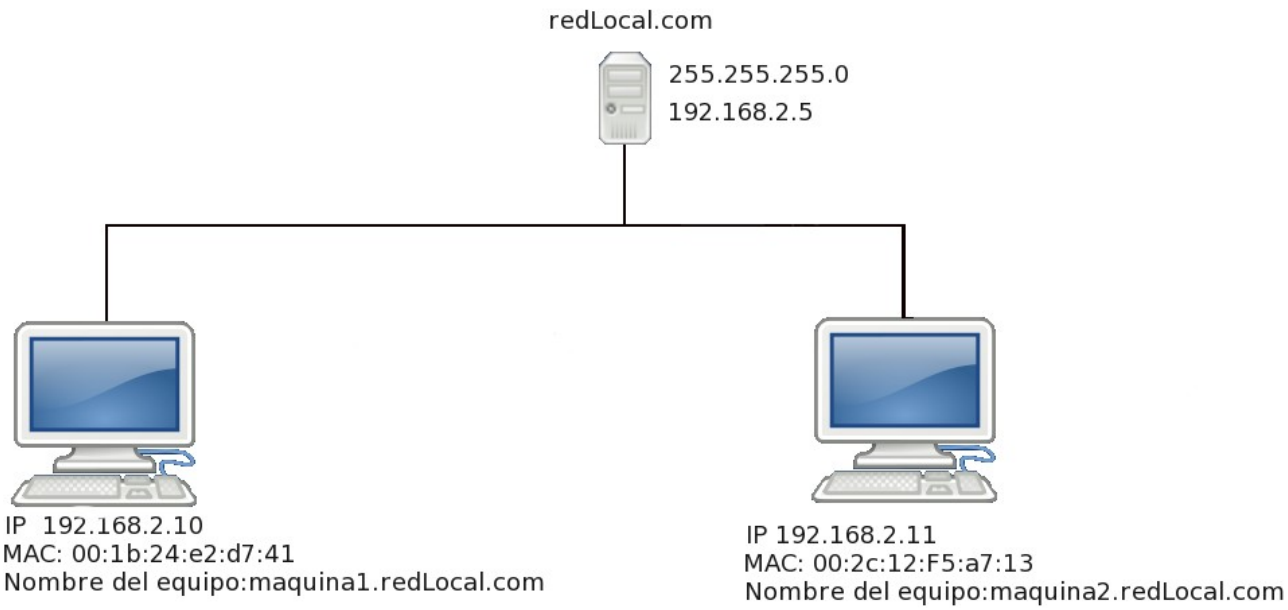
Abriremos una terminal y con la ayuda de “vi” editaremos el fichero dhcpd.conf

```
[localhost@localdomain ~]#vi /etc/dhcpd.conf
```

Una vez abierto el fichero deberemos añadir el siguiente contenido:

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style interim;
ignore client-updates;
shared-network redLocal{
 subnet 192.168.2.0 netmask 255.255.255.0{
                option routers 192.168.2.5;
                option subnet-mask 255.255.255.0;
                option broadcast-address 192.168.2.255;
                option domain-name "redLocal.com.";
                option domain-name-servers 192.168.2.5;

        }
        host maquina1{
                option host-name "maquina1.redLocal.com";
                hardware ethernet 00:1b:24:e2:d7:41;
                fixed-address 192.168.2.10;
        }
        host maquina2{
                option host-name "maquina2.redLocal.com";
                hardware ethernet 00:2c:212:ef5:a7:13;
                fixed-address 192.168.2.11;
        }
}
```

Lo hecho anteriormente hace que el servidor DHCP asigne a dos equipos de la red, las direcciones IP que fueron anexadas en el fichero dhcp.conf



4.3.3 Asignación automática

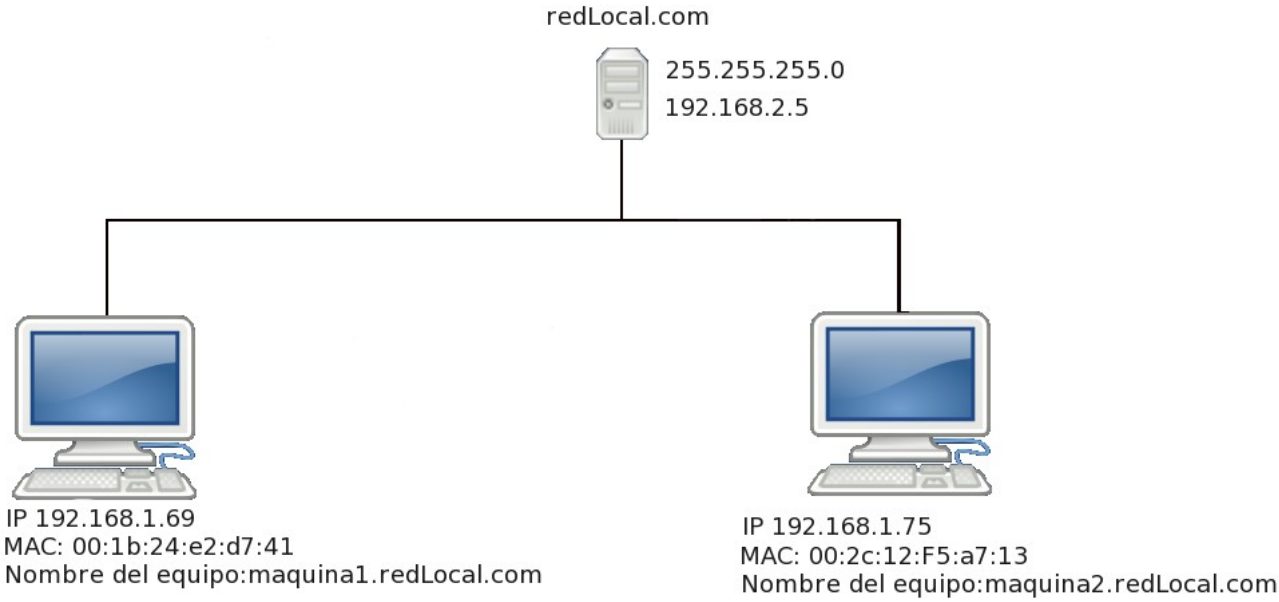
Abriremos una terminal y con la ayuda de “vi” editaremos el fichero dhcpd.conf

```
[localhost@localdomain ~]#vi /etc/dhcpd.conf
```

Una vez abierto el fichero deberemos añadir el siguiente contenido:

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#

ddns-update-style interim;
ignore client-updates;
shared-network factorcentos{
        subnet 192.168.2.0 netmask 255.255.255.0{
                option routers 192.168.2.5;
                option subnet-mask 255.255.255.0;
                option broadcast-address 192.168.2.255;
                option domain-name "factorcentos.com.mx";
                option domain-name-servers 192.168.2.5;
                range 192.168.2.1 192.167.2.100;
        }
}
```

Lo hecho anteriormente hace que el servidor DHCP asigne a dos equipos de la red, dos direcciones IP aleatorias dentro del rango de 192.168.2.10 al 192.168.1.200



4.3.4 Asignación dinámica

Abriremos una terminal y con la ayuda de “vi” editaremos el fichero dhcpd.conf

```
[localhost@localdomain ~]#vi /etc/dhcpd.conf
```

Una vez abierto el fichero deberemos añadir el siguiente contenido:

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#

ddns-update-style interim;
ignore client-updates;
shared-network factorcentos{
        subnet 192.168.2.0 netmask 255.255.255.0{
                option routers 192.168.2.5;
                option subnet-mask 255.255.255.0;
                option broadcast-address 192.168.2.255;
                option domain-name "factorcentos.com.mx";
                option domain-name-servers 192.168.2.5;
                range 192.168.2.1 192.167.2.100;
                default-lease-time 21600;
                max-lease-time 43200;
        }
}
```

Lo hecho anteriormente hace que el servidor DHCP asigne a dos equipos de la red, dos direcciones IP aleatorias dentro del rango de 192.168.2.10 al 192.168.1.200 las cuales serán renovadas cada cierto tiempo asignado de nuevo direcciones IP aleatorias dentro del rango de 192.168.2.10 al 192.168.1.200

4.3.5 Ejemplos de mas asignaciones

Existen algunas opciones adicionales para configurar un servidor de DHCP las cuales casi siempre son necesarias. A continuación vamos a analizar algunas de ellas con prácticos ejemplos, analizando siempre los parámetros mas importantes que podemos llegar a usar

4.3.5.1 Declaración de Subred

Para este tipo de configuración , se debe incluir la declaración **subnet** la cual deberá estar especificada para cada subred en la red original. Si no es así, el servidor DHCP nunca arrancara

Para este ejemplo hemos puesto opciones globales para cada cliente del servidor DHCP en la subred, así como el parámetro **range** lo cual hará que a cada maquina cliente le asigne una dirección IP dentro de las IP declaradas en **range**

```
subnet 192.168.1.0     netmask      255.255.255.0 {
        option routers     192.168.1.1;
        option subnet-mask 255.255.255.0;

        option domain-name "ejemplolinux.com";
        option domain-name-servers 192.168.1.1;

        option time-offset 18000;
        range 192.168.1.10 192.168.1.100;
}
```

4.3.5.2 Declaracion de Red Compartida

Las subredes son un subconjunto de la red original, pero para declararlas deben especificarse dentro de una declaración **shared-network**. Los parámetros dentro de **shared-network** pero fuera de las declaraciones subnet se consideran parámetros globales. El nombre de **shared-network** debe ser el título descriptivo de la red, como, por ejemplo **redLocal**. Dicho nombre puede ser igualmente una dirección IP.

```
shared-network redLocal {
        option domain-name            "wiki.ejemplolinux.com";
        option domain-name-servers    mydns.ejemplolinux.com;
        option routers                192.168.1.1;

      ---Declaración de subredes específicas---

         subnet 192.168.1.2 netmask 255.255.255.0 {
                 parameters for subnet
                 range 192.168.1.3 192.168.1.50;
                 }
         subnet 192.168.1.51 netmask 255.255.255.0 {
                 parameters for subnet
                 range 192.168.1.52 192.168.1.100;
                 }
}
```

4.3.5.3 Declaracion de Grupo

EL parámetro **group** puede utilizarse para aplicar parámetros globales a un grupo de declaraciones. Puede agrupar redes compartidas, subredes, hosts u otros grupos.

```
group {

        option routers 192.168.1.1;
        option subnet-mask 255.255.255.0;

        option domain-name           "ejemplolinux.com";
        option domain-name-servers   192.168.1.1;

        option time-offset           18000;
```

```
        host recepción {
                option host_name "recepcion.ejemplolinux.com";
                hardware ethernet 00:1b:24:e2:d7:41;
                fixed_address 192.168.1.69;
        }

        host soporte {
                option host_name "soporte.ejemplolinux.com";
                hardware ethernet 00:2c:212:ef5:a7:13;
                fixed_address 192.168.1.13;
        }
}
```

4.4 Levantando el servicio

Al terminar de editar todos los ficheros involucrados, solo bastará iniciar el servidor DHCP, el cual podrá inicializarse, detenerse o reinicializarse con el comando *"/etc/init.d"* ó de otra forma añadirlo al arranque del sistema en un nivel o niveles de corrida en particular con el mandato *chkconfig.*

Para levantar por primera vez el servicio teclear en consola lo siguiente:

```
[localhost@localdomain ~]#/etc/init.d/dhcpd start
```

Para reiniciar el servicio:

```
[localhost@localdomain ~]#/etc/init.d/dhcpd restart
```

Para detener el servicio, utilice:

```
[localhost@localdomain ~]#/etc/init.d/dhcpd stop
```

Para añadir el servidor DHCP al arranque del sistema en todos los niveles de corrida, utilice:

```
[localhost@localdomain ~]#chkconfig dhcpd on
```

Índice de contenido

Información de Derechos reservados de esta publicación.

Autor del manual: Javier Eduardo Duarte

Tema 3. Instalación del Servidor FTP

3.1 Acerca del Protocolo FTP

La historia de este protocolo se remonta al año de 1969 cuando el Instituto Tecnológico de Massachusetts mejor conocido como el MIT presentó la propuesta del primer Protocolo para la transmisión de archivos en Internet. **Era un protocolo muy sencillo basado en el sistema de correo electrónico pero sentó las bases para el futuro protocolo de transmisión de archivos (FTP).*

**En 1985, quince años después de la primera propuesta, se termina el desarrollo del aún vigente protocolo para la transmisión de archivos en Internet (FTP), basado en la filosofía de cliente-servidor.*

```
* Fragmento extraído de Wikipedia
```

El protocolo FTP (File Transfer Protocol) es una de las herramientas mas usadas entorno a la administración de portales web y tiene como principal función la transferencia de archivos. Esta transacción puede ser efectuada desde una LAN (Red de área local) o en una WAN (Red de Área Amplia).

El protocolo FTP esta basado principalmente en la arquitectura Cliente-Servidor el cual consiste básicamente en un programa **"Cliente"** que realiza peticiones a otro programa **"Servidor"** el cual responde a su petición. Visto de otra forma podemos entenderlo como el equipo cliente que se conecta al servidor para descargar archivos desde el o para enviarle archivos.

FTP hace uso del modelo TCP/IP y trabaja directamente sobre la capa de aplicación del antes mencionado. Así mismo el protocolo FTP hace uso de los puertos 20 y 21 para la comunicación y control de datos. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico mediante la ayuda de un sniffer y acceder al servidor. Una forma de solucionar este gran problema de seguridad es mediante la utilización de aplicaciones como **"SCP"** y el **"SFTP"** los cuales permiten transferir archivos pero cifrando el trafico , por lo general estas aplicaciones son incluidas en el paquete de openSSH tema que veremos mas adelante.

3.2 Funcionamiento del Protocolo FTP

Generalmente se origina cuando el cliente FTP envía la petición al servidor para indicarle que requiere establecer una comunicación con el, entonces el cliente FTP inicia la conexión hacia el servidor FTP mediante el puerto 21 el cual establecerá un canal de control. A partir de este punto el cliente FTP enviara al servidor las acciones que este debe ejecutar para poder llevar a cabo el envío de datos. Estas acciones incluyen parámetros para la conexión de datos así como también la manera en como serán gestionados y tratados estos datos.

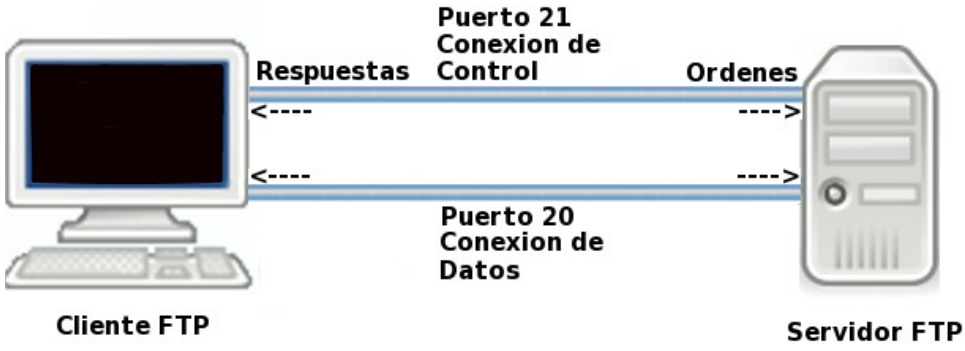
Algunos de los parámetros enviados por el cliente FTP para la conexión de datos son los siguientes:

- Puerto de datos
- Modo de transferencia
- Tipo de representación y estructura

Los parámetros relacionados a la gestión de datos son los siguientes:

- Almacenar
- Recuperar
- Añadir
- Borrar
- Obtener

El proceso de transferencia de datos desde el servidor hacia el cliente deberá esperar a que el servidor inicie la conexión al puerto de datos especificado (en modo activo) y luego de ello transferir los datos en función a los parámetros de conexión especificados anteriormente.



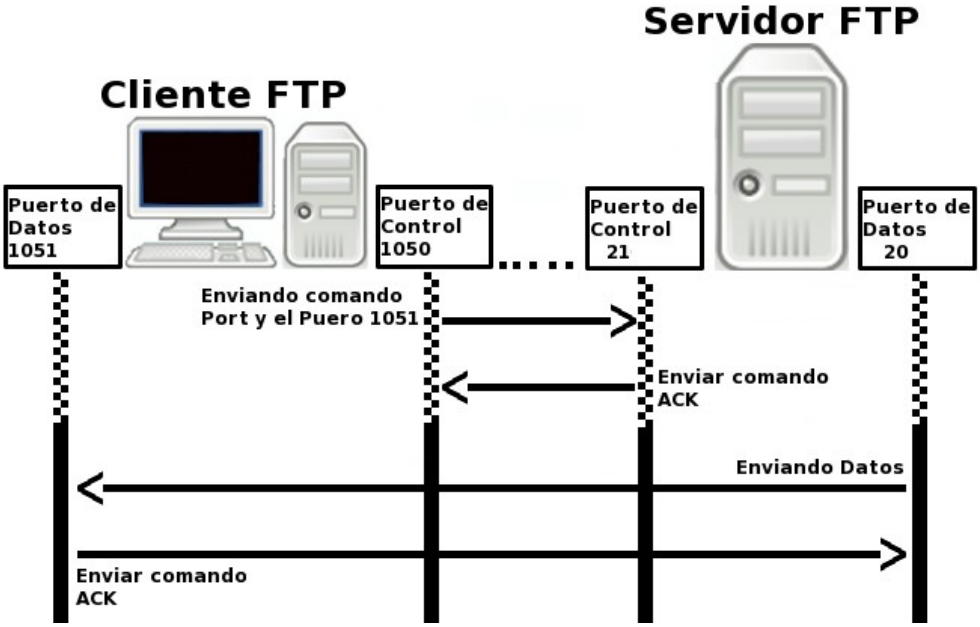
3.3 Modos de conexión del cliente FTP

FTP establecerá dos modos de conexión diferentes para el cliente, el Modo Activo y el Modo Pasivo.

3.3.1 Modo Activo

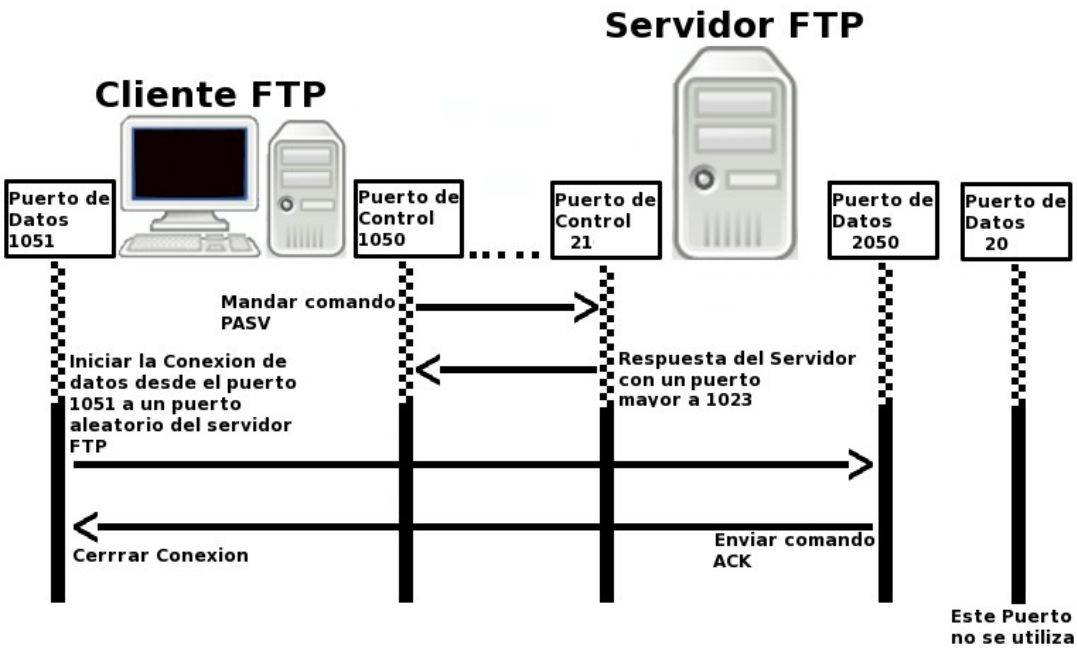
El modo activo generalmente es conocido también como modo estándar y este opera de la siguiente forma. Se establecen dos conexiones distintas, la primera conexión establece una comunicación para la transmisión de comandos a través de un puerto aleatorio mayor que el 1024 del cliente FTP hacia el puerto 21 del servidor FTP y por esa misma conexión se le notifica al servidor FTP cual es el puerto de nuestro cliente FTP que esta a la espera de los datos.

Entonces y para comprender mejor, si usted descarga algún archivo mediante la ayuda de algún cliente de FTP, es el servidor FTP el que inicia la transmisión de datos, desde su puerto 20 al puerto que aleatoriamente el cliente FTP le ha indicado. Se le llama modo activo porque la transmisión de datos es iniciada por el propio servidor FTP.



3.3.2 Modo Pasivo

Esto se logra cuando el cliente FTP inicia la conexión con el servidor FTP mediante el envió del comando PASV en este punto el cliente FTP establece una comunicación mediante un canal de control el cual generalmente utiliza un puerto aleatorio mayor al 1024 para comunicarse con el servidor FTP a través de su puerto 21. Al pasar a modo pasivo el cliente FTP pedirá al servidor FTP que habrá un puerto, el cual deberá ser aleatorio y mayor al 1024, recibida la contestación, será el cliente FTP el que establezca la conexión de datos al servidor FTP a través del puerto especificado anteriormente.



3.3.3 Modo Activo vs Modo Pasivo

Como hemos explicado antes, en el modo activo se abre una conexión para datos desde el servidor FTP al cliente FTP, esto es, una conexión de fuera hacia adentro, entonces, si el cliente FTP se encuentra detrás de un firewall, este filtrara o bloqueara la conexión entrante.

En el modo pasivo es el cliente FTP el que inicia tanto la conexión de control como la de datos, con lo cual el firewall no tendrá ninguna conexión entrante que filtrar.

3.4 Modos de acceso del cliente FTP

Un cliente FTP es la aplicación o software que servirá de intermediario entre el servidor FTP y nuestro equipo, así mismo existen dos versiones de clientes FTP, los gráficos y los que se usan a linea de comandos.

En la mayoría de los casos se implementaran clientes gráficos de FTP esto debido a que son mas fáciles y sencillos de manejar por el usuario. Nosotros recomendamos usar el cliente FTP FileZilla.

FileZilla es un cliente FTP, gratuito, multiplataforma , libre y de código abierto. Sustenta los protocolos FTP, SFTP y SFTP.

Así mismo, los clientes FTP pueden acceder a los servidores FTP de tres formas distintas, estas son:

- Acceso Anónimo
- Acceso de Usuario
- Acceso de Invitado

3.4.1 Acceso Anónimo

El acceso anónimo a un servidor FTP se caracteriza porque este no pide ningún tipo de autenticacion al cliente FTP (login y password) para entrar en el. Generalmente este tipo de accesos son implementados para que cualquier usuario tenga acceso a los recursos que ahí se comparten, los cuales normalmente solo pueden ser leídos o copiados , restringiendo a los usuarios la función de crear o modificar dichos recursos.

3.4.2 Acceso de Usuario

Este tipo de acceso se caracteriza porque este si requiere autenticacion del cliente FTP (login y password) ante el servidor FTP. Generalmente estos accesos son implementados para un grupo selecto de usuarios, los cuales tendrán ciertos privilegios sobre los recursos del servidor como podría ser modificar, eliminar, crear , subir o descargar archivos o carpetas.

Otra característica de este acceso es que permite al usuario FTP acceder a cualquier parte del sistema operativo, lo cual es un grave fallo de seguridad.

3.4.3 Acceso de Invitado

El acceso de invitado bien podría ser un híbrido entre el acceso anónimo y el acceso de usuario, ya que en este tipo de acceso de requiere autenticacion del cliente FTP (login y password) ante el servidor FTP, lo que lo diferencia de los últimos dos es que el usuario FTP solo podrá trabajar en un directorio de trabajo destinado exclusivamente para el, evitando así que el usuario FTP tenga acceso a otras partes del sistema operativo, pero sin restringir los privilegios que tiene sobre su propio directorio de trabajo.

3.5 Proceso de instalación del servidor FTP

3.5.1 Instalando VSFTPD

La instalación de VSFTPD es relativamente sencilla , solo debe teclear en terminal el siguiente comando.

```
[root@ localhost ~]# yum install -y vsftpd
```

Recuerde que este comando se debe ejecutar como root

3.5.2 Archivos de configuración de VSFTPD

La configuración de VSFTPD se realizara sobre dos ficheros distintos, uno de configuración general propio de VSFTPD y otro para especificar al servidor FTP los usuarios que harán uso del acceso de invitado.

El primer fichero de configuración de VSFTPD lo encontramos en la siguiente ruta

```
/etc/vsftpd/vsftpd.conf
```

El segundo fichero de configuración debe ser creado por usted mismo ya que de otra forma nunca podrá especificar al servidor FTP los usuarios que harán uso del acceso de invitado. La ruta en la que se debe crear dicho fichero es la siguiente:

```
/etc/vsftpd
```

Y sera nombrado con el nombre siguiente:

```
chroot_list
```

A este fichero deberán ser agregados los nombres de los usuarios de FTP que trabajaran en su directorio de trabajo, de esta manera se restringe a estos usuarios el acceso a otras partes del sistema operativo, cualquier otro usuario no agregado a este archivo podrá acceder a cualquier parte del sistema operativo, lo cual es un grave fallo de seguridad.

Al final nuestros archivos deberán estar ubicados en las siguientes ruta:

```
/etc/vsftpd/vsftpd.conf   --->   Fichero de configuración propio de VSFTPD


/etc/vsftpd/chroot_list   --->   Fichero que definirá los usuarios
                                 que harán uso del acceso de invitado
                                 [RECUERDE QUE ESTE FICHERO DEBE SER
                                 GENERADO POR USTED]
```

El siguiente paso sera editar y configurar los ficheros que previamente creamos.

3.5.2.1 Configuración del fichero vsftpd.conf

Para llevar a cabo la configuración de este fichero le recomendamos usar el editor de textos VIM.

A continuación le presentamos las diferentes opciones que pueden ser habilitadas o negadas en el fichero de configuración **vsftpd.conf**

3.5.2.1.1 Habilitando o negando accesos anónimos al servidor FTP

Al haber abierto el fichero trate de buscar la linea siguiente:

Para habilitar el acceso anónimo al servidor FTP solo deberá teclear la palabra **YES** , caso contrario si usted desea tener deshabilitada esta opción solo deberá teclear la palabra **NO.**

```
anonymous_enable=YES|NO
```

3.5.2.1.2 Habilitar o negar autenticarse a los usuarios

Para habilitar o negar los accesos autenticados de los usuarios locales en el servidor FTP deberá buscar la siguiente linea:

```
local_enable=YES|NO
```

Deberá teclear la palabra **YES** para habilitar la autenticacion , caso contrario si usted desea tener deshabilitada esta opción solo deberá teclear la palabra **NO.**

3.5.2.1.3 Habilitar o negar la escritura en el servidor FTP

Para habilitar o negar la escritura en el servidor FTP deberá buscar la siguiente linea

```
write_enable=YES|NO
```

Una vez ubicada esta linea recuerde borrar (si es que esta) el signo de numero **(#)** para habilitar esta función.

Establezca el valor YES o NO de acuerdo a lo que se requiera.

3.5.2.1.4 Estableciendo un mensaje de bienvenida en el servidor FTP

Este parámetro sirve para establecer un mensaje de bienvenida el cual será mostrado cada vez que un usuario acceda al servidor de archivos.

Una vez ubicada esta linea recuerde borrar (si es que esta) el signo de numero **(#)** para habilitar esta función.

Para agregar este mensaje al servidor FTP deberá buscar la siguiente linea y editarla.

```
ftpd_banner=Bienvenido al Servidor FTP de Linux Para Todos
```

3.5.2.1.5 Habilitar el acceso de invitado para ciertos usuarios de FTP

Para limitar a los usuarios a trabajar en su propia carpeta de trabajo se deberán editar las siguientes lineas del fichero **vsftpd.conf**

```
chroot_list_enable=YES |NO
```

Una vez ubicada esta linea recuerde borrar (si es que esta) el signo de numero **(#)** para habilitar esta función.

Habilitar este parámetro indicara al servidor FTP que el usuario solo podrá trabajar dentro de su carpeta de trabajo, para ello solo habrá que teclear la palabra **YES**, en caso contrario use la palabra **NO**

El siguiente parámetro se encuentra en función del anterior, de forma que si usted lo habilito también tendrá que habilitar este ultimo, para ello solo deberá borrar el caracter de numero **(#)**

```
chroot_list_file=/etc/vsftpd/chroot_list
```

El parámetro

```
/etc/vsftpd/chroot_list
```

indica la ruta en la cual se encuentra el fichero con los nombres de los usuarios que serán limitados a trabajar en su propia carpeta de trabajo

```
Recuerde que usted creo previamente este fichero
```

3.5.2.1.6 Habilitar al usuario anónimo la función de subir contenido al servidor FTP

Para habilitar o negar al usuario anónimo el subir datos al servidor FTP deberá buscar la siguiente linea:

```
anon_upload_enable=YES|NO
```

Una vez ubicada esta linea recuerde borrar (si es que esta) el signo de numero (#) para habilitar esta función.

Establezca el valor YES o NO de acuerdo a lo que se requiera.

3.5.2.1.7 Habilitar al usuario anónimo la función de crear carpetas en servidor FTP

Para habilitar o negar al usuario crear carpetas en servidor FTP deberá buscar la siguiente linea:

```
anon_mkdir_write_enable=YES|NO
```

Una vez ubicada esta linea recuerde borrar (si es que esta) el signo de numero (#) para habilitar esta función.

Establezca el valor YES o NO de acuerdo a lo que se requiera.

3.5.2.1.8 Estableciendo permisos de escritura, lectura y ejecución al contenido albergado en el servidor FTP

La siguiente linea Indica que los archivos subidos al servidor quedarán con los permisos 022, es decir, sólo escritura para el grupo y los demás.

```
local_umask=022
```

Si tu deseas agregar otro tipo de permisos sobre el contenido que sera albergado en tu servidor FTP solo deberás modificar el valor 022 por el que tu creas mas conveniente.

Nosotros recomendamos usar el permiso "**664"**

```
local_umask=664
```

es decir, lectura y escritura para el propietario del fichero, y sólo lectura para el grupo y los demás

3.5.2.1.9 Limitando la tasa de transferencia a los usuarios anónimos

Usted puede limitar la tasa de transferencia (en bytes) para los usuarios anónimos, solamente deberá agregar la siguiente linea al final del archivo

```
anon_max_rate=10240
```

Como podemos observar hemos limitado la tasa de transferencia a solo 10 Kb para los usuarios anónimos, usted podrá definir ese parámetro de acuerdo a sus necesidades.

3.5.2.1.10 Limitando la tasa de transferencia a los usuarios autenticados

Usted puede limitar la tasa de transferencia (en bytes) para los usuarios anónimos, solamente deberá agregar la siguiente linea al final del archivo

```
local_max_rate=10240
```

Como podemos observar hemos limitado la tasa de transferencia a solo 10 Kb para los usuarios autenticados, usted podrá definir ese parámetro de acuerdo a sus necesidades.

3.5.2.1.11 Limitando el numero de conexiones hacia el servidor FTP

Usted podrá establecer un numero máximo de conexiones que podrán acceder simultáneamente al servidor FTP, para ello solo habrá que añadir la siguiente linea al final de archivo.

```
max_clients=3
```

Como podemos observar hemos limitado el acceso a solamente 3 clientes FTP

3.5.2.1.12 Limitando el numero de conexiones por IP hacia el servidor FTP

Usted podrá establecer un numero máximo de conexiones desde una misma dirección IP que podrán acceder simultáneamente al servidor FTP, para ello solo habrá que añadir la siguiente linea al final de archivo.

```
max_per_ip=3
```

Como podemos observar hemos limitado el acceso a simultaneo a solamente 3 IP´s .

3.5.2.2 Configuración del fichero chroot_list

La configuración de este fichero es relativamente fácil, solo deberá añadir dentro de el los nombres de los usuarios que serán limitados a trabajar dentro de su carpeta personal de trabajo.

Ejemplo:

```
[root@ localhost ~]# vim /etc/vsftpd/chroot_list

paty
angelica
erika
viridiana
iliana
regina

"chroot_list"
```

Al terminar solo deberá guardar los cambios hechos al fichero.

3.5.3 Iniciar , detener o reiniciar el servidor FTP

Para iniciar el servidor FTP por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/vsftpd start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el servidor FTP. Estas opciones pueden ser consultadas en la siguiente tabla:

start	**Inicia el servicio**
stop	**Detiene el servicio**
restart	**Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta**
reload	**Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.**
condrestart	**Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.**
status	**Da a conocer el estado en el que se encuentra el servicio**

Como alternativa también podemos ocupar el siguiente comando para iniciar el servidor FTP

```
[root@ localhost ~]# service vsftpd start
```

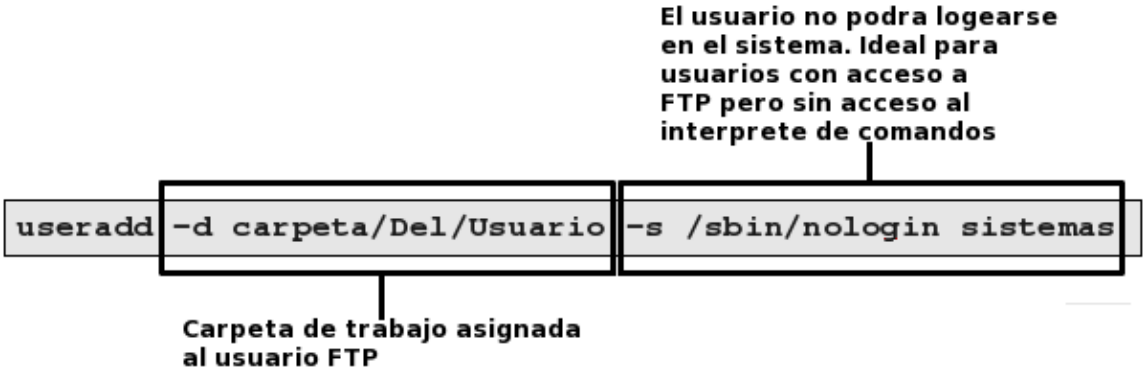
Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root.

3.6 Creación de cuentas de usuario en el servidor FTP

Crear cuentas de usuario en el servidor FTP es un proceso muy parecido a dar de alta usuarios en Linux.

La sintaxis general para dar de alta usuarios es la siguiente:



Las opciones utilizadas son explicadas en la siguiente tabla:

Opciones	Descripción
-d | --home	Carpeta de trabajo que sera asignado al usuario **Ejemplos** a) **-d /home/usuario1** b) **-d /home/cmartinez** c) **-d /home/icastillo**
-s | --shell	**-s /sbin/nologin → El usuario no podrá logearse en el sistema. Ideal para usuarios con acceso a Samba o FTP pero sin acceso al interprete de comandos.**

Adicionalmente se tiene que asignar una contraseña al usuario FTP.

```
[root@ localhost ~]# passwd sistemas
Cambiando la contraseña del usuario .
Nueva UNIX contraseña: xxxxxxxxxx
Vuelva a escribir la nueva UNIX contraseña:xxxxxxxxxx
passwd: todos los tokens de autenticación se actualizaron exitosamente.
```

Ejemplo:

```
[root@ localhost ~]# useradd -d /home/ftp/javier -s /sbin/nologin \ >
javier
```

Explicación:

Como podemos observar, estamos creando una cuenta en el servidor ftp, para ello estamos usando el comando

```
useradd
```

El parámetro siguiente es

```
-d /home/ftp/javier
```

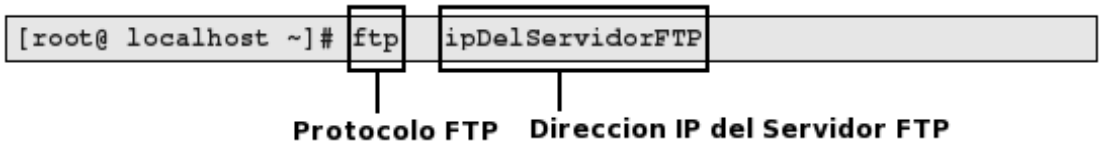
Este parámetro le indica a Linux que la carpeta de trabajo de javier esta ubicada en la ruta **[/home/ftp/javier]**, el ultimo parámetro

```
-s /sbin/nologin
```

Le indica a Linux que el usuario no podrá logearse en el sistema lo cual es ideal para usuarios con acceso a FTP pero sin acceso al interprete de comandos.

3.7 Accediendo al servidor FTP

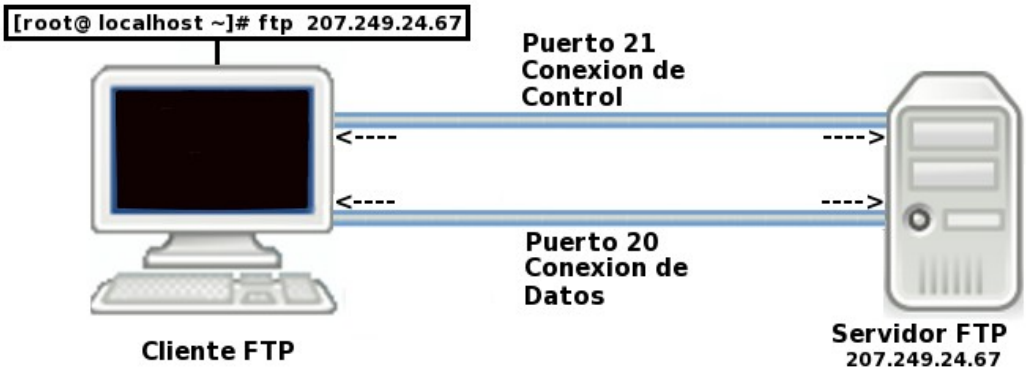
La forma en que accederemos a los recursos del servidor FTP sera a través de la siguiente sintaxis



Ejemplo:

```
[root@ localhost ~]# ftp  207.249.24.67
```

NOTA: Esta acción se debe llevar a cabo desde la maquina que hará la función de cliente FTP



Luego de que el cliente haya establecido un comunicacioncon con el servidor FTP este le pedirá que se autentique . En este punto el usuario deberá teclear su nombre de usuario así como también su contraseña:

```
[root@ localhost ~]# ftp  207.249.24.67
Connected to 207.249.24.67 (207.249.24.67).
220 Bienvenido al Servidor FTP de Linux Para Todos
331 Please specify the password.
Password: xxxxxxxxxx
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

En caso de que se acceda al servidor de forma anónima solo bastara con teclear como nombre de usuario la palabra **"anonymous",** por consiguiente no nos pedirá ninguna contraseña, solo deberá teclear la palabra **"enter".**

Ejemplo:

```
Connected to 207.249.24.67 (207.249.24.67).
220 Bienvenido al Servidor FTP de Linux Para Todos
Name (207.249.24.67:): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

NOTA: La carpeta de trabajo del usuario "anonymous" no existe así que debe crearla usted mismo

Normalmente el acceso por medio del usuario ""anonymous" solo podrá leer y copiar los archivos existentes, pero no modificarlos ni crear otros nuevos.

La ubicación de esta carpeta estará ubicada en la siguiente ruta:

```
/etc/vsftpd/
```

El nombre que llevara esta carpeta sera

```
vació
```

Por consiguiente esta carpeta estará ubicada en:

```
/etc/vsftpd/vacio
```

En caso de no tener creada la carpeta de trabajo para el usuario "anonymous", el servidor FTP nos arrojara el siguiente error.

```
[root@ localhost ~]# ftp  207.249.24.67
Connected to 207.249.24.67 (207.249.24.67).
220 Bienvenido al Servidor FTP de Linux Para Todos
Name (207.249.24.67:): anonymous
331 Please specify the password.
Password:
500 OOPS: cannot change directory:/etc/vsftpd/vacio
Login failed.
ftp>
```

3.8 Copiar u obtener archivos o carpetas desde un servidor FTP

La sintaxis de FTP para llevar a cabo esta operación es la siguiente:

```
[root@ localhost]# ftp ipDelServidorRemoto
```

El siguiente paso sera autenticarnos con la contraseña del usuario remoto

```
Connected to 207.249.24.67 (207.249.24.67).
220 Bienvenido al Servidor FTP de Linux Para Todos
Name (207.249.24.67:): anonymous
331 Please specify the password.
Password: xxxxxxxxxx
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Una vez dentro del servidor solo bastara ejecutar el comando **"get"** para descargar algún fichero o archivo.

```
ftp> get recursoRemoto
```

La siguiente tabla explica mas a detalle los comandos que pueden ser utilizados con FTP:

cd [rutaRemota]	Cambia de directorio dentro del servidor remoto
lcd [rutaLocal]	Cambia de directorio en el equipo local
chgrp [grp] [rutaRemota]	Cambia el grupo de trabajo de un fichero remoto. El [grp] tiene que ser un Group ID
chmod [opciones] [rutaRemota]	Cambia los permisos de Lectura, Escritura o de Ejecución a un fichero remoto
chown [own] [rutaRemota]	Cambia el grupo de trabajo de un fichero remoto. El [own] tiene que ser un User ID
get [rutaRemota] [rutaLocal]	Copia un recurso remoto en un equipo local
lmkdir [rutaLocal]	Crea una carpeta en el equipo local
lpwd	Imprime la ruta local en la cual estamos trabajando
mkdir [rutaRemota]	Crea una carpeta en el equipo remoto

put [rutaLocal] [rutaRemota]	Sube un fichero o archivo desde una ruta local hasta una ruta remota
pwd	Imprime la ruta remota en la cual estamos trabajando
exit	Salimos de SFTP
rename [rutaLocal] [rutaRemota]	Renombra un un fichero remoto
rmdir [rutaRemota]	Borra una carpeta remota
rm [rutaRemota]	Borra un fichero remoto

3.9 Subir o enviar archivos o carpetas a un servidor FTP

La sintaxis de FTP para llevar a cabo esta operación es la siguiente:

```
[root@ localhost]# ftp ipDelServidorRemoto
```

El siguiente paso sera autenticarnos con la contraseña del usuario remoto

```
Connected to 207.249.24.67 (207.249.24.67).
220 Bienvenido al Servidor FTP de Linux Para Todos
Name (207.249.24.67:): anonymous
331 Please specify the password.
Password: xxxxxxxxxx
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Una vez dentro del servidor solo bastara ejecutar el comando **"put"** para descargar algún fichero o archivo.

```
ftp> put recursoLocal
```

La siguiente tabla explica mas a detalle los comandos que pueden ser utilizados con FTP:

cd [rutaRemota]	Cambia de directorio dentro del servidor remoto
lcd [rutaLocal]	Cambia de directorio en el equipo local
chgrp [grp] [rutaRemota]	Cambia el grupo de trabajo de un fichero remoto. El [grp] tiene que ser un Group ID
chmod [opciones] [rutaRemota]	Cambia los permisos de Lectura, Escritura o de Ejecución a un fichero remoto

get [rutaRemota] [rutaLocal]	**Copia un recurso remoto en un equipo local**
lmkdir [rutaLocal]	**Crea una carpeta en el equipo local**
lpwd	**Imprime la ruta local en la cual estamos trabajando**
mkdir [rutaRemota]	**Crea una carpeta en el equipo remoto**
put [rutaLocal] [rutaRemota]	**Sube un fichero o archivo desde una ruta local hasta una ruta remota**
pwd	**Imprime la ruta remota en la cual estamos trabajando**
exit	**Salimos de SFTP**
rename [rutaLocal] [rutaRemota]	**Renombra un un fichero remoto**
rmdir [rutaRemota]	**Borra una carpeta remota**
rm [rutaRemota]	**Borra un fichero remoto**

Índice de contenido

Información de Derechos reservados de esta publicación.

Tema 11. Instalación del Servidor SAMBA

1.1 Sobre Samba

Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que ordenadores con Linux o Mac actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio, como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autenticar con su propio archivo de usuarios.

Samba fue desarrollado originalmente para Unix por Andrew Tridgell utilizando un sniffer o capturador de tráfico para entender el protocolo a través de la ingeniería inversa. El nombre viene de insertar dos vocales al protocolo estándar que Microsoft usa para sus redes, el SMB o server message block.

En un principio, Samba tomó el nombre de smbserver pero tuvieron que cambiarlo por problemas con una marca registrada. Tridgell buscó en el diccionario de su máquina Unix alguna palabra que incluyera las letras “s”, “m” y “b” con la orden grep hasta que dio con Samba.

Samba configura directorios Unix-Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red. Para los usuarios de Microsoft Windows, estos recursos aparecen como carpetas normales de red. Los usuarios de Linux pueden montar en sus sistemas de archivos estás unidades de red como si fueran dispositivos locales, o utilizar la orden smbclient para conectarse a ellas muy al estilo del cliente de la línea de órdenes ftp. Cada directorio puede tener diferentes permisos de acceso sobrepuestos a las protecciones del sistema de archivos que se esté usando en Linux. Por ejemplo, las carpetas home pueden tener permisos de lectura y escritura para cada usuario, permitiendo que cada uno acceda a sus propios archivos; sin embargo, deberemos cambiar los permisos de los archivos localmente para dejar al resto ver nuestros archivos, ya que con dar permisos de escritura en el recurso no será suficiente

1.2 Instalacion de Samba

Para llevar a cabo la instalacion se necesitaran los siguientes paquetes:

- **samba**
- **samba-client**
- **samba-common**

Para instalarlos haga uso de la terminal como se muestra a continuacion:

```
[BASH]# yum install -y samba samba-client samba-common
```

1.3 Configuracion de Samba

Los ficheros que modificaremos seran:

- **/etc/samba/lmhosts**
- **/etc/samba/smb.conf**

1.3.1 Fichero /etc/samba/lmhosts

El fichero **/etc/samba/lmhosts** es el fichero de gestión de los equipos de red estandar usado para resolver nombres a direcciones IP en el sistema.

Podria decirse que este fichero es el equivalente al fichero **/etc/hosts** que es un estandard de Linux-Unix y su estructura es identica a la que se muestra a continuacion:

```
192.168.220.100         desarrollo
192.168.220.101         ventas
```

La única diferencia es que los nombres de la columna derecha son nombres NetBIOS y solo son usados en linux por samba.

Recordemos que los servidores DNS sirven para los casos en donde un equipo requiere conectarse a otro y no tener que hacerlo por la direccion IP, por ejemplo:

```
66.102.11.104         hydra
```

El fichero **/etc/samba/lmhosts** es una simplificación muy básica de ese proceso, pero sólo válida para tu propio equipo.

Recordemos que el proposito del fichero **/etc/hosts** es resolver los nombres de equipos que no pueden ser resueltos de otra manera. También se puede usar para resolver nombres de equipos en pequeñas redes sin servidor DNS.

Es por ello que agregaremos al fichero

```
/etc/samba/lmhosts
```

El nombre que tiene especificado en el fichero

```
/etc/hosts
```

Ejemplo:

```
Fichero /etc/hosts/
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain localhost localhost
192.168.1.105            servidor.empresa.com.mx
```

```
Fichero /etc/samba/lmhosts
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
127.0.0.1               localhost
192.168.1.105           servidor.empresa
```

Como podemos observar solo agregamos la linea final del fichero **`/etc/hosts`** **al final del fichero** **`/etc/samba/lmhosts`**

1.3.2 Fichero /etc/samba/smb.conf

La configuracion basica de Samba se hara sobre el fichero localizado en:

```
"/etc/samba/smb.conf"
```

1.3.2.1 Configuracion de parametros globales

1.-Con la ayuda de algun editor de textos busque la siguiente linea

```
workgroup = MYGROUP
```

En esta linea puedes especificar un nombre para el grupo de usuarios que podran hacer uso de este recurso

Ejemplo:

```
workgroup = Desarrollo
```

2.-busque la siguiente linea

```
server string = Samba Server Version %v
```

En esta linea puedes poner un mensaje de bienvenida para el Servidor Samba

Ejemplo:

```
server string = Servidor Samba Desarrollo
```

3.-busque la siguiente linea

```
netbios name = MYSERVER
```

En esta linea deberas especificar el nombre que tiene asignado el equipo. Su nombre debe ser igual al especificado en el fichero **/etc/samba/lmhosts**

Ejemplo:

```
netbios name = servidor.empresa
```

4.-busque la siguiente linea

```
interfaces = lo eth0 192.168.12.2/24 192.168.13.2/24
```

Esta linea especifica desde que segmentos de red escuchara peticiones el servidor Samba, cualquier otra interfaz no listada aqui sera ignorada

Ejemplo:

```
interfaces = lo eth0 192.168.1.1/24  10.10.1.1
```

5.-busque la siguiente linea

```
hosts allow = 127. 192.168.12. 192.168.13.
```

Esta linea especifica desde que segmentos de red escuchara peticiones el servidor Samba

Ejemplo:

```
hosts allow =  192.168.12.2.
```

Note el punto al final de la linea

6.-busque la siguiente linea

```
log file = /var/log/samba/log.%m
max log size = 50
```

Esta lineas especifican la ubicacion donde quedaran los logs, en este caso la extensión sera conformado por el nombre del equipo desde la cual se hizo la conexión

La segunda linea especifica el tamaño máximo para los archivos de logs

1.3.2.2 Configuracion de los recursos compartidos

La configuracion de las recursos que compartiremos deben ir especificados al final del fichero

```
"/etc/samba/smb.conf"
```

Y deben seguir la siguiente estructura:

```
[nombreDescriptivoDelRecursoCompartido]

       comment = Comentarios
       path = rutaDelREcurso
       public = yes
       writable = yes
       printable = no
       write list = desarrollo
```

Algunas de las opciones que podemos agregar a esta estructura son las siguientes:

Directiva	Valor	Accion
encrypt passwords	yes | no	Esta direcitva indica si las contraseñas seran cifradas cuando el usuario se autentique
invalid users	usuario | grupo	Lista a los usuarios o grupos a los cuales les negara el acceso
valid users	usuario	Lista a los usuarios a los cuales el servidor les dara acceso
admin users	usuario	Lista a los usuarios que asumiran el rol de administrador
read list	usuario	Lista a los usuarios que solo podran leer el recurso compartido
write list	usuario	Lista a los usuarios que podran escribir en el recurso compartido
guest ok	yes | no	Define si se permitirá el acceso como usuario invitado o no
comment	Comentario	En esta seccion podras poner un comentario acerca del recurso que estas compartiendo
path	/ruta/del/recurso	En esta seccion deberas especificar la ruta del recurso que compartes
browseable	yes | no	Define si el recurso podra ser visible o no

Un ejemplo sobre el uso de estas opciones se ve a continuacion

```
[FacturasDiarias]
        comment = Facturas
        path = /var/facturas
        guest ok = no
        write list = jefe
        directory mask = 1770
        create mask = 0660
        browseable = yes
        admin users = jefe contador
        valid users = jefe contador
        writable = yes
        public = yes
```

1.4 Alta de usuarios en Samba

Para dar de alta cuentas de usuario en Samba usaremos el comando **useradd** el cual debera ser aplicado segun la siguiente estructura

```
[BASH]# useradd -s /bin/nologin cuentaDeUsuario
```

el parametro

```
-s /sbin/nologin        Indicara al sistema que el usuario no tendra acceso
                        al interprete de comandos
```

1.5 Asignacion de contraseñas a usuarios en Samba

Para asignar contraseñas a los usuarios en Samba usaremos el comando **smbpaaswd** el cual debera ser aplicado segun la siguiente estructura

```
[BASH]# smbpasswd -a cuentaDeUsuario
```

1.6 Iniciar , detener o reiniciar el servidor Samba

Para iniciar el servidor samba por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/smb start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el servidor Samba. Estas opciones pueden ser consultadas en la siguiente tabla:

start	Inicia el servicio
stop	Detiene el servicio
restart	Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta
reload	Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.
condrestart	Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.
status	Da a conocer el estado en el que se encuentra el servicio

Como alternativa también podemos ocupar el siguiente comando para iniciar el servidor samba

```
[root@ localhost ~]# service smb start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root.

1.7 Conectando con el servidor Samba

La forma para conectar al servidor samba desde terminal sigue la siguiente sintaxis

```
[BASH]# smbclient  //IPdelServidorSamba/recursoCompartido -U usuario
```

Índice de contenido

Información de Derechos reservados de esta publicación.

Autor del manual: Javier Eduardo Duarte

Tema 4. Seguridad con openSSH

4.1 El Protocolo SSH

El protocolo SSH (Secure Shell) es una herramienta que nos permite conectarnos a equipos remotos (Servidores en Producción) así mismo, nos da la capacidad de llevar a cabo tareas administrativas dentro del mismo como, activar o apagar servicios,

Además de la conexión a otros equipos, SSH nos permite copiar datos de forma segura, gestionar claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

Una clave RSA (Sistema Criptografico con Clave Publica) es un algoritmo que genera un par de llaves de autenticacion, la publica y la privada. La publica se distribuye en forma autenticada y la privada que generalmente es guardada en secreto por el propietario.

El protocolo SSH (Secure Shell) esta implementado bajo el estándar TCP/IP, el cual a su vez se encuentra dividido en 5 secciones:

1. Nivel Físico
2. Nivel De Enlace
3. Nivel de Internet
4. Nivel de Transporte
5. Nivel de Aplicación

por lo que el protocolo SSH esta ubicado en la quinta capa del modelo TCP/IP, nos referimos a la capa de aplicación

La capa de aplicación es el nivel que los programas más comunes utilizan para comunicarse a través de una red con otros programas. Los procesos que acontecen en este nivel son aplicaciones específicas que pasan los datos al nivel de aplicación en el formato que internamente use el programa y es codificado de acuerdo con un protocolo estándar.

De manera predeterminada, el protocolo SSH atiende peticiones por el puerto 22

En este capitulo haremos uso de OpenSSH la cual es la alternativa libre y abierta al programa propietario SSH

4.2 Acerca de OpenSSH

OpenSSH (Open Secure Shell) es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, usando como base al protocolo SSH. Este proyecto es liderado actualmente por Theo de Raadt quien actualmente es fundador y líder de proyectos como OpenBSD.

Los desarrolladores de OpenSSH aseguran que este es más seguro que el original, lo cual es debido a la conocida reputación de los desarrolladores de OpenBSD por crear código limpio y perfectamente auditado, lo que contribuye a que sea más seguro. Su seguridad también es atribuible al hecho de que su código fuente se distribuya libremente con una licencia BSD. Aunque todo el código fuente del SSH original también está disponible, existen restricciones con respecto a su uso y distribución, lo que convierte a OpenSSH en un proyecto mucho más atractivo a la hora de atraer nuevos desarrolladores.

Además de la conexión a otros equipos, openSSH nos permite copiar datos de forma segura mediante la implementación de dos herramientas proporcionadas por openSSH, estas son:

- SCP
- SFTP

Estas herramientas en realidad tienen la misma función de copiado solo se diferencian en la forma en como son aplicadas tema del cual hablaremos mas adelante.

4.3 Instalando OpenSSH

A partir de este punto empezaremos a descargar los paquetes necesarios para el perfecto funcionamiento de openSSH, de esta manera si usted se encuentra trabajando bajo algún ambiente gráfico, sea KDE o GNOME le pedimos abra una terminal de BASH, por otra parte si usted se encuentra trabajando bajo linea de comandos no tendrá que hacer nada.

Los paquetes a descargar son los siguientes:

- openssh
- openssh-clients
- openssh-server

La forma en que se instalaran estos paquetes sera tecleando en consola lo siguiente:

```
[root@ localhost ] # yum install -y openssh openssh-clients openssh-server
```

Una vez finalizado el proceso de instalación pasaremos con las configuraciones propias de openSSH, nos referimos a los ficheros de configuración

4.4 Archivos de configuración de OpenSSH

OpenSSH dispone de dos conjuntos diferentes de ficheros de configuración: uno completamente dedicado al cliente (ssh, scp y sftp) y otro orientado completamente al servidor.

4.4.1 Archivos de configuración del lado del servidor

La ubicación de los ficheros de configuración referentes al servidor openSSH se encuentran en la siguiente ruta:

```
/etc/ssh/
```

Dentro del directorio podemos encontrar los siguientes ficheros de configuración:

moduli	Contiene grupos Diffie-Hellman usados para el intercambio de la clave Diffie-Hellman que es imprescindible para la construcción de una capa de transporte seguro. Cuando se intercambian las claves al inicio de una sesión SSH, se crea un valor secreto y compartido que no puede ser determinado por ninguna de las partes individualmente. Este valor se usa para proporcionar la autenticación del host.

ssh_config	El archivo de configuración del sistema cliente SSH por defecto. Este archivo se sobrescribe si hay alguno ya presente en el directorio principal del usuario
sshd_config	El archivo de configuración para el demonio sshd
ssh_host_dsa_key	La clave privada DSA usada por el demonio sshd
ssh_host_dsa_key.pub	La clave pública DSA usada por el demonio sshd
ssh_host_key	La clave privada RSA usada por el demonio sshd para la versión 1 del protocolo SSH.
ssh_host_key.pub	La clave pública RSA usada por el demonio sshd para la versión 1 del protocolo SSH.
ssh_host_rsa_key	La clave privada RSA usada por el demonio sshd para la versión 2 del protocolo SSH.
ssh_host_rsa_key.pub	La clave pública RSA usada por el demonio sshd para la versión 2 del protocolo SSH.

4.4.2 Archivos de configuración del lado del cliente

La ubicación de los ficheros referentes al cliente se encuentran almacenados en el directorio de trabajo de cada usuario:

Ejemplo: "/home/usuario/"

Dentro del directorio podemos encontrar los siguientes ficheros de configuración:

authorized_keys	Este archivo contiene una lista de claves públicas autorizadas. Cuando un cliente se conecta al servidor, el servidor autentica al cliente chequeando su clave pública firmada almacenada dentro de este archivo.
id_dsa	Contiene la clave privada DSA del usuario.
id_dsa.pub	La clave pública DSA del usuario
id_rsa	La clave RSA privada usada por ssh para la versión 2 del protocolo SSH.
id_rsa.pub	La clave pública RSA usada por ssh para la versión 2 del protocolo SSH.
identity	La clave privada RSA usada por ssh para la versión 1 del protocolo SSH.

identity.pub	La clave pública RSA usada por ssh para la versión 1 del protocolo SSH.
known_hosts	Este archivo contiene las claves de host DSA de los servidores SSH a los cuales el usuario ha accedido. Este archivo es muy importante para asegurar que el cliente SSH está conectado al servidor SSH correcto

4.4.3 Configuración de fichero sshd_config

La función que desempeñan los ficheros de configuración de openSSH son de vital importancia para la seguridad de nuestro servidor , ya que si no se llegaran a configurar apropiadamente estos ficheros la vulnerabilidad de nuestro servidor seria demasiado sensible a ataques informáticos, es por ello que le enseñaremos la manera apropiada en la que deberá ser configurado este vital fichero.

4.4.3.1 Blindando el fichero sshd_config

Este fichero lo podrá localizar en en la siguiente ruta

```
/etc/ssh/
```

El siguiente paso sera abrir el fichero con la ayuda del editor de textos VI

```
[root@ localhost #] vi /etc/ssh/sshd_config
```

A partir de este punto comenzaremos a blindar SSH

4.4.3.2 Cambiando el puerto por defecto

SSH tiene asignado por defecto el puerto 22, esto es algo que conocen todos nuestros posibles atacantes , por lo que es una buena idea cambiarlo.

Para modificar esta opción y las siguientes que iremos mencionando editaremos el fichero de configuración **shd_config**, que por defecto se encuentra en el directorio **/etc/ssh/**.

Se recomienda usar un puerto cualquiera por encima del 1024, así que usted puede elegir el que quiera. En este ejemplo usaremos el 34765, por lo que tendrá que editar el parámetro ***Port*** del fichero de configuración el cual deberá quedar así:

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

Port 34567
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

4.4.3.3 Desactivando el Protocolo 1

Hay dos versiones de ssh en cuanto a su protocolo de comunicación, estas son:

- Versión 1
- Versión 2.

La versión 1 de openSSH hace uso de varios algoritmos de cifrado de datos mas sin embargo, algunos de estos algoritmos han dejado de ser mantenidos por sus creadores y por lo tanto presenta serios huecos de seguridad que potencialmente permite a un intruso insertar datos en el canal de comunicación. Para evitar el uso del protocolo 1 y sus posibles ataques a este, basta con indicar que solo admita comunicaciones de ssh basadas en el protocolo 2, por lo que tendrá que editar el parámetro **Protocol** del fichero de configuración el cual deberá quedar así:

```
# Disable legacy (protocol version 1) support in the server for new
# installations. In future the default will change to require explicit
# activation of protocol 1
Protocol 2
```

4.4.3.4 Deshabilitando el acceso a root

Este es quizá el parámetro mas importante de seguridad que podemos indicar para blindar nuestro servidor. Prácticamente la mayoría de sistemas operativos Linux crean por defecto al usuario root , es por ello que la mayoría de los ataques informáticos se concentran en atacar al equipo a través de la cuenta de root y mucho mas si la cuenta tiene asignada una contraseña débil

Una manera de deshabilitar el logeo al sistema a través de la cuenta de root es poner en '**no**' la variable **PermitRootLogin** , con esto el usuario root no tendrá permiso de acceder mediante ssh y por lo tanto cualquier intento de ataque directo a root será inútil. Con esto siempre tendremos que ingresar como un usuario normal y ya estando adentro entonces mediante un **su –** cambiarnos a la cuenta de root.

Para llevar a cabo estos cambios tendrá que editar el parámetro **PermitRootLogin** del fichero de configuración el cual deberá quedar de la siguiente manera:

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
```

4.4.3.5 Definiendo un número máximo de intentos de conexión

Muchos de los ataques llevados a cabo por piratas informáticos se basan en fuerza bruta, estableciendo un número máximo de intentos de conexión lograremos que sus intentos por entrar a nuestro servidor sean disuadidos.

Para llevar a cabo estos cambios tendrá que editar el parámetro **MaxAuthTries** del fichero de configuración el cual deberá quedar de la siguiente manera:

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
MaxAuthTries 2
```

El número **2** indica la cantidad de veces que podemos equivocarnos al ingresar el usuario y/o contraseña, en este caso después de dos intentos, se perderá o cerrará la conexión. Claro, es totalmente posible volver a intentarlo, pero con solo dos intentos por vez.

4.4.3.6 Activando el modo estricto

La opción **StrictModes** debe activarse para que, por ejemplo, los usuarios que establecen permisos de escritura para todos en sus ficheros y directorios no se lleven una desagradable noticia cuando otro usuario los modifique, de esta manera se protege la información de los usuarios.

Para llevar a cabo estos cambios tendrá que editar el parámetro **StrictModes** del fichero de configuración el cual deberá quedar de la siguiente manera:

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
StrictModes yes
MaxAuthTries 2
```

4.4.3.7 Impidiendo la conexión al servidor gráfico

Si nuestro servidor no tienen entorno gráfico instalado, o no queremos que los usuarios se conecten a él, definiremos esta opción en el fichero de configuración:

Para llevar a cabo estos cambios tendrá que editar el parámetro **X11Forwarding** del fichero de configuración el cual deberá quedar de la siguiente manera:

```
# Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding yes
```

4.4.3.8 Limitando el tiempo para autenticarse con SSH

El número indica la cantidad de segundos en que la pantalla de login estará disponible para que el usuario capture su nombre de usuario y contraseña, si no lo hace, el login se cerrará, evitando así dejar por tiempo indeterminado pantallas de login sin que nadie las use, o peor aun, que alguien este intentando mediante un script varias veces el adivinar un usuario y contraseña. Si somos el único usuario del sistema considero que con 20 o 30 segundos es mas que suficiente.

Para llevar a cabo estos cambios tendrá que editar el parámetro **LoginGraceTime** del fichero de configuración el cual deberá quedar de la siguiente manera:

```
# Authentication:

LoginGraceTime 30
PermitRootLogin no
StrictModes yes
MaxAuthTries 2
```

4.5 Iniciar, detener o reiniciar el servidor openSSH

Llegado a este punto usted ya deberá contar con las configuraciones de seguridad apropiadas, por lo que solo faltaría iniciar el servicio de SSH.

Para iniciar el servicio de SSH tendrá que teclear en consola y como **root** lo siguiente:

```
[root@ localhost ]# /etc/init.d/sshd start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el servicio. Estas opciones pueden ser consultadas en la siguiente tabla:

start	**Inicia el servicio**
stop	**Detiene el servicio**
restart	**Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta**
reload	**Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.**
condrestart	**Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.**
status	**Da a conocer el estado en el que se encuentra el servicio**

4.6 Anexando el servicio de SSH al arranque del servidor

Para añadir el servicio de SSH al arranque del servidor solo tendrá que teclear en consola y como **root** lo siguiente:

```
[root@ localhost ]# chkconfig sshd on
```

Esto es útil cuando por motivos ajenos a usted se reinicia el servidor, de esta manera cuando el equipo arranque, automáticamente levantara el servicio de SSH sin necesidad de levantarlo manualmente después.

4.7 Aprendiendo a utilizar openSSH

En esta parte del capitulo le enseñaremos a:

- Conectarse a un equipo remotamente a través de SSH
- Copiar archivos o carpetas desde un equipo remoto
- Enviar archivos o carpetas a un equipo remoto

4.7.1 Conectándose a un equipo remoto a través de SSH

Para establecer una conexión con un servidor SSH remoto desde Centos haremos uso del Bash, o también conocido como Terminal.

La sintaxis para llevar a cabo esta operación es la siguiente:

```
[root@ localhost ]# ssh usuarioRemoto@ipDelServidorRemoto
```

En caso de haber establecido un puerto de escucha distinto al puerto 22, solo deberá especificar el puerto por el cual requiere autenticarse al servidor. Ejemplo

```
[root@ localhost ]# ssh -p[puertoDeEscucha] usuarioRemoto@ipDelServidorRemoto
```

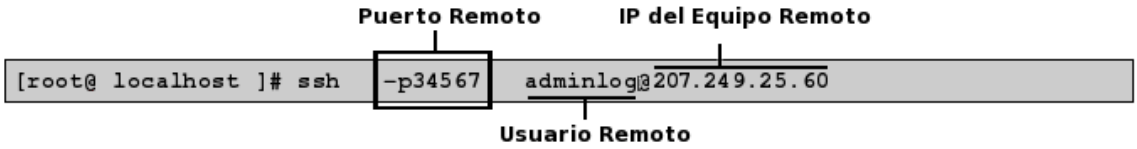
Ejemplo 1: La empresa Factor Integración para la cual trabajamos, nos ha pedido reiniciar el servicio de apache , para ello nos ha proporcionado los siguientes datos:

- IP del servidor remoto -> **207.249.25.60**
- Nombre del usuario remoto -> **adminlog**
- Puerto de autenticacion -> **34765**

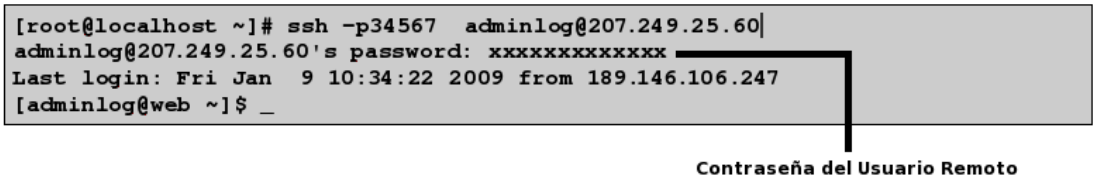
Solución:

1.-Para conectarnos al servidor remoto habrá que especificar el puerto de escucha, el usuario remoto y la IP del servidor remoto

(Recuerde que no esta permitido conectarse como root desde SSH)



2.-El siguiente paso sera teclear la contraseña del usuario remoto



3.-Una vez dentro del servidor remoto nos logearemos ahora si como **"root"**

```
[adminlog@ web ]# su -
Contraseña: xxxxxxxxxxxxxxxxx
[root@ web ]#
```

4.-Por ultimo, solo bastara reiniciar el servidor de apache

```
[root@ web ]# /etc/init.d/httpd restart
```

5.-Para salir del SSH solo basta teclear "exit"

```
[root@ web ]# exit
Connection to 207.249.25.60 closed.
[root@ localhost ~] # _
```

4.7.2 Copiar u obtener archivos o carpetas desde un equipo remoto

Para copiar archivos, ficheros o carpetas desde un equipo remoto hacia nuestro equipo existen dos maneras:

- Mediante el uso del comando SCP
- Mediante el uso del comando SFTP

4.7.2.1 Copiando ficheros a través de SCP (Shell Secure Copy)

Es un medio de transferencia segura de archivos entre un equipo local y uno remoto haciendo uso del protocolo Open Secure Shell (openSSH).

La diferencia en utilizar SCP (Shell) y SFTP (Security File Transfer Protocol) para copiar archivos, carpetas o ficheros radica en que para SCP tenemos que conocer exactamente donde se encuentra el recurso que queremos copiar, de otra forma nunca lo descargara, en cambio SFTP nos deja navegar entre las carpetas lo cual hace mas sencillo la ubicación del recurso que deseamos copiar. La única desventaja que presenta **SCP** es que únicamente permite la transferencia de archivos (descarga y subida de ficheros).

La sintaxis de SCP para llevar a cabo esta operación es la siguiente:

```
[root@ localhost ]#scp usuarioRemoto@ipDelServidorRemoto:rutaDelRecursoRemoto
```

En caso de haber establecido un puerto de escucha distinto al puerto 22, solo deberá especificar el puerto por el cual requiere autenticarse al servidor.

Ejemplo:

```
[root@ localhost ]#scp -P[puertoDeEscucha]
usuarioRemoto@ipDelServidorRemoto:rutaDelRecursoRemoto
```

Aunado a esto, para descargar una carpeta tendrá que seguir la siguiente sintaxis:

```
[root@ localhost ]#scp -P[puertoDeEscucha] -r
usuarioRemoto@ipDelServidorRemoto:rutaDelDirectorioRemoto
```

Ejemplo 2: La misma empresa, Factor Integración, nos ha pedido copiar la carpeta de inventarios de la empresa la cual esta hospedada en un servidor remoto , para ello nos ha proporcionado los siguientes datos:

- IP del servidor remoto -> **207.249.25.60**
- Nombre del usuario remoto -> **adminlog**
- Puerto de autenticacion -> **34567**
- Ruta del Recurso Remoto **-> /tmp/Conta**

Solución:

Para poder hacer la copia desde servidor remoto habrá que especificar el puerto de escucha, el usuario remoto, la IP del servidor remoto y la ruta (**sin errores**) del recurso remoto.

Lo anterior nos copiará la carpeta **"/tmp/Conta"** remota en el directorio actual **"."** naturalmente siempre que usuario tenga permisos sobre la carpeta y su cuenta esté entre las de los que pueden hacer ssh.

La opción **"-r"** significa recursivo, es decir, copia la carpeta y todo su contenido, incluidas las subcarpetas y el contenido de éstas.

4.7.2.2 Copiando ficheros a través de SFTP (Security File Transfer Protocol)

El protocolo de transferencia de archivos SFTP es un protocolo que proporciona la transferencia de archivos y la funcionalidad de manipulación de los mismos Se utiliza normalmente con SSH a fin de asegurar la transferencia de archivos.

En comparación de capacidades con el anterior protocolo SCP, que únicamente permite la transferencia de archivos, el protocolo SFTP permite una serie de operaciones sobre archivos, ficheros, o carpetas remotos, en pocas palabras, nos permite navegar directamente en el servidor remoto con el fin de localizar el recurso que deseamos descargar.

La sintaxis de SFTP para llevar a cabo esta operación es la siguiente:

```
[root@ localhost]# sftp usuarioRemoto@ipDelServidorRemoto
```

En caso de haber establecido un puerto de escucha distinto al puerto 22, solo deberá especificar el puerto por el cual requiere autenticarse al servidor. Ejemplo.

```
[root@ localhost]# sftp -o Port=[PuertoDeEscucha]
usuarioRemoto@ipDelServidorRemoto
```

El siguiente paso sera autenticarnos con la contraseña del usuario remoto

```
Connecting to IPDelServidorRemoto...
usuarioRemoto@IPDelServidorRemoto's password:  xxxxxxxxxxxxxxxxxxxx
```

Una vez dentro del servidor solo bastara ejecutar el comando **"get"** para descargar algún fichero o archivo.

```
[root@ localhost]# sftp -o Port=[PuertoDeEscucha]
usuarioRemoto@ipDelServidorRemoto
Connecting to IPDelServidorRemoto...
usuarioRemoto@IPDelServidorRemoto's password:  xxxxxxxxxxxxxxxxxxxx
sftp> get recursoRemoto
```

La siguiente tabla explica mas a detalle los comandos que pueden ser utilizados con **SFTP:**

cd [rutaRemota]	**Cambia de directorio dentro del servidor remoto**
lcd [rutaLocal]	**Cambia de directorio en el equipo local**
chgrp [grp] [rutaRemota]	**Cambia el grupo de trabajo de un fichero remoto. El [grp] tiene que ser un Group ID**
chmod [opciones] [rutaRemota]	**Cambia los permisos de Lectura, Escritura o de Ejecución a un fichero remoto**
chown [own] [rutaRemota]	**Cambia el grupo de trabajo de un fichero remoto. El [own] tiene que ser un User ID**
get [rutaRemota] [rutaLocal]	**Copia un recurso remoto en un equipo local**

lmkdir [rutaLocal]	**Crea una carpeta en el equipo local**
lpwd	**Imprime la ruta local en la cual estamos trabajando**
mkdir [rutaRemota]	**Crea una carpeta en el equipo remoto**
put [rutaLocal] [rutaRemota]	**Sube un fichero o archivo desde una ruta local hasta una ruta remota**
pwd	**Imprime la ruta remota en la cual estamos trabajando**
exit	**Salimos de SFTP**
rename [rutaLocal] [rutaRemota]	**Renombra un un fichero remoto**
rmdir [rutaRemota]	**Borra una carpeta remota**
rm [rutaRemota]	**Borra un fichero remoto**

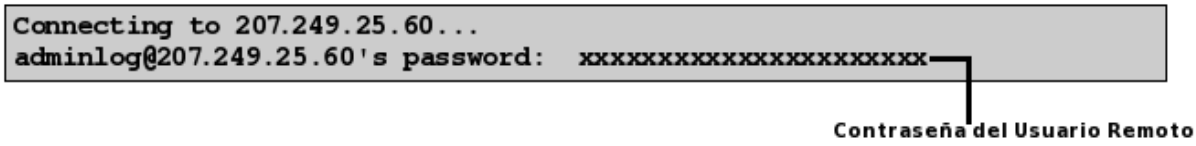
Ejemplo 3: La misma empresa, Factor Integración, nos ha pedido copiar el fichero **inventarioEnero.odt** que se encuentra dentro la ruta **"/tmp/Conta/"** , para ello nos ha proporcionado los siguientes datos:

- IP del servidor remoto -> **207.249.25.60**
- Nombre del usuario remoto -> **adminlog**
- Puerto de autenticacion -> **34567**
- Ruta del Recurso Remoto **-> /tmp/Conta**

Solución:

1.-Para poder traer la copia desde servidor remoto hacia nuestro equipo habrá que especificar el puerto de escucha, el usuario remoto y la IP del servidor remoto

2.- Nos pedirá autenticarnos con la contraseña del usuario remoto, en este caso la contraseña del usuario **"adminlog"**



3.-Una vez autenticados con el servidor nos dará acceso a través de SFTP

```
sftp>
```

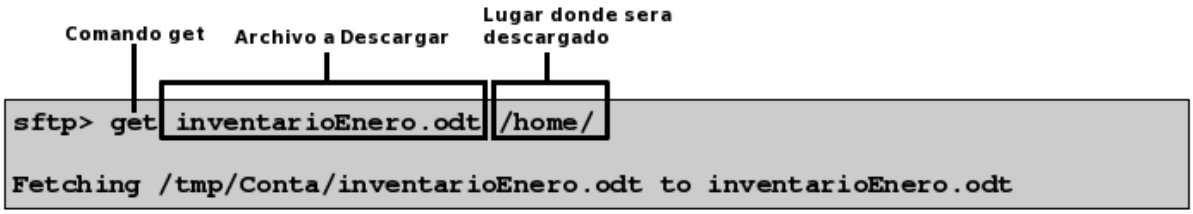
4.- Nos moveremos entre directorios con la ayuda del comando **"cd"** hasta estar ubicados en **"/tmp/Conta"**

```
sftp> cd /tmp/Conta
```

5.-Dentro de la carpeta **"Conta"** aplicar el comando **"dir"** para visualizar el contenido de la misma

```
sftp>dir

inventarioEnero.odt  inventarioFebrero.odt  inventarioMarzo.odt
```

6.-Con la ayuda del comando **"get"** descargaremos el fichero nombrado **"inventarioEnero.odt"** dentro de la carpeta **"home"** de nuestro sistema



4.7.3 Subir o enviar archivos o carpetas a un equipo remoto

Para subir archivos, ficheros o carpetas desde nuestro equipo hacia un equipo remoto existen dos maneras:

- Mediante el uso del comando SCP
- Mediante el uso del comando SFTP

4.7.3.1 Enviando ficheros a través de SCP (Shell Secure Copy)

La sintaxis de SCP para llevar a cabo esta operación es la siguiente:

```
[root@ localhost ]#scp rutaDelRecursoLocal
usuarioRemoto@ipDelServidorRemoto:rutaRemota
```

En caso de haber establecido un puerto de escucha distinto al puerto 22, solo deberá especificar el puerto por el cual requiere autenticarse al servidor. Ejemplo

```
[root@ localhost ]#scp -P[puertoDeEscucha] rutaDelRecursoLocal
usuarioRemoto@ipDelServidorRemoto:rutaRemota
```

Aunado a esto, para subir una carpeta tendrá que seguir la siguiente sintaxis:

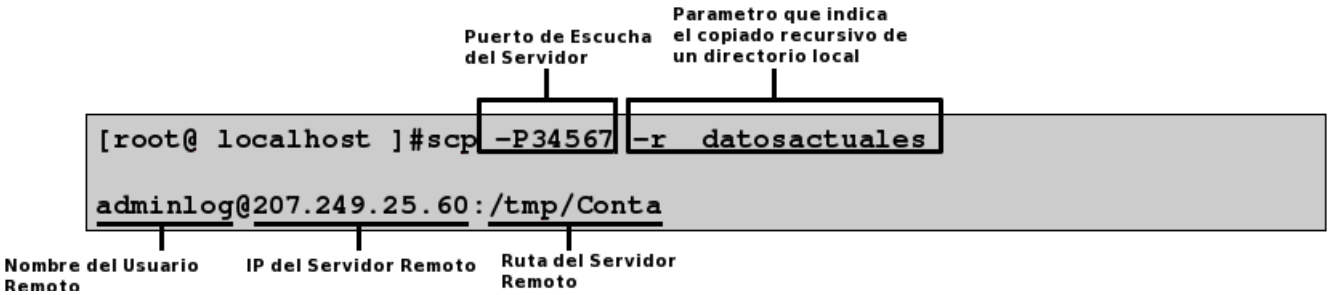
```
[root@ localhost ]#scp -P[puertoDeEscucha] -r directorioLocal
usuarioRemoto@ipDelServidorRemoto:rutaRemota
```

Ejemplo 4: Se nos ha pedido subir una actualización referente a la pagina web de la empresa , para ello nos ha proporcionado los siguientes datos:

- IP del servidor remoto -> **207.249.25.60**
- Nombre del usuario remoto -> **adminlog**
- Puerto de autenticacion -> **34567**
- Ruta del Servidor a donde se tiene que subir la información **-> /tmp/Conta**

Solución:

Para subir este directorio al servidor remoto habrá que especificar la ruta del directorio local,el puerto de escucha, el usuario remoto, la IP del servidor remoto y la ruta (**sin errores**) a donde se quiere enviar el directorio



Luego de haber hecho esto nos pedirá autenticarnos con la contraseña del usuario remoto

```
adminlog@207.249.25.60's password:xxxxxxxxxxxx
```

Al finalizar nos mostrara un ventana mostrando el progreso de cada copia hecha al servidor remoto como la que se muestra a continuación.

```
Actualizacion1.html       100%                0.0KB/s       05:00
actualizacion2.html       100%                0.0KB/s       07:00
actualizacion3.html       100%                0.0KB/s       15:00
actualizacion4.html       100%                0.0KB/s       15:00
actualizacion5.html       100%                0.0KB/s       25:00
actualizacion6.html       100%                0.0KB/s       30:00
actualizacion7.html       100%                0.0KB/s       31:00
actualizacion8.html       100%                0.0KB/s       40:00
```

4.7.3.2 Enviando ficheros a través de SFTP (Security File Transfer Protocol)

La sintaxis de SFTP para llevar a cabo esta operación es la siguiente:

```
[root@ localhost]# sftp usuarioRemoto@ipDelServidorRemoto
```

En caso de haber establecido un puerto de escucha distinto al puerto 22, solo deberá especificar el puerto por el cual requiere autenticarse al servidor. Ejemplo.

```
[root@ localhost]# sftp -o Port=[PuertoDeEscucha]
usuarioRemoto@ipDelServidorRemoto
```

El siguiente paso sera autenticarnos con la contraseña del usuario remoto

```
Connecting to IPDelServidorRemoto...
usuarioRemoto@IPDelServidorRemoto's password:  xxxxxxxxxxxxxxxxxxxx
```

Una vez dentro del servidor solo bastara ejecutar el comando **"put"** para descargar algún fichero o archivo.

```
[root@ localhost]# sftp -o Port=[PuertoDeEscucha]
usuarioRemoto@ipDelServidorRemoto
Connecting to IPDelServidorRemoto...
usuarioRemoto@IPDelServidorRemoto's password:  xxxxxxxxxxxxxxxxxxxx
sftp> put recursoLocal
```

La siguiente tabla explica mas a detalle los comandos que pueden ser utilizados con **SFTP:**

cd [rutaRemota]	**Cambia de directorio dentro del servidor remoto**
lcd [rutaLocal]	**Cambia de directorio en el equipo local**
chgrp [grp] [rutaRemota]	**Cambia el grupo de trabajo de un fichero remoto. El [grp] tiene que ser un Group ID**
chmod [opciones] [rutaRemota]	**Cambia los permisos de Lectura, Escritura o de Ejecución a un fichero remoto**
chown [own] [rutaRemota]	**Cambia el grupo de trabajo de un fichero remoto. El [own] tiene que ser un User ID**
get [rutaRemota] [rutaLocal]	**Copia un recurso remoto en un equipo local**
lmkdir [rutaLocal]	**Crea una carpeta en el equipo local**
lpwd	**Imprime la ruta local en la cual estamos trabajando**
mkdir [rutaRemota]	**Crea una carpeta en el equipo remoto**
put [rutaLocal] [rutaRemota]	**Sube un fichero o archivo desde una ruta local hasta una ruta remota**
pwd	**Imprime la ruta remota en la cual estamos trabajando**
exit	**Salimos de SFTP**

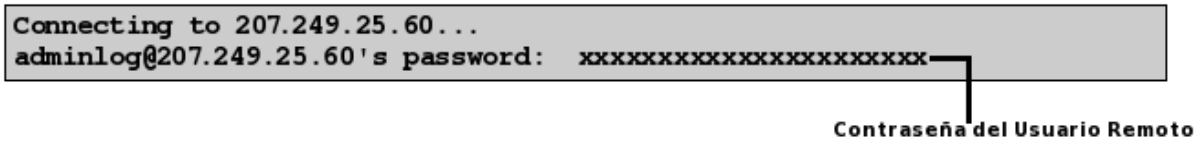
rename [rutaLocal] [rutaRemota]	**Renombra un un fichero remoto**
rmdir [rutaRemota]	**Borra una carpeta remota**
rm [rutaRemota]	**Borra un fichero remoto**

Ejemplo 5: Se nos ha pedido subir una actualización referente a la pagina web de la empresa , pero esta vez sera usando **SFTP**, para ello nos ha proporcionado los siguientes datos:

- IP del servidor remoto -> **207.249.25.60**
- Nombre del usuario remoto -> **adminlog**
- Puerto de autenticacion -> **34567**
- Ruta del Servidor a donde se tiene que subir la información **-> /tmp/Conta**
- Solución:

  1.- Para subir este directorio al servidor remoto habrá que especificar el puerto de escucha, el usuario remoto y la IP del servidor remoto

2.- Nos pedirá autenticarnos con la contraseña del usuario remoto, en este caso la contraseña del usuario **"adminlog"**



3.-Una vez autenticados con el servidor nos dará acceso a través de SFTP

```
sftp>
```

4.- Nos moveremos entre directorios con la ayuda del comando **"cd"** hasta estar ubicados en **"/tmp/Conta"**

```
sftp> cd /tmp/Conta
```

5.-Dentro de la carpeta **"Conta"** aplicar el comando "lpwd" para verificar la ruta en la cual estamos ubicados localmente

```
sftp> lpwd
Local working directory: /home/juanito
```

6.-Si no se encuentra ubicado en el directorio de trabajo indicado cámbiese de directorio mediante el comando "lcd"

```
sftp> lcd /home/juanito/datosActualizados
lcd /home/juanito/datosActualizados
```

7.- Cuando este ubicado en el directorio de trabajo que contiene la información que desea subir al servidor remoto teclee lo siguiente:

```
sftp> put datosactuales
```

El comando **"put"** tiene la funcionalidad de subir archivos desde una maquina local hasta un equipo remoto.

8.- Por ultimo teclee la palabra exit para salir del **"SFTP"**

```
sftp> exit
[root@localhost ]#
```

4.8 Evitar que nos pida autenticacion el servidor SSH

Siempre que intentemos conectarnos a un equipo remoto con SSH nos va a pedir la contraseña de acceso para asegurarse de que tenemos acceso al mismo. Hay una forma de evitar que nos pase eso siempre. Para ello hemos de generar un par de llaves RSA y DSA las cuales sirven como claves de autenticacion entre los dos equipos remotos.

4.8.1 RSA

Es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye en forma autenticada, y otra privada, la cual es guardada en secreto por su propietario.

Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes mayores que 10100 elegidos al azar para conformar la clave de descifrado.

4.8.2 DSA (Digital Signature Algorithm)

Es un estándar del Gobierno Federal de los Estados Unidos de América para firmas digitales. Fue un Algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de los Estados Unidos para su uso en su Estándar de Firma Digital. Este algoritmo como su nombre lo indica, sirve para firmar y no para cifrar información. Una desventaja de este algoritmo es que requiere mucho más tiempo de cómputo que RSA.

El proceso para generar estas claves es el siguiente:

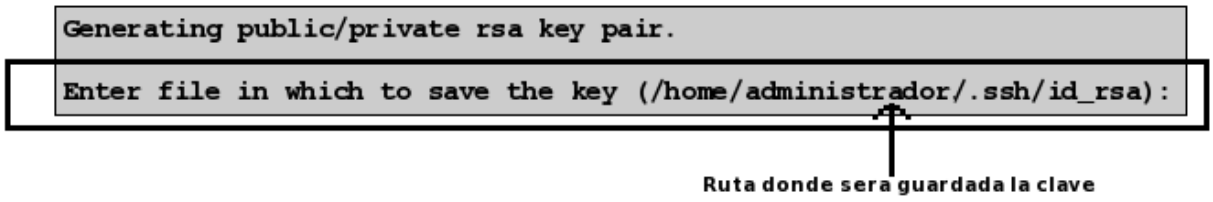
4.8.3 Generación de claves RSA

1.-Teclee el siguiente comando desde una terminal BASH

[NOTA: El comando debe ejecutarse en el equipo cliente]

```
[root@ localhost ]# ssh-keygen -t rsa
```

2.-Al haber tecleado el comando este nos preguntara si queremos guardar esa clave en otra ubicación, por defecto seleccionaremos la que nos da por defecto



3.- Al haber aceptado nos pedirá introducir una contraseña y confirmarla nuevamente

```
Enter passphrase (empty for no passphrase):xxxxxxxxxxxxx
Enter same passphrase again: xxxxxxxxxxxxxx
```

4.- Finalmente nos creara dos tipos de clave:

- Una Publica, la cual sera almacenada en la ruta:

```
/home/administrador/.ssh/id_rsa.pub
```

- Una Privada, la cual sera almacenada en la ruta:

```
/home/administrador/.ssh/id_rsa
```

Tras haber terminado de generar las claves nos tendrá que aparecer algo similar a esto

```
Your identification has been saved in /home/administrador/.ssh/id_rsa.
Your public key has been saved in /home/administrador/.ssh/id_rsa.pub.
The key fingerprint is:
c8:d1:10:62:52:1d:97:5d:7d:5a:d3:84:b5:24:48:3d administrador@localdomain
```

5.- El siguiente paso sera cambiar los permisos de ejecución del siguiente directorio

```
/home/administrador/.ssh
```

lo cual se hará de la siguiente manera:

```
[root@ localhost ]# chmod 755 /home/administrador/.ssh
```

6.- Lo siguiente sera copiar el contenido del fichero

```
/home/administrador/.ssh/id_rsa.pub
```

al fichero

```
/home/usuarioRemoto/.ssh/authorized_keys
```

del equipo remoto. Si este no existe no se preocupe, generelo con el uso del comando **"touch"** y pegue dentro de este el contenido del fichero

En caso de que el fichero

```
authorized_keys
```

exista solo pegue el contenido del fichero

```
id_rsa.pub
```

al fichero

```
authorized_keys
```

7.- El siguiente paso sera cambiar los permisos de ejecución del siguiente directorio remoto

```
/home/usuarioRemoto/.ssh/authorized_keys
```

lo cual se hará de la siguiente manera:

```
[root@ localhost ]# chmod 644 /home/usuarioRemoto/.ssh/authorized_keys
```

Con esto habremos concluido la generación de la clave RSA, ahora solo nos falta generar la clave **DSA**

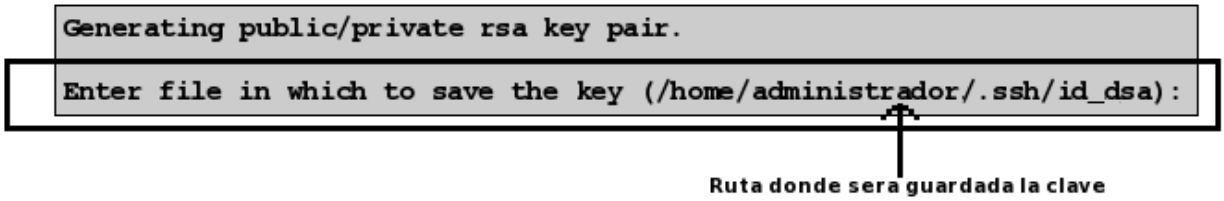
4.8.4 Generación de claves DSA

1.-Teclee el siguiente comando desde una terminal BASH

[NOTA: El comando debe ejecutarse en el equipo cliente]

```
[root@ localhost ]# ssh-keygen -t dsa
```

2.-Al haber tecleado el comando este nos preguntara si queremos guardar esa clave en otra ubicación, por defecto seleccionaremos la que nos da por defecto



3.- Al haber aceptado nos pedirá introducir una contraseña y confirmarla nuevamente

```
Enter passphrase (empty for no passphrase):xxxxxxxxxxxxxx
Enter same passphrase again: xxxxxxxxxxxxxx
```

4.- Finalmente nos creara dos tipos de clave:

- Una Publica, la cual sera almacenada en la ruta:

```
/home/usuario/.ssh/id_dsa.pub
```

- Una Privada, la cual sera almacenada en la ruta:

```
/home/usuario/.ssh/id_dsa
```

Tras haber terminado de generar las claves nos tendrá que aparecer algo similar a esto

```
Your identification has been saved in /home/administrador .ssh/id_dsa.
Your public key has been saved in /home/administrador/.ssh/id_dsa.pub.
The key fingerprint is:
5d:7d:5a:d3:84:b5:24:48:3d:c8:d1:10:62:52:1d:97: administrador@localdomain
```

5.- El siguiente paso sera cambiar los permisos de ejecución del siguiente directorio

```
/home/administrador/.ssh
```

lo cual se hará de la siguiente manera:

```
[root@ localhost ]# chmod 755 /home/administrador/.ssh
```

6.- Lo siguiente sera copiar el contenido del fichero

```
/home/usuario/.ssh/id_dsa.pub
```

al fichero

```
/home/usuarioRemoto/.ssh/authorized_keys
```

del equipo remoto. Si este no existe no se preocupe, generelo con el uso del comando **"touch"** y pegue dentro de este el contenido del fichero

En caso de que el fichero

```
authorized_keys
```

exista solo pegue el contenido del fichero

```
id_dsa.pub
```

al fichero

```
authorized_keys
```

7.- El siguiente paso sera cambiar los permisos de ejecución del siguiente directorio remoto

```
/home/usuarioRemoto/.ssh/authorized_keys
```

lo cual se hará de la siguiente manera:

```
[root@ localhost ]# chmod 644 /home/usuarioRemoto/.ssh/authorized_keys
```

Con esto habremos concluido la generación de las dos claves y de esa manera ya no tendremos que autenticarnos cada vez que nos conectemos vía SSH hacia algún equipo remoto

4.9 Montando un sistema de ficheros remoto usando sshfs y fuse

Nosotros podemos acceder a un sistema de ficheros remoto usando **sshfs** en conjunto con la aplicación **"fuse"** el cual es un comando que nos permite montar un sistema de ficheros remotos cifrados mediante la implementacion del protocolo openSSH.

De esta manera nosotros podemos acceder a los archivos remotos como si estuvieran dentro de nuestra maquina, solo debemos recordar que la conexión entre las computadoras sera un tanto lenta.

4.9.1 Sobre sshfs

sshfs (Secure Shell File System) es un sistema de ficheros de Linux que tiene como funcionalidad montar sistemas de ficheros remotos en nuestro equipo mediante la implementacion del modulo del kernel **FUSE**

Los efectos prácticos de esto es que el usuario final puede interactuar amigablemente con archivos remotos estando en un servidor SSH,viéndolos como si estuvieran en su computadora local.

4.9.2 Sobre FUSE

El sistema de archivos en espacio de usuario FUSE (Filesystem in Userspace) es un modulo cargable del kernel de linux que permite a los usuarios crear sus propios sistemas de ficheros. Esto se logra mediante la ejecución del código del sistema de archivos en el espacio de usuario, mientras que el módulo FUSE sólo proporciona un puente a la interfaz del kernel real

4.10 Instalando sshfs y fuse

Los paquetes necesarios para la instalación serán:

- **sshfs**
- **fuse-utils**

1.- Teclee la siguiente instrucción desde una terminal BASH para instalar los paquetes antes descritos:

```
[root@ localhost ]# yum install -y fuse-utils sshfs
```

2.- El siguiente paso sera crear un punto de montaje para el sistema de ficheros remoto, esto lo haremos tecleando el siguiente comando:

```
[root@ localhost ]# mkdir  /mnt/carpetaRemota
```

3.- Cambie el propietario y grupo del directorio antes creado

```
[root@ localhost ]# chown suUsuario:suGrupo /mnt/carpetaRemota
```

4.- De de alta al grupo “fuse”

```
[root@ localhost ]# groupadd fuse
```

5.- Añadase al grupo de trabajo “fuse”

```
[root@ localhost ]# usermod -G fuse suUsuario
```

6.- Por ultimo solo deberá montar el sistema de ficheros remoto, para llevar a cabo esta operación deberá ejecutarlo como root del sistema

```
[root@ localhost ]# sshfs usurioRemoto@servidorRemoto:/directorioRemoto
    /mnt/carpetaRemota
```

7.- Si se tiene especificado algún puerto de escucha para el servidor de SSH solo deberá especificare mediante el parámetro “-P”

```
[root@ localhost ]# sshfs -P[puertoDeEscucha]
usurioRemoto@servidorRemoto:/directorioRemoto
    /mnt/carpetaRemota
```

8.-Por ultimo, si quiere verificar que se encuentra montado el directorio remoto abra un navegador de archivos como Nautilus o Konqueror y con al ayuda de ellos visualice el contenido de dicho directorio.

Índice de contenido

Información de Derechos reservados de esta publicación.

Autor del manual: Javier Eduardo Duarte

Tema 5. Servidor Web Apache

5.1 Como empezó todo

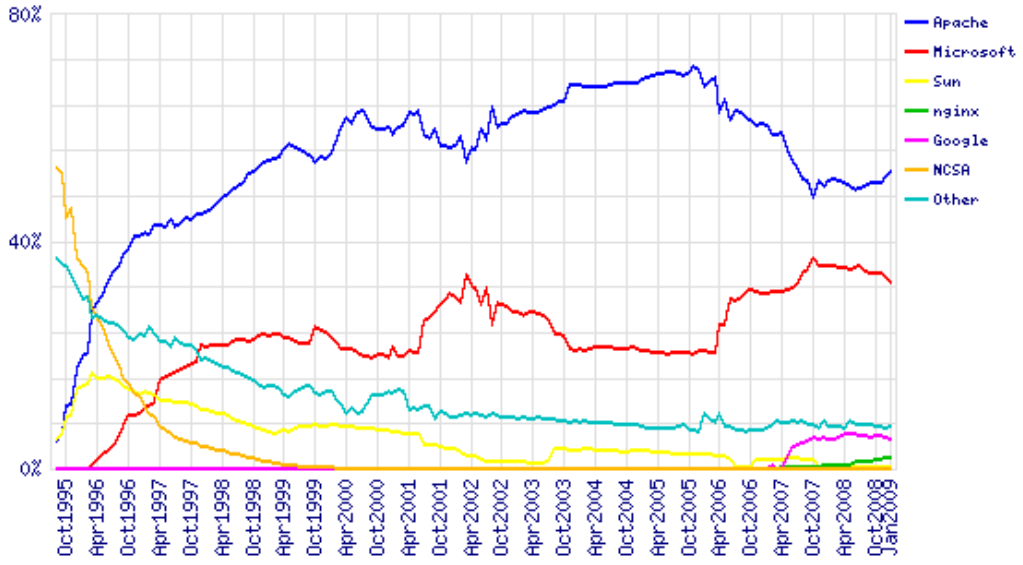
El nombre del servidor web apache proviene de la palabra en ingles patchy server que en español se puede entender como servidor parchado, ¿Tal vez te preguntaras, porque parchado?, la explicación es sencilla, el servidor web apache fue conformado por diversos parches del servidor web usado en ese momento, nos referimos al servidor web NCSA el cual era desarrollado en ese entonces por el National Center Supercomputing.

El desarrollo del servidor web apache se remonta al lejano año de 1995, dicho desarrollo dio como resultado una especie de versión beta de lo que llegaría a convertirse en la primera versión de apache ya que estaba compuesto en su totalidad por una colección de parches del servidor web NCSA. Fue hasta el año de 1996 cuando fue lanzada la primera versión estable de Apache la cual tenia entre sus principales características la reescritura por completo de su código base, también incluía la carga de módulos en tiempo de ejecución. Meses mas tarde fue lanzada la versión 1.1 la cual tenia como novedad la inclusión de un modulo de autenticacion contra bases de datos. La versión 1.3 de apache vio la luz en el año de 1998 y esta incluía como principal característica soporte para plataformas Windows.

Actualmente el servidor web apache se encuentra en su versión 2 e incluye notables mejoras con respecto a versiones anteriores, algunas de ellas son:

- Modo Híbrido
- Nuevo sistema de configuración y compilación
- Soporte nativo para Ipv6
- Mensajes de error en diferentes idiomas
- Mejoras adicionales.

Como dato adicional, cabe menciona que apache es el servidor web numero uno a nivel mundial el cual abarca cerca de un 52.26 % del mercado total de Internet desbancando a servidores web como el IIS (Internet Information Server) de Microsoft.



Estos cifras pueden ser verificadas visitando el portal de Netcraft

```
http://news.netcraft.com/
```

Existe también una fundación dedicada a dar soporte legal y financiero al desarrollo de los proyectos relacionados con Apache , el nombre de esta fundación es Apache Software Foundation, la cual actualmente esta conformada por una comunidad de desarrolladores los cuales día a día contribuyen a la expansión y mejora de proyectos.

Entre los proyectos mas destacados de esta fundación podemos encontrar los siguientes:

- Http Server.- Servidor Web Apache

  http://www.apache.org/
- Jakarta.-Proyectos en el lado del servidor basados en Java

  http://tomcat.apache.org/
- mod_perl.- Modulo de apache para la programación dinámica en Perl

  http://perl.apache.org/
- SpamAssin.-Sistema de detección de Spam

  http://spamassassin.apache.org/

5.2 Proceso de instalación del servidor web Apache

5.2.1 Instalando el servidor web apache

La instalación del servidor web apache es relativamente sencilla , solo debe teclear en terminal el siguiente comando.

```
[root@ localhost ~]# yum install -y httpd
```

Recuerde que este comando se debe ejecutar como root

5.2.2 Archivos de configuración del servidor web Apache

La configuración del servidor web apache se realizara sobre dos ficheros distintos, uno de configuración general del servidor web apache y otro para indicarle al servidor apache los dominios virtuales que deben ser cargados al sistema.

El fichero de configuración principal de apache lo encontramos en la siguiente ruta

```
/etc/httpd/conf/
```

La carpeta donde deberán ser añadidos los ficheros de configuración de los dominios virtuales sera en la siguiente ruta:

```
/etc/httpd/conf.d/
```

5.2.2.1 Configuración del fichero httpd.conf

La ubicación de este fichero lo encontramos en:

```
/etc/httpd/conf/  ----->   httpd.conf
```

El contenido del fichero “httpd.conf” esta compuesto por un gran numero de secciones es por ello que solo describiremos las mas relevantes del mismo, usted podrá habilitar o deshabilitar cada una de las funciones que describiremos según su necesidad.

5.2.2.1.1 Directiva ServerTokens

Esta directiva limita la cantidad de información que sera mostrada por nuestro servidor web apache como puede ser, la version del servidor web apache que tenemos instalado o los servicios que corren paralelamente con apache como php o MySQL.

Para delimitar la cantidad de información mostrada por el sistema existen cuatro opciones

ServerTokens ProductOnly	**Solo mostrara el nombre del servidor web instalado.** **Ejemplo:** **Server Apache**
ServerTokens Minimal	**Muestra el nombre asi como la version de apache instalada.** **Ejemplo:** **Server Apache 2.1**
ServerTokens OS	**Mostrara el nombre, version y sistema operativo sobre el cual se encuentra montado:** **Ejemplo:** **Server Apache 1.3/(Linux)**
ServerTokens Full	**Mostrara nombre, version, sistema operativo asi como los servicios que hacen uso del servidor web.** **Ejemplo:** **Apache 1.3/(Linux)/PHP3/MySQL**

5.2.2.1.2 Directiva ServerRoot

Esta directiva le indica al servidor web la ubicación donde se almacenan los ficheros de configuración de apache.

El valor por defecto es:

```
ServerRoot "/etc/httpd"
```

Si usted quisiera ubicar estos ficheros en otra ruta diferente solo deberá especificarla, aunque no es recomendable

5.2.2.1.3 Directiva Timeout

Esta directiva indica el número de segundos antes de que se cancele un conexión por falta de respuesta. Su valor por defecto es 120

```
Timeout 120
```

5.2.2.1.4 Directiva KeepAlive

Esta directiva indica si se permiten o no las conexiones persistentes, es decir más de una petición por conexión. Puede tomar los valores de “On” u “Off”.

```
KeepAlive On|Off
```

5.2.2.1.5 Directiva MaxKeepAliveRequests

Esta directiva indica el máximo número de peticiones que se permiten en conexiones persistentes. Un valor 0 permite un número ilimitado. Se recomienda dejar esta valor elevado para obtener un mayor rendimiento. Por ejemplo100

```
MaxKeepAliveRequests 100
```

5.2.2.1.6 Directiva KeepAliveTimeout

Esta directiva indica el número de segundos de espera para la siguiente petición del mismo cliente con la misma conexión. Por ejemplo 15

```
KeepAliveTimeout 15
```

5.2.2.1.7 Directiva Listen

Listen permite asociar Apache a una dirección y/o puerto específico además del predeterminado.

Ejemplo:

```
Listen 192.168.1.1:8080
Listen 80
```

5.2.2.1.8 Directiva Include

```
Include conf.d/*.conf
```

Esta directiva indica al servidor web la ruta en donde se encuentran almacenados los ficheros de configuración adicionales de apache como por ejemplo los dominios virtuales.

Es habitual dejar el fichero de configuración con las características globales que no se tienen que modificar en el fichero principal e incluir los ficheros que pueden estar sujetos a modificación en el directorio

```
"/etc/httpd/conf.d"
```

De esta forma para añadir o quitar algún fichero de configuración de apache sólo tenemos que borrarlo del directorio /etc/httpd/conf.d

5.2.2.1.9 Directiva LoadModule

Esta directiva corresponde al soporte de Dynamic Shared Object (Objetos Dinámicos Compartidos). Son módulos que incorporan ciertas funcionalidades que se le incorporan al servidor Apache. Para que un módulo sea funcional tienen que estar construido como un DSO e incorporar la correspondiente directiva `LoadModule' antes de que se a utilizada. Los módulos compilados de forma estática no es necesario incluirlos.

Ejemplo:

```
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule authn_alias_module modules/mod_authn_alias.so
LoadModule authn_anon_module modules/mod_authn_anon.so
```

5.2.2.1.10 Directiva User

Esta directiva especifica qué usuario es el que ejecuta los procesos del servidor web y en consecuencia los permisos de lectura y escritura que se aplican sobre los recursos.

```
User apache
```

5.2.2.1.11 Directiva Group

Esta directiva especifica qué grupo es el que ejecuta los procesos del servidor web y en consecuencia los permisos de lectura y escritura que se aplican sobre los recursos.

```
Group apache
```

5.2.2.1.12 Directiva ServerAdmin

Esta directiva especifica la persona a la que se le debe notificar los problemas referentes al portal web , esto a través de su cuenta de correo.

Ejemplo:

```
ServerAdmin administrador@tuDominio.net
```

5.2.2.1.13 Directiva ServerName

Esta directiva especifica el nombre y puerto que el servidor utiliza para identificarse. Con una correcta configuración, este valor se puede determinar automáticamente, pero es recomendable especificarlo explíciatamente para evitar problemas durante el arranque.

```
ServerName www.tuDominio.net:80
```

5.2.2.1.12 Directiva UseCanonicalName

UseCanonicalName determina como Apache construye las autoreferencias de URL y las variables SERVER_NAME y SERVER_PORT.

Cuando está directiva esta como "Off" apache usa los valores suministrados por el cliente. Cuando está como "On" , apache usa la directiva ServerName.

```
UseCanonicalName On|Off
```

5.2.2.1.13 Directiva DocumentRoot

Esta directiva indica al servidor web la ruta en donde se encuentran almacenados los ficheros web de tu sitio principal

```
DocumentRoot "/var/www/html"
```

NOTA:Esta directiva cambia cuando se implementan sitios virtuales

5.2.2.1.14 Directiva Options

La directiva Options indica varias posibles opciones de comportamiento y estas pueden ser aplicadas a un directorio concreto. Un claro ejemplo de aplicación de estas directiva se puede observar en el siguiente cuadro:

```
Directory /web/docs>
      Options Indexes FollowSymLinks
</Directory>

<Directory /web/docs/spec>
      Options Includes
</Directory>
```

Las opciones que podemos observar se explican con mas detalle en el siguiente cuadro:

All	todas las opciones salvo MultiViews
ExecCGI	Se permite la ejecución de scripts CGI.
FollowSymLinks	el servidor seguirá los enlaces simbólicos. Tener esta opción activa aumenta el rendimiento ya que el servidor no comprueba si un fichero o directorio es un enlace simbólico y es más rápido, pero en algunos casos puede presentar problemas de inseguridad.
Includes	Se permiten incluir Server-side.
Indexes	Si una URL solicita un directorio y no existe DirectoryIndex (v.g., index.html) en ese directorio, el servidor devolverá una lista del contenido del directorio.
MultiViews	Se permite mostrar contenido negociado en función de diversos valores.
SymLinksIfOwnerMatch	Se sigue un enlace simbólico sólo si los propietarios del enlace y del destino coinciden.

5.2.2.1.15 Directiva AllowOverride

La directiva AllowOverride controla qué directivas se pueden situar el los ficheros .htaccess y estas pueden ser aplicadas igualmente a un directorio concreto. Un claro ejemplo de aplicación de estas directiva se puede observar en el siguiente cuadro:

```
<Directory "/var/www/icons">
    Options Indexes MultiViews FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

Los valores de AllowOverride pueden ser "All", "None", o una combinación de:

AuthConfig	Permitir el uso de directivas de autorización (AuthDBMGroupFile, AuthDBMUserFile, AuthGroupFile, AuthName, AuthType, AuthUserFile, Require, etc).
FileInfo	Permitir el uso de directivas de control de tipo de documentos (DefaultType, ErrorDocument, ForceType, LanguagePriority, SetHandler, SetInputFilter, SetOutputFilter, etc).
Indexes	Permitir el uso de directivas que controlan los índices de directorios (AddDescription, AddIcon, AddIconByEncoding, AddIconByType, DefaultIcon, DirectoryIndex, FancyIndexing, HeaderName, IndexIgnore, IndexOptions, ReadmeName, etc).
Limit	Permitir el uso de directivas de acceso de hosts (Allow, Deny y Order).
Options	Permitir el uso de las opciones antes vistas en la directiva Options

5.2.2.1.16 Directiva Allow

La directiva Allow indica al sistema los equipos que pueden acceder a una determinada área del servidor. El acceso se puede controlar por nombre, IP, rango de IP, igualmente pueden ser aplicadas a un directorio concreto

El primer argumento de esta directiva es siempre **"from"**. Los siguientes argumentos pueden tener diferentes formas:

All permite el acceso a todos los equipos excepto los especificados en Deny y Order que se verá más adelante.

Para permitir el acceso a un dominio en especifico solo se deberá especificar el antes mencionado

Ejemplo:

```
Allow from linuxparatodos.net
```

También puede aplicarse esa misma regla usando direcciones IP

Ejemplo:

```
Allow from 207.249.24.61
```

5.2.2.1.17 Directiva Deny

La directiva Deny indica al sistema los equipos que no podrán acceder al servidor web. El acceso se puede controlar por nombre, IP, rango de IP, igualmente pueden ser aplicadas a un directorio concreto

El primer argumento de esta directiva es siempre **"from"**. Los siguientes argumentos pueden tener diferentes formas:

Para denegar el acceso a un dominio en especifico solo se deberá especificar el antes mencionado

Ejemplo:

```
Deny from microsoft.com
```

También puede aplicarse esa misma regla usando direcciones IP

Ejemplo:

```
Allow from 207.249.0.60
```

5.2.2.1.17 Directiva Order

Esta directiva trabaja en conjunto con las dos directivas anteriores asi mismo se encarga de controlar el orden en que se ejecutan las antes descritas. Igualmente pueden ser aplicadas a un directorio concreto

Ejemplo 1:

```
Order Deny,Allow
```

En este ejemplo se evaluá primero Deny, de esta forma se permite el acceso a cualquier equipo que no este listado en Deny, de esta forma el acceso se garantiza por defecto.

Ejemplo 2:

```
Order Allow,Deny
```

En este ejemplo se evaluá primero Allow, de esta forma se niega el acceso a cualquier equipo que no este listado en Allow, de esta forma el acceso se niega por defecto.

5.2.2.1.18 Directiva Alias

La directiva Alias permite alojar ficheros fuera del directorio especificado en **DocumentRoot ,** igualmente pueden ser aplicadas a un directorio concreto

La sintaxis necesaria para aplicar la directiva Alias es la siguiente:

```
Alias directorioAlternativo "/vaw/www/manual"
```

Ejemplo

```
Alias /home/gerencia "/var/www/gerencia"
```

5.2.2.1.18 Directiva ErrorLog

ErrorLog indica la ubicación del fichero de registro de errores en las consultas. Es conveniente especificar un fichero de registro en cada VirtualHost con el nombre asociado a ese servidor. De esta forma podemos separar los registros de los distintos dominios que tengamos albergados en el servidor web.

Ejemplo:

```
ErrorLog logs/error_log
```

5.2.2.1.19 Directiva ErrorLevel

LogLevel Controla el número de mensajes registrados en error_log.

Puede ser: debug, info, notice, warn, error, crit, alert, emerg.

5.2.2.1.19 Directiva Redirect

La directiva Redirect permite indicar al cliente que un documento ha sido modificado o actualizado.

Ejemplo

```
Redirect permanent /portal1  http://www.ies-bezmiliana/portal2
```

5.2.3 Iniciar , detener o reiniciar el servidor web Apache

Para iniciar el servidor FTP por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/httpd start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el servidor FTP. Estas opciones pueden ser consultadas en la siguiente tabla:

start	**Inicia el servicio**
stop	**Detiene el servicio**
restart	**Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta**
reload	**Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.**
condrestart	**Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.**
status	**Da a conocer el estado en el que se encuentra el servicio**

Como alternativa también podemos ocupar el siguiente comando para iniciar el servidor FTP

```
[root@ localhost ~]# service httpd start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root.

5.3 Creación de dominios virtuales en Apache

La creación de dominios virtuales sobre un servidor web como apache tiene una vital importancia cuando se trata de dar hospedaje a varios sitios web dentro del mismo servidor.

Lograr implementar de manera correcta los dominios virtuales sobre el servidor web apache es tarea sencilla por lo que le recomendamos primero haber leído todas las directivas que pueden ser aplicadas al fichero

```
httpd.conf
```

A partir de este punto comenzaremos a crear los dominios virtuales, es por ello que pedimos tu total concentración y paciencia para que leas poco a poco estos puntos.

5.3.1 Paso 1.- Activando la directiva NameVirtualHost

El primer paso sera abrir el fichero

```
httpd.conf
```

el cual esta almacenado en la ruta:

```
/etc/httpd/conf/
```

En dicho fichero debemos localizar la siguiente linea y descomentarla si es que lo esta

```
NameVirtualHost *:80
```

La función de esta directiva sirve para indicar la dirección IP en la que se esta brindando el servicio o bien insertando un asterisco(*) para que esté activa en cualquier interfaz del servidor que es como nosotros lo debemos tener.

5.3.2 Paso 2.- Estructura de directorios para dominios virtuales

Lo siguiente sera crear la estructura que contendrá cada uno de los dominios virtuales que serán hospedados en nuestro servidor.

Ejemplo: Suponga que tenemos 5 nombres de dominio que serán hospedados en nuestro servidor web

```
www.turbolinux.com.mx
www.comerciolinux.com
www.escuelalinux.edu
www.linuxunido.org
www.linuxbloger.net
```

por cada dominio se deberá crear un directorio, dicho directorio sera nombrado de la misma forma que el dominio, solo omitiendo el **"www".**

```
[root@ localhost ~]# mkdir turbolinux.com.mx
[root@ localhost ~]# mkdir comerciolinux.com
[root@ localhost ~]# mkdir escuelalinux.edu
[root@ localhost ~]# mkdir linuxunido.org
[root@ localhost ~]# mkdir linuxbloger.net
```

Estos directorios deberán ser creados dentro de la ruta

```
"/var/www/"
```

Al final estos directorios deberán quedar de la siguiente manera

```
/var/www/turbolinux.com.mx
/var/www/comerciolinux.com
/var/www/escuelalinux.edu
/var/www/linuxunido.org
/var/www/linuxbloger.net
```

Si no están en la ruta antes descrita solo debe moverlos con el comando **"mv"**

Lo siguiente sera crear dentro de cada uno de estos directorios la estructura básica que debe llevar cada uno de estos dominios. Esta estructura estará conformada por cuatro directorios:

- html
- cgi-bin
- icons
- error

por lo que deberá crear estos cuatro directorios para cada uno de los directorios de dominio.

Ejemplo para el dominio turbolinux.com.mx

```
# mkdir /var/www/turbolinux.com.mx/html
# mkdir /var/www/turbolinux.com.mx/cgi-bin
# mkdir /var/www/turbolinux.com.mx/icons
# mkdir /var/www/turbolinux.com.mx/error
```

y asi para los siguientes restantes dominios

5.3.3 Paso 3.- Creación y modificación de los ficheros de configuración de los dominios virtuales

Una vez creadas las carpetas de dominios asi como también la estructura de cada uno pasaremos al ultimo paso, crear los ficheros de configuración correspondientes a cada dominio.

Nuevamente por cada dominio se deberá crear un fichero de configuración, dicho fichero sera nombrado de la misma forma que el dominio, solo omitiendo el **"www".**

```
[root@ localhost ~]# mkdir turbolinux.com.mx.conf
[root@ localhost ~]# mkdir comerciolinux.com.conf
[root@ localhost ~]# mkdir escuelalinux.edu.conf
[root@ localhost ~]# mkdir linuxunido.org.conf
[root@ localhost ~]# mkdir linuxbloger.net.conf
```

Estos directorios deberán ser creados dentro de la ruta

```
"/etc/httpd/conf.d/"
```

Al final estos directorios deberán quedar de la siguiente manera

```
/etc/httpd/conf.d/turbolinux.com.mx.conf
/etc/httpd/conf.d/comerciolinux.com.conf
/etc/httpd/conf.d/escuelalinux.edu.conf
/etc/httpd/conf.d/linuxunido.org.conf
/etc/httpd/conf.d/linuxbloger.net.conf
```

Si no están en la ruta antes descrita solo debe moverlos con el comando **"mv"**

Lo siguiente sera crear dentro de cada uno de estos ficheros la estructura básica que deben contener para que puedan ser leídos por el fichero principal de configuración de apache, nos referimos al fichero **"httpd.conf"** . Esta estructura estará conformada por la siguiente configuración básica:

Ejemplo de configuración para el dominio turbolinux.com.mx

```
<VirtualHost *:80>
    ServerAdmin administrador@tuDominio.net
    DocumentRoot "/var/www/turbolinux.com.mx/html"
    ServerName  www. turbolinux.com.mx
    ServerAlias turbolinux.com.mx
</VirtualHost>
```

Los parámetros usados son descritos en la siguiente tabla:

VirtualHost	La función de esta directiva sirve para indicar la dirección IP en la que se esta brindando o bien insertando un asterisco(*) para que esté activa en cualquier interfaz del servidor que es como nosotros lo debemos tener.
ServerAdmin	Esta directiva especifica la persona a la que se le debe notificar los problemas referentes al portal web , esto a través de su cuenta de correo.
DocumentRoot	Esta directiva indica al servidor web la ruta en donde se encuentran almacenados los ficheros web de tu sitio principal
ServerName	Esta directiva especifica el nombre y puerto que el servidor utiliza para identificarse. Con una correcta configuración, este valor se puede determinar automáticamente, pero es recomendable especificarlo explíciatamente para evitar problemas durante el arranque.
ServerAlias	Esta directiva sirve para que el mismo sitio web sea accesible desde distintos nombres de dominio. Ejemplo: turbolinux.com.mx ---> www.turbolinux.com.mx

Índice de contenido

Información de Derechos reservados de esta publicación.

Autor del manual: Javier Eduardo Duarte

Tema 6. Servidor LAMP (Linux+Apache+Mysql+PHP)

6.1 Sobre LAMP

Un servidor LAMP es un conjunto de aplicaciones instaladas en un servidor Linux los cuales, al trabajar en conjunto logran dar vida a una aplicación mucho mas grande y robusta

Generalmente un servidor LAMP esta constituido por los siguientes paquetes:

- **L**inux: El sistema operativo;
- **A**pache. El servidor web;
- **M**ySQL. El gestor de bases de datos;
- **P**erl, PHP, o Python. Lenguajes de programación.

De ahí el nombre de servidor LAMP

Algunas aplicaciones que hacen uso de un servidor LAMP son las siguientes:

- Zimbra.-Servidor de Correo Electrónico
- Openfire.-Servidor de Mensajería Instantánea
- CMS.- Gestores de Contenidos (Joomla,Drupal,Wordpress)

6.2 Proceso de instalación de LAMP

En este capitulo te enseñaremos como se instala y configura un servidor de LAMP mediante la implementacion de un gestor de contenidos que en este caso sera un Joomla.

6.2.1 Instalando el servidor LAMP(Apache+MySQL+PHP)

La instalación de un servidor LAMP requiere de aplicaciones previamente instaladas como es el caso del servidor web apache el cual fue instalado en el capitulo anterior pero de igual manera lo volveremos a nombrar aquí.

Abra una consola y teclee lo siguiente para llevar a cabo la instalación de los paquetes del servidor LAMP

```
[root@ localhost ~]# yum install -y httpd mysql mysql-server php-mysql
php-cli php-common
```

Recuerde que este comando se debe ejecutar como root

Por ultimo solo deberá iniciar (o en su caso reiniciar) servicios como el servidor web apache asi como también el manejador de bases de datos MySQL

```
[root@ localhost ~]# /etc/init.d/httpd start
[root@ localhost ~]# /etc/init.d/mysql start
```

El siguiente punto sera descargar el gestor de contenidos Joomla.

6.3 Descargando Joomla

Descargue Joomla del siguiente portal web:

```
http://www.joomlaspanish.org/
```

Como puede observarse usted puede descargar Joomla de tres formas distintas, la única diferencia radica en la forma en la que esta empaquetado el paquete.

Le recomendamos descargar Joomla a la carpeta de root

```
------>   /root/Joomla_1.5.9-Spanish-pack_completo.tar.gz
```

NOTA: No extraiga o desempaquete el gestor de contenidos, solo descarguelo en la ruta antes mencionada , posteriormente se le indicara donde debe ser extraído el contenido de este paquete

6.4 Configurando dominios virtuales en Apache

Como podrá recordar en el capitulo anterior hablamos extensamente sobre el tema de los dominios virtuales en apache, pero de igual manera volveremos a retomar el tema aquí

La creación de dominios virtuales sobre un servidor web como apache tiene una vital importancia cuando se trata de dar hospedaje a varios sitios web dentro del mismo servidor.

Lograr implementar de manera correcta los dominios virtuales sobre el servidor web apache es tarea sencilla por lo que le recomendamos primero haber leído todas las directivas que pueden ser aplicadas al fichero

```
httpd.conf
```

A partir de este punto comenzaremos a crear los dominios virtuales, es por ello que pedimos tu total concentración y paciencia para que leas poco a poco estos puntos.

6.4.1 Paso 1.- Activando la directiva NameVirtualHost

El primer paso sera abrir el fichero

```
httpd.conf
```

el cual esta almacenado en la ruta:

```
/etc/httpd/conf/
```

En dicho fichero debemos localizar la siguiente linea y descomentarla si es que lo esta

```
NameVirtualHost *:80
```

La función de esta directiva sirve para indicar la dirección IP en la que se esta brindando el servicio o bien insertando un asterisco(*) para que esté activa en cualquier interfaz del servidor que es como nosotros lo debemos tener.

6.4.2 Paso 2.- Estructura de directorios para dominios virtuales

Lo siguiente sera crear la estructura que contendrá cada uno de los dominios virtuales que serán hospedados en nuestro servidor.

Ejemplo: Suponga que tenemos 5 nombres de dominio que serán hospedados en nuestro servidor web

```
www.turbolinux.com.mx
www.comerciolinux.com
www.escuelalinux.edu
www.linuxunido.org
www.linuxbloger.net
```

por cada dominio se deberá crear un directorio, dicho directorio sera nombrado de la misma forma que el dominio, solo omitiendo el **"www".**

```
[root@ localhost ~]# mkdir turbolinux.com.mx
[root@ localhost ~]# mkdir comerciolinux.com
[root@ localhost ~]# mkdir escuelalinux.edu
[root@ localhost ~]# mkdir linuxunido.org
[root@ localhost ~]# mkdir linuxbloger.net
```

Estos directorios deberán ser creados dentro de la ruta

```
"/var/www/"
```

Al final estos directorios deberán quedar de la siguiente manera

```
/var/www/turbolinux.com.mx
/var/www/comerciolinux.com
/var/www/escuelalinux.edu
/var/www/linuxunido.org
/var/www/linuxbloger.net
```

Si no están en la ruta antes descrita solo debe moverlos con el comando **"mv"**

Lo siguiente sera crear dentro de cada uno de estos directorios la estructura básica que debe llevar cada uno de estos dominios. Esta estructura estará conformada por cuatro directorios:

- html
- cgi-bin
- icons
- error

por lo que deberá crear estos cuatro directorios para cada uno de los directorios de dominio.

Ejemplo para el dominio turbolinux.com.mx

```
# mkdir /var/www/turbolinux.com.mx/html
# mkdir /var/www/turbolinux.com.mx/cgi-bin
# mkdir /var/www/turbolinux.com.mx/icons
# mkdir /var/www/turbolinux.com.mx/error
```

y asi para los siguientes restantes dominios

6.4.3 Paso 3.- Creación y modificación de los ficheros de configuración de los dominios virtuales

Una vez creadas las carpetas de dominios asi como también la estructura de cada uno pasaremos al ultimo paso, crear los ficheros de configuración correspondientes a cada dominio.

Nuevamente por cada dominio se deberá crear un fichero de configuración, dicho fichero sera nombrado de la misma forma que el dominio, solo omitiendo el **"www".**

```
[root@ localhost ~]# mkdir turbolinux.com.mx.conf
[root@ localhost ~]# mkdir comerciolinux.com.conf
[root@ localhost ~]# mkdir escuelalinux.edu.conf
[root@ localhost ~]# mkdir linuxunido.org.conf
[root@ localhost ~]# mkdir linuxbloger.net.conf
```

Estos directorios deberán ser creados dentro de la ruta

```
"/etc/httpd/conf.d/"
```

Al final estos directorios deberán quedar de la siguiente manera

```
/etc/httpd/conf.d/turbolinux.com.mx.conf
/etc/httpd/conf.d/comerciolinux.com.conf
/etc/httpd/conf.d/escuelalinux.edu.conf
/etc/httpd/conf.d/linuxunido.org.conf
/etc/httpd/conf.d/linuxbloger.net.conf
```

Si no están en la ruta antes descrita solo debe moverlos con el comando **"mv"**

Lo siguiente sera crear dentro de cada uno de estos ficheros la estructura básica que deben contener para que puedan ser leídos por el fichero principal de configuración de apache, nos referimos al fichero **"httpd.conf"** . Esta estructura estará conformada por la siguiente configuración básica:

Ejemplo para el dominio turbolinux.com.mx

```
<VirtualHost *:80>
    ServerAdmin administrador@tuDominio.net
    DocumentRoot "/var/www/turbolinux.com.mx/html"
    ServerName  www. turbolinux.com.mx
    ServerAlias turbolinux.com.mx
</VirtualHost>
```

Los parámetros usados son descritos en la siguiente tabla:

VirtualHost	La función de esta directiva sirve para indicar la dirección IP en la que se esta brindando o bien insertando un asterisco(*) para que esté activa en cualquier interfaz del servidor que es como nosotros lo debemos tener.
ServerAdmin	Esta directiva especifica la persona a la que se le debe notificar los problemas referentes al portal web , esto a través de su cuenta de correo.
DocumentRoot	Esta directiva indica al servidor web la ruta en donde se encuentran almacenados los ficheros web de tu sitio principal
ServerName	Esta directiva especifica el nombre y puerto que el servidor utiliza para identificarse. Con una correcta configuración, este valor se puede determinar automáticamente, pero es recomendable especificarlo explíciatamente para evitar problemas durante el arranque.
ServerAlias	Esta directiva sirve para que el mismo sitio web sea accesible desde distintos nombres de dominio. Ejemplo: turbolinux.com.mx ---> www.turbolinux.com.mx

6.4.4 Paso 4.- Integrando el gestor de contenidos Joomla a los dominios virtuales

El ultimo paso sera colocar en la carpeta “html” de cada uno de los dominios virtuales el paquete que descargamos del portal “http://www.joomlaspanish.org/” nos referimos al gestor de contenidos Joomla, por lo que solo bastara con copiar y pegar en cada uno de los directorios “html” de cada dominio una copia del mismo.

```
# cp /root/Joomla_1.5.9-Spanish-pack_completo.tar.gz  \
> /var/www/turbolinux.com.mx/html/

# cp /root/Joomla_1.5.9-Spanish-pack_completo.tar.gz  \
> /var/www/comerciolinux.com/html/

# cp /root/Joomla_1.5.9-Spanish-pack_completo.tar.gz  \
> /var/www/escuelalinux.edu/html/

# cp /root/Joomla_1.5.9-Spanish-pack_completo.tar.gz  \
> /var/www/linuxunido.org/html/

# cp /root/Joomla_1.5.9-Spanish-pack_completo.tar.gz  \
> /var/www/linuxbloger.net/html/
```

Lo siguiente sera extraer el contenido del paquete **“Joomla_1.5.9-Spanish-pack_completo.tar.gz”** dentro del directorio “html” de cada uno de los dominios virtuales

```
[root@ localhost ~]# tar -xzvf  Joomla_1.5.9-Spanish-pack_completo.tar.gz
```

Al terminar deberá borrar el paquete **“Joomla_1.5.9-Spanish-pack_completo.tar.gz”** de cada uno de los directorios html de cada dominio

El siguiente paso sera configurar el servidor de base de datos MySQL para que funcione en sincronía con Joomla

6.5 Configurando MySQL

6.5.1 Acerca de MySQL

MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones.

Por un lado se ofrece bajo la GNU GPL para cualquier uso compatible con esta licencia, pero las empresas que quieran incorporarlo en productos privativos pueden comprar a la empresa una licencia específica que les permita este uso. Está desarrollado en su mayor parte en ANSI C.

Al contrario que proyectos como Apache, donde el software es desarrollado por una comunidad pública y el copyright del código está en poder del autor individual, MySQL es propiedad y está patrocinado por una empresa privada, que posee el copyright de la mayor parte del código.

Esto es lo que posibilita el esquema de licenciamiento anteriormente mencionado. Además de la venta de licencias privativas, la compañía ofrece soporte y servicios. Para sus operaciones contratan trabajadores alrededor del mundo que colaboran vía Internet. MySQL AB fue fundado por David Axmark, Allan Larsson, y Michael Widenius y desde enero de 2008 es una subsidiaria de Sun Microsystems

6.5.2 Configurando la cuenta de root en el manejador MySQL

Para comenzar a manipular los accesos del usuario root al manejador MySQL primero tendrá que tener levantado a MySQL de lo contrario le arrojara un error en consola cuando intente entrar a MySQL . Si aun no levanta el servicio de MySQL hágalo

```
[root@localhost]# /etc/init.d/mysqld start
```

si lo tiene levantado haga caso omiso de este comentario

Una vez levantado el servidor MySQL deberemos asignar un “**password”** a la cuenta de root , para ello teclearemos en consola lo siguiente:

```
[root@localhost]# mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2 to server version: 5.0.27
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql>    <---[En este punto hemos entrado al modo consola de MySQL]
```

Para asignar un “password” al usuario “root” solo bastara con teclear la siguiente sentencia SQL

```
mysql>SET PASSWORD FOR 'root'@'localhost' = PASSWORD('PASSWORD');
```

Obviamente deberá cambiar la palabra **“PASSWORD”** por la contraseña que desea asignar a root.

Si todo marcho, salga del manejador de datos MySQL y trate de logearse nuevamente a MySQL pero ahora proporcionando la contraseña que acaba de asignar mediante el uso del parámetro -p

```
[root@localhost]# mysql -u root -p
Enter password: xxxxxxxx
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.0.67 Source distribution

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

6.5.3 Integrando MySQL con Joomla

Ahora que tenemos ya instalado tanto al gestor de contenidos Joomla como el manejador de Bases de datos MySQL , solo nos resta integrar estas dos aplicaciones para que operen de manera conjunta.

Para ello tendremos que generar en el manejador MySQL lo siguiente:

Una cuenta para el administrador de Joomla	Esta cuenta de usuario sera la asignada al administrador del gestor de contenidos Joomla
Un password para la cuenta de administrador de Joomla	Sera el password asignado a la cuenta del administrador del gestor de contenidos Joomla
Una base de Datos para el gestor de contenidos Joomla	Base de Datos en la cual serán dados de alta los usuarios de este gestor de contenidos, nos referimos nuevamente a Joomla

Una vez leído lo anterior comenzaremos por crear la base de datos que usara el gestor de contenidos Joomla asi como también el alta de la cuenta de administrador de Joomla y la asignación de un password para el mismo, para ello abriremos una terminal y nos pasaremos al modo consola de MySQL como se muestra a continuación:

```
[root@localhost]# mysql -u root -p
Enter password: ****************
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.0.45 Source distribution

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Una vez dentro creamos la base de datos que usara Joomla.

Para generar la base de datos solo basta teclear lo siguiente:

```
Mysql> CREATE DATABASE joomla;
Query OK, 1 row affected (0.00 sec)

mysql>
```

El siguiente paso es asignarle al administrador de joomla una cuenta dentro de MySQL y luego de ello asignarle a este usuario permisos de lectura, escritura y ejecución sobre la base de datos que antes creamos, esto se consigue de la siguiente manera.

```
mysql> GRANT ALL ON joomla.* TO 'adminjoomla'@'localhost' IDENTIFIED BY
'PASSWORD' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
mysql>
```

Obviamente deberá cambiar la palabra **"PASSWORD"** por la contraseña que desea asignar al usuario adminjoomla.

Al terminar teclee la palabra **"exit"** para salir de MySQL.

```
mysql>exit
Bye
```

Por ultimo,solo tendrá que reiniciar el servidor de bases de datos MySQL asi como también el de apache

```
[root@ localhost ~]# /etc/init.d/httpd restart
[root@ localhost ~]# /etc/init.d/mysql restart
```

Solo para recordar lo antes visto te posteo una tabla de bastante utilidad

Nombre de la cuenta del adminsitrador de Joomla	**adminjoomla**
Contraseña asignada a "adminjoomla"	**Recuerde que esta contraseña la asigna usted**
Nombre de la base de datos asignada a Joomla	**joomla**

NOTA: Si usted olvido la contraseña que asigno para el administrador de Joomla no se preocupe, el fichero

```
.mysql_history
```

Guarda el histórico de las acciones que se llevaron a cabo en el servidor de base de datos de MySQL por lo que podrá consultarlo para obtener la contraseña si es que la olvido. Generalmente este fichero se encuentra depositado en el directorio de trabajo de root

6.6 Instalación de Joomla

Al llegar a este punto usted deberá contar con su servidor web configurado para dominios virtuales y dentro de cada dominio virtual tener depositado el contenido del paquete de Joomla, asi mismo también debe contar con la base de datos de Joomla activas.

Una vez confirmada esta información podemos continuar con la ultima parte de este capitulo, nos referimos a la instalación del gestor de contenidos Joomla

6.6.1 Sobre Joomla

Joomla es un sistema de administración de contenidos de código abierto construido con PHP bajo una licencia GPL. Este administrador de contenidos se usa para publicar portales web en Internet mediante la implementacion de un servidor LAMP. En Joomla se incluyen características como:

- Indexamiento web
- Feed RSS
- Versiones imprimibles de páginas
- Flash con noticias
- Blogs
- Foros
- Encuestas
- Calendario
- Búsqueda en el sitio web

6.6.2 Instalando Joomla

El proceso para llevar a cabo la instalación de Joomla sera el siguiente:

Abra un navegador web, de preferencia que sea Morilla Firmale y en la barra de direcciones teclee el nombre de alguno de los sitios web virtuales que configuramos en el servidor de apache, nosotros elegimos acceder al portal web

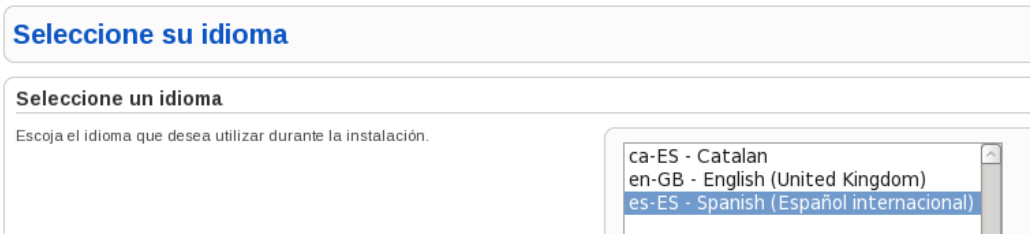
```
www.turbolinux.com.mx
```

Usted puede acceder a cualquiera de los otros cuatro que se crearon.

Una vez dentro del portal web podremos visualizar el Instalador de Joomla el cual consta de 7 pasos para su instalación Estos pasos son:

6.6.2.1 Paso 1) Seleccionando el idioma para la instalación

Este paso es relativamente sencillo, solo debemos elegir el idioma en el cual queremos que se instale Joomla, es este caso nuestra elección sera **es-ES-Spanish (Español Internacional)** y dar clic Siguiente.

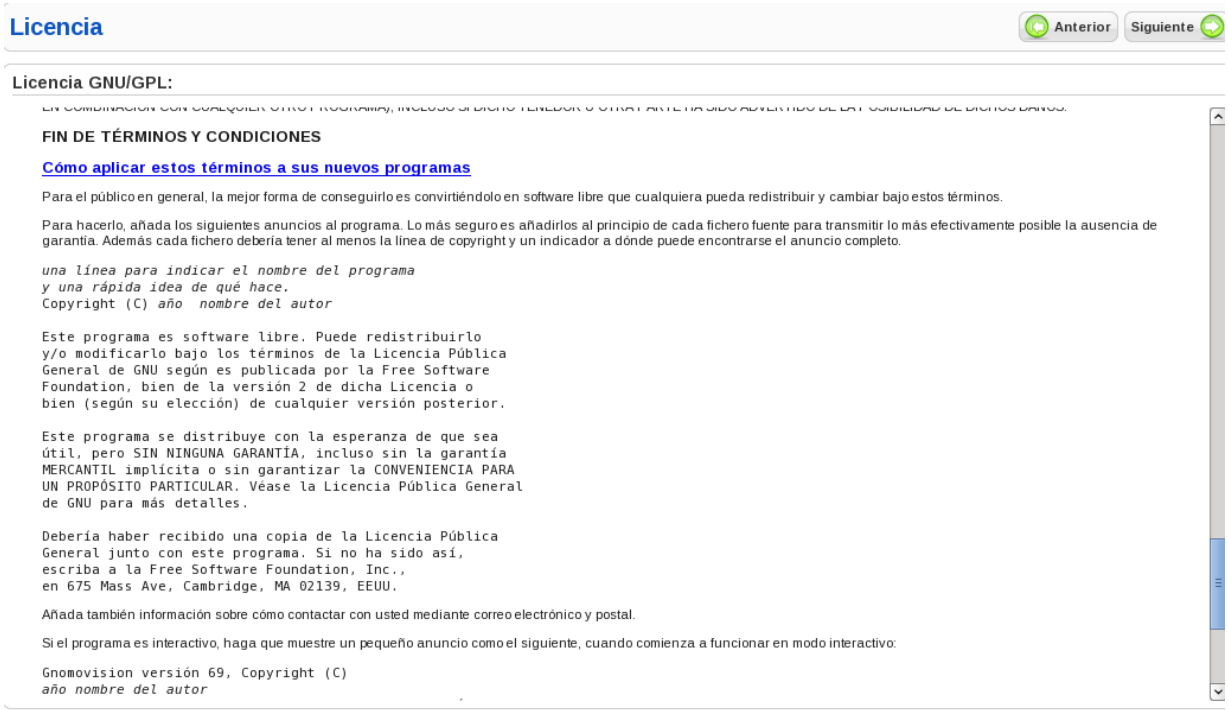


6.6.2.2 Paso 2) Comprobación de paquetes para Joomla

El paso 2 se encarga de verificar que las bases da datos creadas para Joomla asi como algunas características mas estén activas y en perfecto funcionamiento, aquí solo deberemos dar clic en siguiente.

6.6.2.3 Paso 3) Licencia GNU/GPL

Aquí solo habrá que aceptar la licencia bajo la cual se distribuye Joomla y dar nuevamente clic en siguiente.



6.6.2.4 Paso 4) Configurando MySQL con Joomla

En este paso tendremos que introducir los siguientes datos:

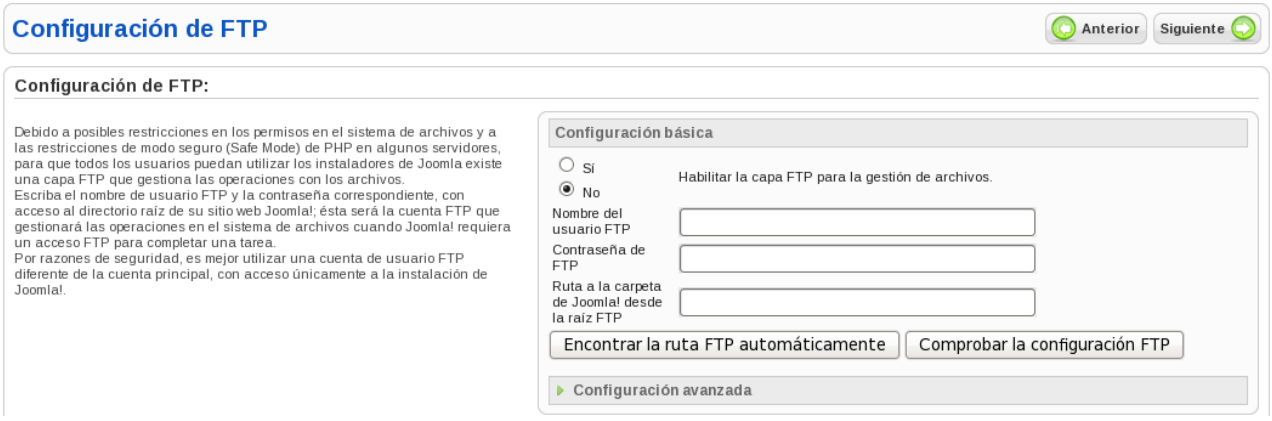
```
Tipo de base de datos----> mysql
Nombre Del Servidor ---->localhost
Nombre Del Usuario ----> adminjoomla (Este usuario lo creo usted)
Contraseña ------>esta contraseña la asigno usted
Nombre de la base de datos  ---> joomla (Esta base de datos usted la creo)
```

Al final su configuración tendrá que verse de la siguiente manera:

Daremos clic en siguiente y si todo marcha bien nos direccionara a otra pagina.

6.6.2.5 Paso 5) Configurando el FTP

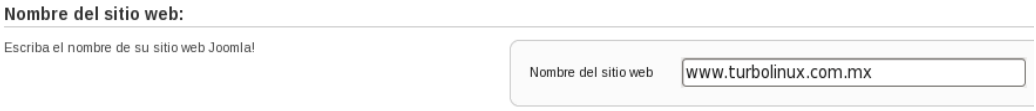
Este paso es irrelevante para este capitulo por lo que daremos clic nuevamente en siguiente:



6.6.2.6 Paso 6) Configuración Principal de Joomla

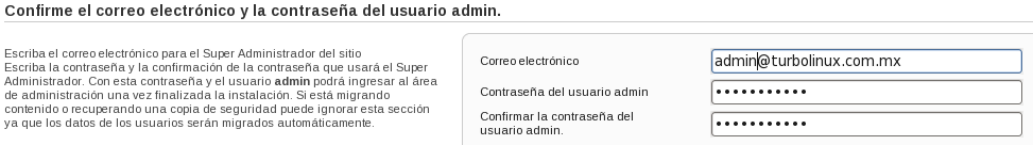
Este paso es el mas importante de todos, aquí usted tedra que llenar algunos campos relevantes para la configuración de Joomla. La primera sección consta de lo siguiente:

Nombre del Sitio Web: En este campo usted tendrá que teclear el nombre del portal web, en este caso nosotros pondremos "www.turbolinux.com.mx**"**



Confirmación **del correo electrónico y contraseña del usuario admin: Aquí** usted tendrá que llenar los campos referentes al correo electrónico de la persona que sera el administrador de este portal web asi como también la asignación de una contraseña para el mismo.

Con esta contraseña y el usuario **admin** podrá ingresar al área de administración una vez finalizada la instalación.



Subir datos de ejemplo, restaurar o migrar contenido de respaldo: Se recomienda a los principiantes que instalen el contenido de ejemplo en español o en su idioma. Para esto es necesario seleccionar esa opción y hacer clic sobre el botón **"Instalar los datos de ejemplo predefinidos"** y luego de ello hacer clic en siguiente.

6.6.2.7 Paso 7) Finalizando la instalación de Joomla

Para finalizar la instalación debe eliminar completamente el directorio de instalación de Joomla ya que por motivos de seguridad no podrá avanzar más allá de esa pantalla hasta que el directorio **"installation"** sea removido completamente. Esta es una característica de seguridad de Joomla.

La ruta del directorio "installation" la podemos ubicar en:

```
/var/www/turbolinux.com.mx/html/   ----->   installation
```

el mismo procedimiento tendrá que ser ejecutado para los demás dominios en los que instalemos Joomla.

Una vez borrado el directorio podremos dar clic en el botón "Portada", el cual nos direccionara a la pagina principal de **"turbolinux.com.mx"**

6.6.2.8 Accediendo a la consola de administración de Joomla

Para acceder a la consola de administración de joomla solo basta teclear la siguiente ruta en nuestro navegador web.

```
Www.turbolinux.com.mx/administrator
```

Nos deberá mostrar algo parecido a esto

En ella tendremos que teclear el nombre de usuario del administrador de Joomla asi como la contraseña que asignamos en el paso 6

Nombre de Usuario---> admin (Este login esta predefinido por Joomla)

Contraseña ---> Esta contraseña fue creada por usted

Al haber pasado la autenticacion nos direccionara a la siguiente pantalla

En esta consola podrá modificar los atributos visuales y de administración de su portal web.

6.6.2.9 Accediendo a nuestro portal web

Para acceder a la pagina principal de nuestro portal web solo habrá que teclear en la barra de direcciones de cualquier navegador web (preferenteme firefox) el nombre de nuestro portal web, en este caso

www.turbolinux.com.mx

el cual deberá lucir asi

Índice de contenido

Información de Derechos reservados de esta publicación.

Autor del manual: Javier Eduardo Duarte

Tema 7. Servidor de Mensajeria Instantanea Openfire

7.1 Introducción

Jabber es un protocolo libre para mensajería instantánea, basado en el estándar XML y gestionado por XMPP Standards Foundation.

La red de Jabber está formada por miles de grandes y pequeños servidores en todo el mundo, interconectados por Internet. Habitualmente la red es utilizada por alrededor de un millón de personas.

Es el proyecto más aceptado como la alternativa libre al sistema MSN Messenger de Microsoft, al AOL o al Yahoo Messenger. Aunque es un protocolo bastante minoritario, está creciendo más cada día, gracias a los usuarios y a Google , que ha creado un cliente de mensajería instantánea que utiliza basado en Jabber nos referimos al Google Talk.

7.1.1 Caracteristicas

Protocolo abierto: Con todas las ventajas del software libre, se puede programar un servidor o un cliente o ver el código, entre otras cosas.

Descentralizado: Se puede crear un servidor para Jabber, y se puede interoperar o unirse al resto de la red Jabber.

Extensible: Se puede ampliar con mejoras sobre el protocolo original. Las extensiones comunes son manejadas por la XMPP Standards Foundation.

Seguro: Cualquier servidor Jabber está aislado del exterior. El servidor de referencia permite SSL para comunicaciones cliente-servidor y algunos clientes aceptan GPG como cifrado de las comunicaciones usando cifrado asimétrico. En desarrollo uso de claves de sesión y SASL.

Multiredes: Un transporte o pasarela permite comunicarse con otros protocolos usados por clientes como MSN Messenger, ICQ, AOL o Yahoo!.

Salas de conversación: Conocido como Multi-User Chat. Es una de las extensiones que han sido añadidas a la mensajería Jabber, la cual le permite la creación de grupos de debate como en las redes IRC, con la posibilidad de poseer usuarios con distintos privilegios (moderadores, participantes e invitados), iniciar conversaciones privadas y transferir archivos.

Existen miles de servidores Jabber en Internet y se estima que al menos un millón de personas usa el servicio regularmente (datos de la XMPP Standards Foundation en 2004). Sin embargo, no es tan conocido como otros sistemas propietarios más extendidos.

7.2 Sobre Openfire

Openfire (antes llamado Servidor Wildfire) es un servidor Jabber/XMPP escrito en Java provee licencias comerciales y GNU.

La administración del servidor se hace a través de una interfaz web, que corre por defecto en el puerto 9090 (HTTP) y 9091 (HTTPS). Los administradores pueden conectarse desde cualquier lugar y editar la configuración del servidor, agregar y borrar usuarios, crear cuartos de conferencia permanentes, etc.

7.2.1 Caracteristicas

Openfire implementa las siguientes características:

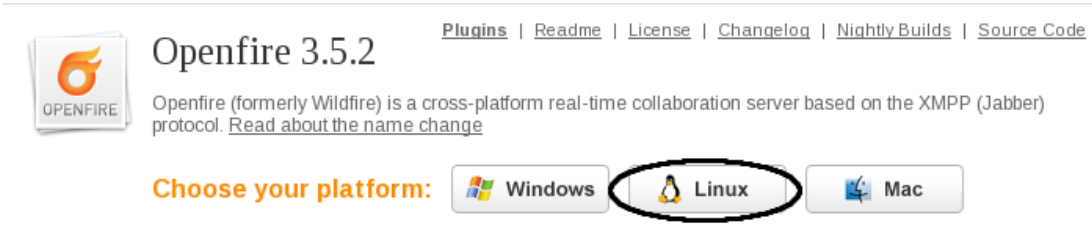
- Panel de administración web
- Interfaz para agregar plugins
- SSL/TLS
- Amigable
- Adaptable según las necesidades
- Conferencias
- Interacción con MSN, Google Talk, Yahoo messenger, AIM, ICQ
- Estadísticas del Servidor, mensajes, paquetes, etc.
- Cluster con multiples servidores
- Transferencia de Archivos
- Compresión de datos
- Tarjetas personales con Avatar
- Mensajes offline
- Favoritos
- Autenticación vía Certificados, Kerbeos, LDAP, PAM y Radius
- Almacenamiento en Active Directory, LDAP, MS SQL, MySQL, Oracle y PostgreSQL
- SASL: ANONYMOUS, DIGEST-MD5 y Plain

7.3 Instalación de Openfire

El primer paso para la implementacion de un servidor Jabber sera descargar el paquete que contiene dicha aplicación, para ello tendremos que dirigirnos al siguiente portal web.

http://www.igniterealtime.org/projects/openfire/index.jsp

Una vez dentro, nos pedirá que seleccionemos la plataforma bajo la cual se desea instalar Openfire, daremos clic en el botón **"Linux"**



Posteriormente nos desplegara un menú que nos mostrara cuatro versiones de openfire, en este caso seleccionaremos y descargaremos el paquete que fue diseñado para distribuciones Linux basadas en Redhat.

El siguiente paso sera instalar el paquete, para ello haremos uso del comando **"rpm"**

```
[root@localhost]# rpm -ivh openfire-3.5.2-1.i386.rpm
Preparando...                ########################################### [100%]
   1:openfire                ########################################### [100%]
```

Los parámetros usados durante la instalación de openfire se explican en la siguiente tabla:

rpm	RPM Package Manager (o RPM, originalmente llamado Red Hat Package Manager) es una herramienta de administración de paquetes pensada básicamente para Linux. Es capaz de instalar, actualizar, desinstalar y verificar programas.
i	Parametro de la herramienta RMP, que tiene como funcion, indicar que se trata de una instalacion. Tambien puede usarse como: [root@localhost]# rpm --install parquete.rpm
v	Parametro de la herramienta RMP, que tiene como funcion, indicar el progreso de la instalacion. 'v' puede ser traducido como verbose.
h	Parametro de la herramienta RMP, que tiene como funcion, indicar el progreso de la instalacion en forma de indicador 'h' puede ser traducido como hash. Ejemplo Preparando... ### [100%] 1:openfire ### [100%]

El siguiente paso sera crearle una base de datos a Openfire por lo que haremos uso del servidor LAMP que instalamos en el capitulo anterior.

7.3.1 Integrando MySQL con el servidor Openfire

Ahora que tenemos ya instalado tanto el servidor Openfire como el manejador de Bases de datos MySQL , solo nos resta integrar estas dos aplicaciones para que operen de manera conjunta.

Para ello tendremos que generar en el manejador MySQL lo siguiente:

Una cuenta de usuario	**Esta cuenta de usuario sera la asignada al administrador del servidor de mensajería Openfire**
Un password para la cuenta de usuario	**Sera el password asignado a la cuenta del administrador del servidor de mensajería Openfire**
Una base de Datos	**Base de Datos en la cual serán dados de alta los usuarios de este servidor de mensajería y gestionada por el administrador del servidor Openfire**

Una vez leído lo anterior comenzaremos por dar de alta la cuenta de usuario asi como un password para el mismo, para ello abriremos una terminal y nos pasaremos al modo consola de MySQL como se muestra a continuación:

```
[root@localhost]# mysql -u root -p
Enter password: ****************
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.0.45 Source distribution

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Lo siguiente sera dar de alta la base de datos para el servidor de mensajería openfire

```
Mysql> CREATE DATABASE openfire;
Query OK, 1 row affected (0.00 sec)

mysql>
```

Diríjase al directorio

```
[root@localhost]# cd /opt/openfire/resources/database
```

e importe el fichero .sql a la base de datos que creamos**,** en este caso como nuestro manejador de bases de datos es MySQL seleccionamos el fichero .sql que hace referencia a mysql como se muestra a continuación:

```
[root@localhost]# cat openfire_mysql.sql | mysql -u root -p openfire
Enter password:*******
```

nos pedirá teclear la contraseña de root de MySQL misma que creamos en el capitulo anterior

Lo siguiente sera asignarle al administrador de openfire una cuenta dentro de MySQL y luego de ello asignarle a este usuario permisos de lectura, escritura y ejecución sobre la base de datos que antes creamos, esto se consigue de la siguiente manera.

```
mysql> GRANT ALL ON openfire.* TO 'adminopenfire'@'localhost' IDENTIFIED BY
'PASSWORD' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)
mysql>
```

La palabra **"PASSWORD"** se refiere al password del usuario **"adminopenfire**" el cual sera asignado por usted.

7.4 Activando openfire

Para iniciar el servidor de mensajería Openfire por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/openfire start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el servidor de mensajería Openfire. Estas opciones pueden ser consultadas en la siguiente tabla:

start	**Inicia el servicio**
stop	**Detiene el servicio**
restart	**Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta**
reload	**Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.**
condrestart	**Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.**
status	**Da a conocer el estado en el que se encuentra el servicio**

Como alternativa también podemos ocupar el siguiente comando para iniciar el servidor de mensajería Openfire

```
[root@ localhost ~]# service openfire start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

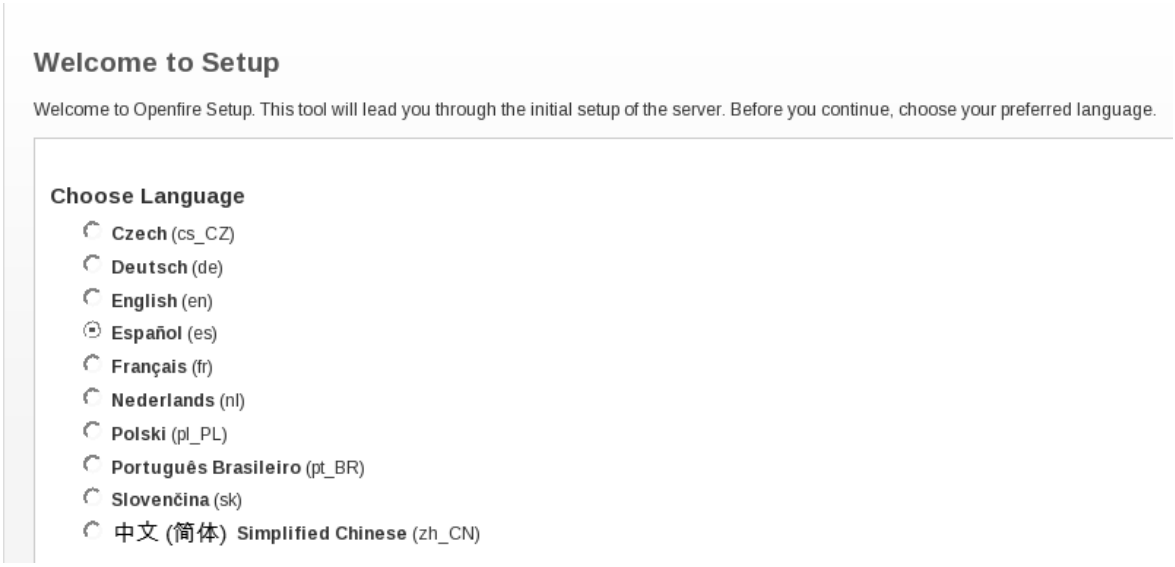
Recuerde que estos comandos se ejecutan como root.

7.5 Completando el proceso de instalación del servidor Openfire

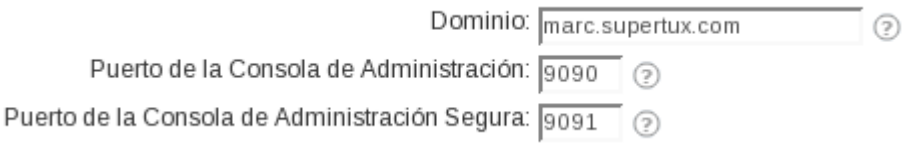
Para completar el proceso de instalación del servidor de mensajería Openfire primero deberán estar levantados los servicios de apache, mysql asi como el openfire, asi que si alguno de estos esta apagado no podrá visualizar la interfaz gráfica del servidor Openfire.

Una vez que nos hemos asegurado que estos servicios están levantados , solo tendremos que abrir un navegador y teclear en la parte superior, la URL de la dirección IP del servidor que tiene instalado el servidor seguido del puerto por el cual recibe peticiones el servidor Openfire somo se muestra a continuación:

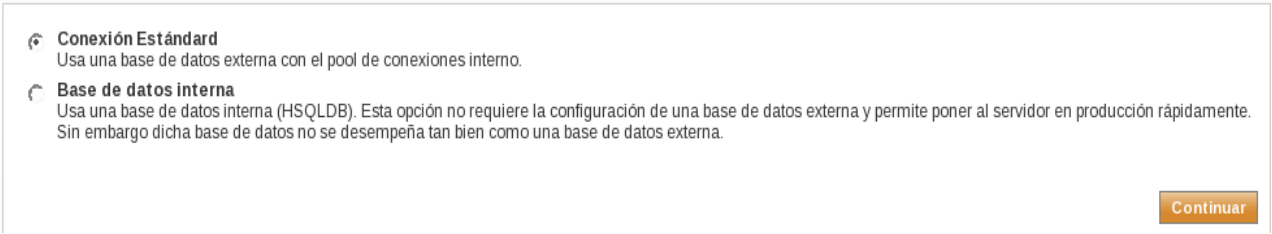
Posteriormente , nos hará elegir el idioma sobre el cual trabajara el servidor, elegimos como idioma **"Español"** y damos clic en **"Continue"**



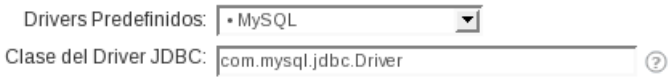
El siguiente paso sera elegir el dominio sobre el cual trabajara el servidor, en este caso nuestro dominio tiene por nombre "**marc.supertux.com",** la elección de los puertos **9090** y **9091** son los puertos por los cuales podremos acceder en futuras sesiones para fines de gestión y administración del servidor, a menos que usted quiera cambiar estos puertos,se recomienda dejarlos como están:



El siguiente paso sera configurar la fuente de datos, de las cuales elegiremos la **"Conexión Estandard**" y luego de ello , dar clic en el botón "**Continuar"**



posteriormente en la sección **"Driver Predefinido"** seleccionaremos el driver de **MySQL** esto es porque nosotros configuramos el servidor con **MySQL,** en caso de haber sido PosgreSQL se tendría que haber elegido el driver de PosgreSQL, el campo "**Clase del Driver JDBC"** sera generado automáticamente después de haber seleccionado el **driver** de **MySQL** como a continuación se muestra:



El siguiente campo

"URL de la Base de Datos"

nos mostrara el siguiente texto:

```
dbc:mysql://[host-name]:3306/[database-name]
```

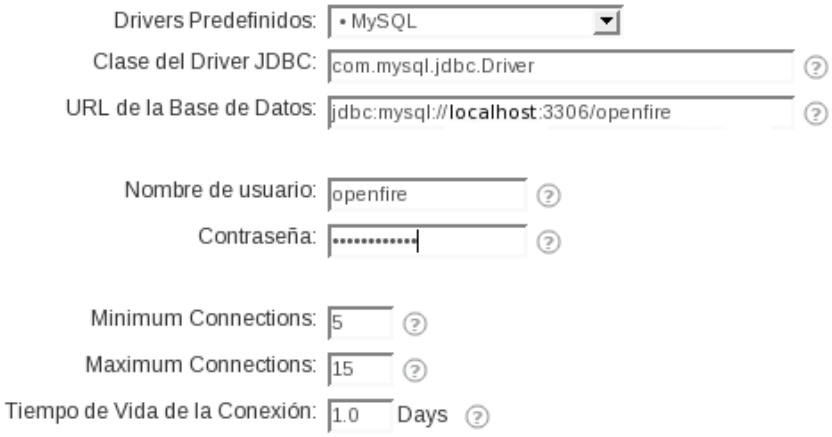
debemos sustituir el **[host-name]** por la palabra **"localhost"**, asi como también agregar el nombre de la base de datos que creamos previamente en el campo **[database-name],**la cual tiene por nombre **openfire.**

Una vez terminado,debiera quedar asi:

```
dbc:mysql://localhost:3306/openfire
```

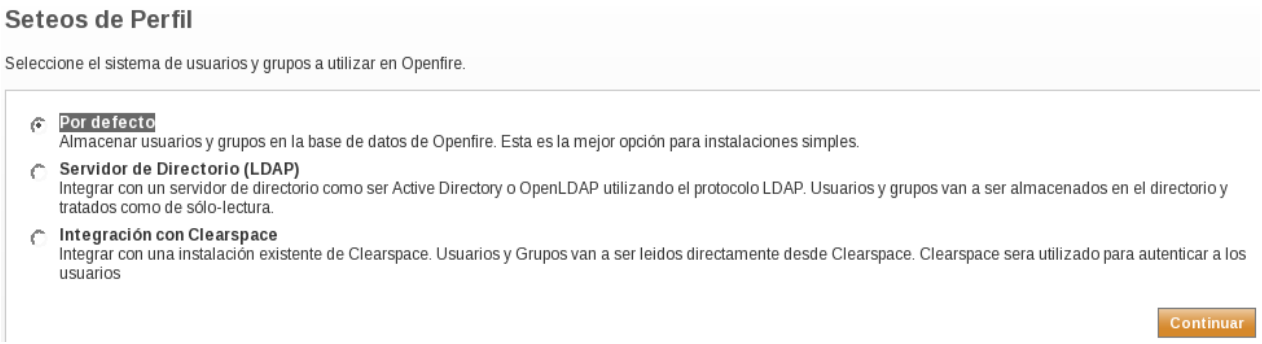
Por ultimo, solo deberá teclear el nombre de usuario y la contraseña de la base de datos generada anteriormente.

El login de usuario es **"root"** e igualmente tendrá que teclear la contraseña que usted le asigno a **"root"**

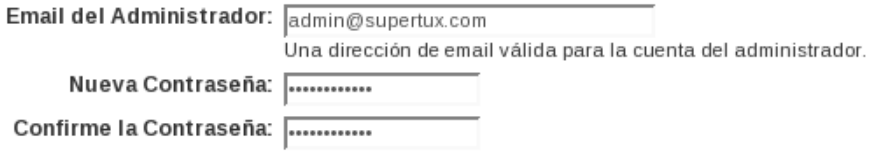


Damos clic en el botón **"Siguiente".**

El siguiente paso sera elegir en la sección **"Seteos de Perfil"** la opción **"Por defecto" y** posteriormente dar clic en siguiente:



Por ultimo, solo tenemos que brindar una cuenta de correo electrónico de quien administrara el servidor de mensajería Openfire.



Una vez confirmado, nos redireccionara a la consola de administración del servidor de mensajería de Openfire y con ello la instalación habrá concluido.

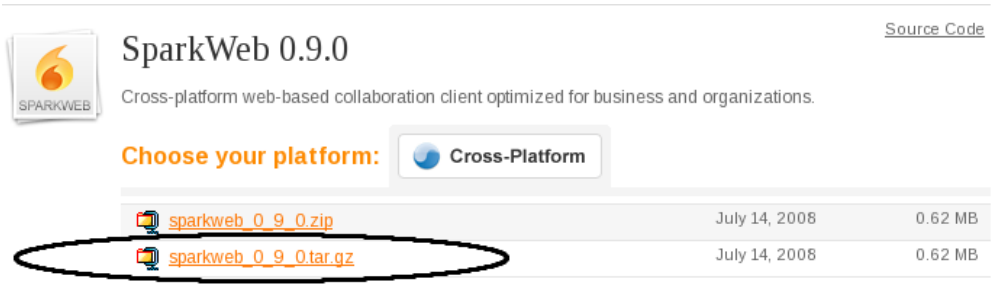
Para logearnos en la consola de administración solo tendremos que teclear la palabra **“”admin”** acompañado del password que usted le asigno.

7.6 Instalación del Cliente Openfire

El primer paso para la implementacion del cliente de mensajería sera descargar el paquete que contiene dicha aplicación, para ello tendremos que dirigirnos al siguiente enlace:

```
http://www.igniterealtime.org/downloads/index.jsp
```

Y descargar el paquete nombrado **"SparkWeb"** , del cual descargaremos la version con extensión **.tar.gz**.



Al finalizar la descarga extraiga el contenido del mismo en alguno de los 5 dominios virtuales que tenemos configurados, por ejemplo al de turbolinux

```
[root@localhost]# tar  -xzvf sparkweb_0_9_0.tar.gz -C
/var/www/turbolinux.com.mx/html/
```

la sentencia "**-C /var/www/turbolinux.com.mx/html/"** indica que el contenido del paquete sera extraído en la ruta antes mencionada.

7.7. Configuración del Cliente de Mensajeria SparkWeb

Posteriormente a la instalación de SparkWeb, crearemos un Alias en el servidor web, por lo que teclearemos el siguiente comando para crear el fichero

```
[root@localhost]# vim /etc/httpd/conf.d/chat.conf
```

El contenido de dicho fichero deberá contener lo siguiente:

```
Alias   /chat     /var/www/turbolinux.com.mx/html/sparkweb
```

Luego de ello,solo bastara guardar los cambios.

Por ultimo, solo nos bastara hacer una modificación al contenido de la carpeta **sparkweb,** para ello tendremos que ir a la ruta

```
[root@localhost]# cd  /var/www/turbolinux.com.mx/html/sparkweb/
```

Una vez dentro, tendremos que ubicar el fichero llamado **"SparkWeb.html"** al cual renombraremos de la siguiente manera:

```
[root@localhost]# mv SparkWeb.html index.html
```

El siguiente paso es editar el fichero **index.html.** En el tendremos que ubicar las lineas "**igniterealtime.org"** y **"socket" y** "**port 5220**"

```
return {
                server: "igniterealtime.org",
                connectionType: "socket",
                port: "7070",
                autoLogin: "false"
        };
```

y sustituirla por el nombre de nuestro dominio virtual, asi como también el tipo de conexión y desde luego el puerto 7070 que es por el cual se conectan los clientes web.

```
return {
                server: "turbolinux.com.mx",
                connectionType: "http",
                port: "5222",
                autoLogin: "false"
        };
```

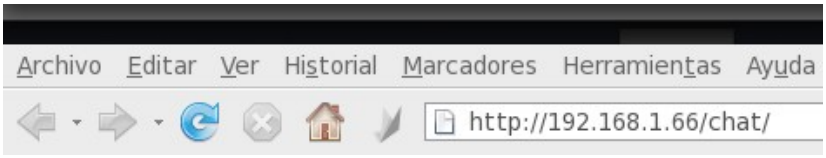
Por ultimo, solo tenemos que iniciar el servidor web Apache.

Cualquier cambio que se haga al fichero deberá estar acompañado del reinicio del servidor web Apache para que se puedan visualizar los cambios.

```
[root@localhost]#  /etc/init.d/httpd restart
```

7.8 Visualizando el Cliente de Mensajeria SparkWeb

Para comenzar a interactuar con el servidor de Mensajeria Openfire, solo bastara abrir un explorador web y teclear en la parte superior, la URL del servidor Openfire, seguido del Alias que le asignamos dentro del fichero /etc/httpd/conf.d/chat.conf.



Acto seguido, nos redireccionara a la siguiente pagina

7.8.1 Dando de alta cuentas en el Servidor de Mensajeria Openfire

Acceda a la consola de administración de **"www.turbolinux.com.mx"** de la siguiente manera

www.turbolinux.com.mx:9090

y ya dentro, diríjase a la sección **"Usuarios/Grupos"**

En esta sección se darán de alta a los usuarios que podrán hacer uso del chat, los cuales serán gestionados por el administrador del servidor.

Como ejemplo daremos de alta a dos usuarios, para ello daremos clic en la sección **"Crear Nuevo Usuario"**

Los usuarios que daremos de alta serán:

Carlos
Angelica

La forma en que se tienen que dar de alta estos usuarios es llenando los campos correspondientes como se muestra a continuación

Después, solo habrá que dar click en el botón **"Crear usuario".**

Para verificar que están dados de alta estos usuarios, solo se tiene que dar click en la sección , en ella se podrán visualizar los dos usuarios creados, mas las cuenta de administrador.

Ahora solo nos basta entrar al cliente de mensajería Spark Web y logearnos para empezar a chatear.

Para comenzar a interactuar con el servidor de Mensajeria Openfire, solo bastara abrir un explorador web y teclear en la parte superior, la URL del servidor Openfire, seguido del Alias que le asignamos dentro del fichero /etc/httpd/conf.d/chat.conf.

Una vez ahí, solo tenemos que teclear el **login** seguido del p**asswd**

Solo bastara buscar a angelica para empezar a chatear con ella

Índice de contenido

Información de Derechos reservados de esta publicación.

Autor del manual: Javier Eduardo Duarte

Tema 8. Servidor DNS

8.1 Acerca de DNS

En la mayoría de las redes modernas, incluyendo la Internet, los usuarios localizan paginas web por su nombre de dominio *(ej. www.google.com)*,esto permite al usuario acceder a las millones de paginas web de la Internet sin necesidad de recordar todas y cada una de las direcciones IP asociadas al nombre de la pagina que desea visitar.

Una forma de solucionar este problema es mediante la complementación de un mecanismo que al momento que un usuario pregunte por el nombre de una pagina web este servidor conozca que dirección IP le corresponde al sitio web por el cual pregunta el usuario. El mecanismo del cual hablamos es un servidor de nombres mayormente conocido como servidor DNS (Domain Name Server)

Así mismo un servidor DNS tiene la función de almacenar la información asociada a los nombres de dominio existentes por los cuales el usuario pregunta, por ejemplo:

- www.linuxparatodos.net
- www.gmail.com
- www.yahoo.com

Por lo tanto el servidor DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. Cuando un equipo cliente solicita información desde un servidor de nombres, usualmente se conecta al puerto 53

Falsamente se asocia a un DNS con una base de datos, cosa que es totalmente falso,pues los principios fundamentales de las bases de datos especifican que no pueden contener datos redundantes es decir, los datos no pueden ser la misma información la cual es almacenada varias veces en la misma base de datos

El mapeo de nombres a direcciones IP es ciertamente la función más conocida de los servidores DNS. Por ejemplo, si la dirección IP del sitio www.linuxparatodos.net es 254.192.169.20, la mayoría de la gente para acceder a ella teclea en un navegador web la dirección web *www.linuxparatodos.net* y no la dirección IP.

La institución encargada de asignar nombres de dominios en Internet es conocida como NIC (acrónimo de Network Information Center o Centro de Información sobre la Red) esta institución es la encargada de asignar los nombres de dominio en Internet, ya sean nombres de dominio genéricos o por países, permitiendo personas o empresas montar sitios de Internet mediante a través de un ISP mediante un DNS. Técnicamente existe un NIC por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país. Por ejemplo: NIC México es la entidad encargada de gestionar todos los dominios con terminación .mx, la cual es la terminación correspondiente asignada a los dominios de México.

FQDN (acrónimo de Fully Qualified Domain Name o Nombre de Dominio Plenamente Calificado) es un Nombre de Dominio ambiguo que especifica la posición absoluta del nodo en el árbol jerárquico del DNS. Se distingue de un nombre regular porque lleva un punto al final.

Ejemplos:
www.hotmail.com
www.google.com

8.2 Componentes de un DNS

Un DNS se compone de tres componentes básicos, los cuales son:

- Cliente DNS
- Servidor DNS
- Zonas de Autoridad

8.2.1 Cliente DNS

Cuando hablamos del cliente DNS nos referimos al host o usuario que hace la petición; o sea, a la computadora del usuario la cual genera la petición al DNS preguntando por el nombre de algún dominio existente en internet.

8.2.2 Servidor DNS

Existen 3 tipos de servidores básicos de un DNS los cuales son:

- Servidor Maestro
- Servidor Esclavo
- Servidor de Cache

8.2.2.1 Servidor Primario o Maestro

Un servidor DNS maestro almacena los registros de las zonas originales y de autoridad. Ademas el servidor DNS maestro es el encargado de responder a las peticiones hechas por otros servidores DNS

8.2.2.2 Servidor Secundario o Esclavo

Un servidor DNS esclavo también tiene la capacidad de responder a las peticiones hechas por un Cliente DNS así como otro servidor de DNS, la diferencia radica en que los servidores esclavos obtienen la información acerca de los nombres de dominio desde los servidores maestros

8.2.2.3 Servidor De Cache

Este ofrece servicios de resolución de nombres como respuesta a las peticiones hechas por los clientes de dns, dichos servicios de resolución de nombres son guardados cierto espacio de tiempo para poder acceder a dicha información mas rápidamente.

Este tipo de servidores no tiene ninguna autoridad sobre las zonas de autoridad.

Los servidores DNS son los encargados de hacer las consultas producto de las peticiones solicitadas por los clientes DNS. Para ello el servidor DNS hace uso de 2 tipos de consultas

- Consultas Iterativas
- Consultas Recursivas

8.2.2.3.1 Consultas Recursiva

Una consulta iterativa funciona de la siguiente manera:

Imagine que tenemos un cliente DNS el cual hace la petición a nuestro servidor dns-1 sobre el dominio ***"***www.ejemplo.com***",*** nuestro servidor dns-1 no sabe quien es ***"***www.ejemplo.com***"*** pero el conoce quien puede tener ese dominio por lo que ahora dns-1 le hace la petición a dns-2, dns-2 le responde a dns-1 que no sabe quien es "www.ejemplo.com" pero el sabe quien puede tener ese dominio registrado, por lo que ahora dns-2 le hace la petición a dns-3, dns-3 responde la petición hecha por dns-2 contestando que el si conoce quien es "www.ejemplo.com" por lo que dns-3 enviá la dirección IP asociada a "www.ejemplo.com" a dns-2, dns-2 le responde la petición a dns1 y dns-1 a su vez le responde a el cliente DNS.

8.2.2.3.2 Consultas Iterativas

Una consulta recursiva funciona de la siguiente manera:

Imagine que tenemos un cliente DNS el cual hace la petición a nuestro servidor dns-1 sobre el dominio “www.ejemplo.com”, nuestro servidor dns-1 no sabe quien es “www.ejemplo.com” pero el conoce quien puede tener ese dominio por lo que dns-1 le responde al Cliente DNS que le pregunte al dns-2, dns-2 no sabe quien es “www.ejemplo.com” pero el conoce quien puede tener ese dominio por lo que dns-2 le responde al Cliente DNS que le pregunte al dns-3, dns-3 sabe quien es “www.ejemplo.com” por lo que dns-3 responde a la petición hecha por el Cliente DNS devolviendo la IP que le corresponde a “www.ejemplo.com” .

8.2.2.3.3 Diferencias entre las Consultas Iterativas contra las Consultas Recursivas

Las diferencias entre las consultas iterativas contras las recursivas son:

- Cuando se hacen consultas iterativas quien asume toda la carga es nuestro cliente DNS (nuestra maquina)
- Cuando se hacen consultas recursivas quien asume toda la carga es el servidor DNS pues el es el encargado de proporcionar una respuesta completa a la petición hecha por el Cliente dns

Conociendo esta información se puede concluir que las consultas recursivas son mejores que las consultas iterativas, debido a que las consultas recursivas liberan a nuestro cliente DNS (nuestra maquina) de la tarea de responder las peticiones solicitadas por el mismo, haciendo que toda la carga la asuma el servidor DNS.

8.2.3 Zonas de Autoridad

Las zonas de autoridad contienen las características sobre las cuales nuestro dominio actuara, en ella se configuran los aspectos importantes así como las opciones especificas de cada zona, estas configuraciones hechas a las zonas son cargadas desde el servidor maestro.

La información de cada Zona de Autoridad es almacenada de forma local en un fichero en el Servidor DNS. Este fichero puede incluir varios tipos de registros como pueden ser:

CNAME	**Canonical Name – (Nombre Canónico) Se usa para crear nombres de hosts adicionales, o alias, para los hosts de un dominio.**
A	**Address – (Dirección) Este registro se usa para traducir nombres de hosts a direcciones IP.**
NS	**Name Server – (Servidor de Nombres) Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.**
MX	**Mail Exchange – (Intercambiador de Correo) Define el lugar donde se aloja el correo que recibe el dominio.**
PTR	**Pointer – (Indicador) También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio.**
SOA	**Start of authority – (Autoridad de la zona) Proporciona información sobre la zona.**

HINFO	Host Information – (Información del sistema informático) Descripción del host, permite que la gente conozca el tipo de máquina y sistema operativo al que corresponde un dominio.
TXT	Text - (Información textual) Permite a los dominios identificarse de modos arbitrarios.
LOC	Localización - Permite indicar las coordenadas del dominio.
WKS	Generalización del registro MX para indicar los servicios que ofrece el dominio. Obsoleto en favor de SRV.
SRV	Servicios - Permite indicar los servicios que ofrece el dominio.

8.3 Sobre BIND (Berkeley Internet Name Server)

BIND es el servidor DNS mas comúnmente implementado en Sistemas Operativos Linux, y actualmente el mas usando en Internet.

Originalmente BIND nació a principios de los años 80 bajo el patrocinio de DARPA (Agencia de Investigación de Proyectos Avanzados de Defensa) agencia del Departamento de Defensa de los Estados Unidos, el cual fue desarrollado en la Universidad de California, Berkeley por cuatro estudiantes. A mediados de los años 80 su desarrollo paso a manos de los empleados de DEC (Digital Equipment Corporation, compañía que mas tarde seria adquirida por Compaq y esta a su vez comprada por HP)

Paul Vixie,empleado de DEC continuó trabajando en BIND luego de desvincularse de DEC. Más adelante ayudaría a fundar la ISC (Internet Systems Consortium), la cual se convirtió en la responsable del mantenimiento de BIND.

El desarrollo de BIND 9 fue realizado con el auspicio conjunto del área comercial y militar. La mayoría de las funcionalidades de BIND 9 fueron impulsadas por proveedores de UNIX quienes querían asegurar que BIND se mantuviera competente con la oferta de Microsoft en el sector de soluciones DNS.

La versión mas actual de BIND, en particular la versión 9.0 fue reescrita desde cero, esto con el fin de reparar algunas de sus funcionalidades arquitectónicas de la misma (problemas en la programación de Bajo Nivel) que agrega características importantes como: TSIG, notificación DNS, nsupdate, IPv6, rndc flush, vistas, procesamiento en paralelo, y una arquitectura mejorada en cuanto a portabilidad.

8.4 Proceso de instalación del servidor DNS

La instalación de un servidor DNS requiere de los siguientes paquetes

```
[BASH]# yum install -y bind bind-chroot bind-libs \
> bind-utils caching-nameserver
```

Recuerde que este comando se debe ejecutar como root

8.4.1 Configuraciones previas que debe tener el servidor DNS

8.4.1.1 Configurando el fichero /etc/hosts

A este fichero deberemos agregar el nombre del equipo que desempeñara la función de servidor DNS asi como la dirección IP asignada a este equipo, al final este fichero deberá verse de una forma similar a esta.

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          localhost.localdomain localhost
192.168.1.10       dns1.tuDominio.com  dns1
::1             localhost6.localdomain6 localhost6
```

Como ejemplo nosotros asignaremos al servidor DNS la dirección IP **192.168.1.10**, usted deberá adecuar esta dirección IP según sea su caso.

8.4.1.2 Configurando el fichero /etc/sysconfig/network

A este fichero deberemos agregar igualmente el nombre del equipo que desempeñara la función de servidor DNS, al final este fichero deberá verse de una forma similar a esta.

```
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=dns1.tuDominio.com
```

8.4.1.3 Configurando el fichero /etc/sysconfig/network-scripts/ifcfg-eth[N]

A este fichero deberemos agregar igualmente el nombre del equipo que desempeñara la función de servidor DNS, al final este fichero deberá verse de una forma similar a esta.

NOTA: La letra [N] indica el numero de la tarjeta de red sobre la cual escucha el DNS

```
# nVidia Corporation MCP61 Ethernet
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:E0:4D:3F:C3:39
ONBOOT=yes
DHCP_HOSTNAME=dns1.tuDominio.com
```

8.4.2 Ficheros de configuración del servidor DNS

La configuración del servidor DNS dependerá en gran medida de los siguientes ficheros.

/var/named/chroot/etc	En esta ruta se deberá crear el fichero "named.conf"
/var/named/chroot/var/named	En esta ruta se crearan los ficheros de zona que serán invocados por named.conf

8.4.2.1 Creación de los ficheros de zona

Procederemos con la creación de nuestras zonas de dominio, para ello teclearemos en terminal lo siguiente:

```
[BASH]# touch /var/named/chroot/var/named/tuDominio.com.zone

[BASH]# touch /var/named/chroot/var/named/1.168.192.in-addr-arpa.zone
```

Lo que hicimos fue crear dos ficheros vacíos a los cuales nombramos

```
tuDominio.com.zone
```

y

```
1.168.192.in-addr-arpa.zone
```

El siguiente paso ahora sera añadir las instrucciones para que puedan ser identificados como ficheros de zona y que a su vez puedan ser invocados por **"named.conf"**

8.4.2.1.1 Editando el fichero "tuDominio.com.zone"

El siguiente paso sera editar el fichero **"tuDominio.com.zone**" al cual deberemos añadir el siguiente contenido.

```
[BASH]# vi /var/named/chroot/var/named/tuDominio.com.zone
------------------------------------------------------------------------
$TTL    86400
@       IN      SOA     dns1.tuDominio.com.com. admin.tuDominio.com. (
                2008061001; Numero de Serie
                28800; Tiempo de Refresco
                7200; Tiempo de Reintentos
                604800; Expiracion
                86400; Tiempo Total de Vida
                )
@       IN      NS      dns1
@       IN      MX      10      correo
@       IN      A       192.168.1.10
dns1    IN      A       192.168.1.10
correo  IN      A       192.168.1.11
```

Los parámetros mas importantes del fichero anterior son descritos en la siguiente tabla

dns1	La palabra dns1 se refiere al nombre del equipo que fungirá como servidor DNS, es este caso hacemos el supuesto que nuestro equipo tiene asignada la dirección IP 192.168.1.10
admin	El nombre admin corresponde al usuario que administrara el servidor DNS.

tuDominio.com	Éste es nuestro dominio referencial con el que estamos trabajando,otros ejemplos de dominio son: *linuxparatodos.net *gmail.com
PUNTO AL FINAL	Recuerde no olvidar poner el punto al final de las sentencias: dns1.tuDominio.com. <---------- root.tuDominio.com. <----------
correo	Estamos haciendo el supuesto que ademas de un DNS contamos con un servidor de correo electrónico al cual hemos asignado la dirección Ip 192.168.1.11
NS (Name Server)	Asigna Nombre al DNS
MX (Mail Exchanger)	Registro de Mail Exchange, el cual indica a dónde debe ser dirigido el correo
A (Address)	Registro de dirección que especifica una dirección IP que se debe asignar a un nombre
SOA (Start of Authority)	Registro de recursos que declara información importante de autoridad relacionada con espacios de nombres al servidor de nombres

8.4.2.1.2 Editando el fichero "1.168.192.in-addr.arpa.zone"

A este fichero deberemos añadir el siguiente contenido.

```
[BASH]# vi /var/named/chroot/var/named/ 1.168.192.in-addr.arpa.zone
-------------------------------------------------------------------------
$TTL    86400
@       IN      SOA     dns1.tuDominio.com. root.tuDominio.com. (
                2008061002; Numero de Serie
                28800; Tiempo de Refresco
                7200; Tiempo de Reintentos
                604800; Expiracion
                86400; Tiempo Total de Vida
                )
@       IN      NS      dns1.tuDominio.com.
10      IN      PTR     dns1.tuDominio.com.
```

El numero **[10]** hace referencia al ultimo octeto de la dirección IP asignada a nuestro DNS, nos referimos a la dirección IP **192.168.1.10.**

Por ejemplo si la dirección IP del servidor DNS fuera la 254.168.1.25, el numero que debiera ir colocado en la parte inferior de su izquierda debiera ser el numero [**25]**

Ejemplo:

```
25      IN      PTR     dns1.tuDominio.com.
```

8.4.2.2 Creación y configuración del fichero “named.conf”

Abra una terminal y genere el fichero **“named.conf”** dentro de la ruta **“/var/named/chroot/etc/”**

```
[BASH]# touch /var/named/chroot/etc/named.conf
```

Una vez creado asegúrese de agregarle los siguientes propietarios

```
[BASH]# chown root:named named.conf
```

Al terminar solo deberá añadir al fichero el siguiente contenido

```
[BASH]# vi named.conf
---------------------------------------------------------------------
options {
       directory "/var/named/";
       dump-file "/var/named/data/cache_dump.db";
       statistics-file "/var/named/data/named_stats.txt";
       allow-recursion {
              127.0.0.1;
              192.168.1.0/24;
       };
       forwarders {
              200.33.146.209;
              200.33.146.217;
       };
       forward first;
};
zone "." {
       type hint;
       file "named.ca";
};
zone "localhost" {
       type master;
       file "localhost.zone";
       allow-update { none; };
};
zone "tuDominio.com" {
       type master;
       file "tuDominio.com.zone";
       allow-update { none; };
};
zone "1.168.192.in-addr.arpa" {
       type master;
       file "1.1.192.in-addr.arpa.zone";
       allow-update { none; };
};
```

Los parámetros mas importantes del fichero anterior son descritos en la siguiente tabla

zone	Define las características de una zona, tal como la ubicación de su archivo de configuración y opciones especificas de la zona.
"tuDominio.com"	Aquí debe ir el nombre de nuestro dominio
file "tuDominio.com.zone";	Contiene los ficheros de configuración de tus zonas de tu dominio.
allow-update{ none; };	Especifica los host que están autorizados para actualizar dinamicamente la información en sus zonas. Por defecto, no se autoriza la actualización dinámica de la información. Esto se logra añadiendo la palabra none.
"1.168.192.in-addr.arpa"	IP de resolución inversa. En este caso estamos usando nuestra IP referencial 192.168.1.10
type master;	Designa el servidor de nombres actual como el servidor autoritario para esa zona
file "1.168.192.in-addr.arpa.zone";	Contiene los ficheros de configuración de tus zonas de tu dominio.

8.5 Iniciar , detener o reiniciar el servidor DNS

Para iniciar el servidor FTP por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/named start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el servidor DNS. Estas opciones pueden ser consultadas en la siguiente tabla:

start	Inicia el servicio
stop	Detiene el servicio
restart	Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta
reload	Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.
condrestart	Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.
status	Da a conocer el estado en el que se encuentra el servicio

Como alternativa también podemos ocupar el siguiente comando para iniciar el servidor FTP

```
[root@ localhost ~]# service named start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root.

Para verificar que bind esta cargando las zonas, deberemos ejecutar el siguiente comando

```
[BASH]#tail -80 /var/log/messages | grep named
```

8.6 Etapa de Pruebas

Compruebe que el dominio resuelve correctamente ejecutando los siguientes comandos:

```
[BASH]# host tuDominio.com 192.168.1.10
[BASH]# dig @192.168.1.10 tuDominio.com
[BASH]# dig @192.168.1.10 tuDominio.com MX
```

Al ejecutar el comando **"dig @192.168.1.10 tuDominio.com MX"** deberíamos observar lo siguiente:

```
[BASH]# dig @192.168.1.10 tuDominio.com MX
; <<>> DiG 9.5.0rc1 <<>> @192.168.1.10 tuDominio MX
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32324
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
; tuDominio.com.           IN      MX

;; ANSWER SECTION:
tuDominio.com.     86400   IN      MX      10 mail. tuDominio.com.

;; AUTHORITY SECTION:
tuDominio.com.     86400   IN      NS      dns1.tuDominio.com.

;; ADDITIONAL SECTION:
tuDominio.com. 86400 IN A      192.168.1.10

;; Query time: 1 msec
;; SERVER: 192.168.1.117#53(192.168.1.10)
;; WHEN: Thu Jun 12 17:39:33 2008
;; MSG SIZE  rcvd: 99
```

8.7 Errores Comunes

No olvide desactivar el Firewall del servidor DNS, de otro modo nuestras peticiones al DNS serán rebotadas

Índice de contenido

Información de Derechos reservados de esta publicación.

Autor del manual: Javier Eduardo Duarte

Tema 9. Servidor de correo Sendmail

factor evolución

9.1 Sobre Sendmail

Las raíces de Sendmail se remontan al nacimiento del correo electrónico, una década antes de que naciese ARPANET, el precursor de Internet. Por entonces, cada buzón de usuario era un fichero con derechos de sólo lectura y las aplicaciones de correo eran simplemente texto incorporado en ese fichero. Cada usuario tenía que abrir y meterse de lleno en el fichero de correo para buscar correos antiguos y leer el correo nuevo era toda una faena. La primera transferencia real de un fichero de mensaje de correo entre dos equipos tuvo lugar hasta el año de 1972, año en el que el correo electrónico empezó a transferirse por FTP a través de un protocolo de red NCP. Este método de comunicación más sencillo muy pronto se hizo popular, incluso hasta el punto de representar la mayor parte del tráfico de ARPANET en menos de un año.

Sin embargo, la falta de estándares entre los protocolos existentes convirtió al correo electrónico en más difícil de enviar desde algunos sistemas y así continuó hasta que ARPANET creó el estándar TCP/IP en 1982. Un nuevo protocolo, SMTP, que se materializaba en el transporte de mensajes. Estos avances, en combinación con la sustitución de los ficheros host por dns, permitieron que se materializasen los agentes MTA con funciones completas. Sendmail, que creció a partir de un precedente sistema de entrega de correo electrónico denominado Delivermail, muy pronto se convirtió en estándar a medida que Internet comenzaba a expandirse y a utilizarse más ampliamente.

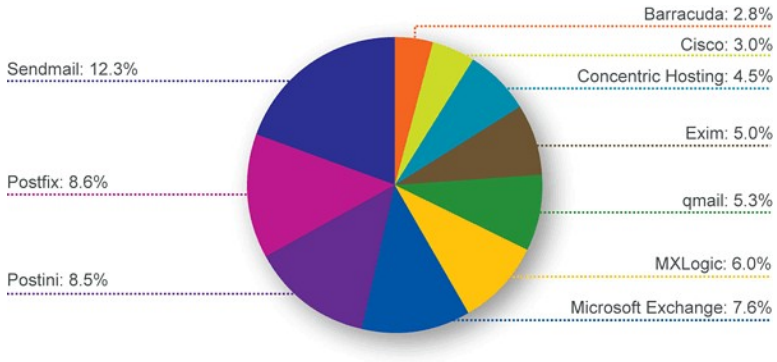
El unico punto debil que preseta sendmail es que este este posee el mayor numero de errores los cuales son reparados casi de inmediato.

9.1.1 Sendmail en la actualidad

Algunos analisis y encuentas nos expresan comentarios muy buenos sobre Sendmail, esto de acuerdo a una encuesta realizada por la editorial O'Reilly, la cual formulo la siguiente pregunta

¿Cuantas empresas tienen implementado como servidor de correo a Sendmail?

Para dicha encuesta se seleccionaron al rededor de 400 000 dominios, de los cuales el 12.3 % de los encuestados respondieron que tenian implementado a Sendmail como servidor de correo, el segundo lugar fue para Postfix con un 8.6 % y en tercer lugar tenemos a Postini con el 8.5%



Esta encuesta la puedes encontrar en la siguiente direccion web

```
http://www.oreillynet.com/lpt/a/6849
```

9.2 Protocolo SMTP

Simple Mail Transfer Protocol (SMTP) Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos

SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres.

Las respuestas del servidor constan de un código numérico de tres digitos, seguido de un texto explicativo. El número va dirigido a un procesado automático de la respuesta por autómata, mientras que el texto permite que un humano interprete la respuesta. En el protocolo SMTP todas las órdenes, réplicas o datos son líneas de texto, delimitadas por el carácter <CRLF>. Todas las réplicas tienen un código numérico al comienzo de la línea.

En el conjunto de protocolos TCP/IP, el SMTP va por encima del TCP, usando normalmente el puerto 25 en el servidor para establecer la conexión.

9.3 Protocolo POP3

POP3 está diseñado para recibir correo, no para enviarlo; le permite a los usuarios con conexiones intermitentes ó muy lentas (tales como las conexiones por módem), descargar su correo electrónico mientras tienen conexión y revisarlo posteriormente incluso estando desconectados. Cabe mencionar que la mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor, de manera tal que, un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta. En contraste, el protocolo IMAP permite los modos de operación conectado y desconectado.

Los clientes de correo electrónico que utilizan IMAP dejan por lo general los mensajes en el servidor hasta que el usuario los elimina directamente. Esto y otros factores hacen que la operación de IMAP permita a múltiples clientes acceder al mismo buzón de correo. La mayoría de los clientes de correo electrónico soportan POP3 ó IMAP; sin embargo, solo unos cuantos proveedores de internet ofrecen IMAP como valor agregado de sus servicios.

9.4 Protocolo IMAP

Internet Message Access Protocol, o su acrónimo IMAP, es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. IMAP tiene varias ventajas sobre POP, que es el otro protocolo empleado para obtener correo desde un servidor. Por ejemplo, es posible especificar en IMAP carpetas del lado servidor. Por otro lado, es más complejo que POP ya que permite visualizar los mensajes de manera remota y no descargando los mensajes como lo hace POP.

9.4.1 Ventajas sobre POP3

Respaldo para los modos de operación conetado y desconectado

Al utilizar POP3, los clientes se conectan brevemente al servidor de correo, solamente el tiempo que les tome descargar los nuevos mensajes. Al utilizar IMAP, los clientes permanecen conectados el tiempo que su interfaz permanezca activa y descargan los mensajes bajo demanda. Esta manera de trabajar de IMAP puede dar tiempos de respuesta más rápidos para usuarios que tienen una gran cantidad de mensajes o mensajes grandes.

Respaldo para que la información de estado del mensaje se mantenga en el servidor

A través de la utilización de señales definidas en el protocolo IMAP4 de los clientes, se puede vigilar el estado del mensaje, por ejemplo, si el mensaje ha sido o no leído, respondido o eliminado. Estas señales se almacenan en el servidor, de manera que varios clientes conectados al mismo correo en diferente tiempo pueden detectar los cambios hechos por otros clientes.

Respaldo para búsquedas de parte del servidor

IMAP4 proporciona un mecanismo para que los clientes pidan al servidor que busque mensajes de acuerdo a una cierta variedad de criterios. Este mecanismo evita que los clientes descarguen todos los mensajes de su buzón de correo, agilizando, de esta manera, las búsquedas.

9.5 Instalación de Sendmail

El proceso de instalacion de Sendmail requiere de los siguientes paquetes

- sendmail
- sendmail.cf
- dovecot
- cyrus
- cyrus-sasl-mmd5
- cyrus-sasl-plain
- make
- m4

9.5.1 Sobre el paquete sendmail y senmail.cf

Este paquete incluye el MUA Sendmail asi como los archivos de configuacion propios de sendmail

9.5 2 Sobre el paquete dovecot

Dovecot es el servidor de IMAP y POP3 de Linux

9.5.3 Sobre el paquete cyrus-sasl

SASL son las siglas de Simple Authentication and Security Layer, método que añade un soporte adicional para la autenticación de los protocolos que fundamentan su conexión en la estandarización fijada por la IETF (Internet Engineering Task Force). Se usa en servidores, como Cyrus IMAP, para controlar las peticiones de acceso de los clientes. El protocolo de autenticación incluirá comandos para la correcta apertura del canal cliente-servidor y las subsiguientes aperturas del canal para la toma de nuevos datos. Opcionalmente, puede negociarse una capa de seguridad entre el protocolo mismo y la conexión. Cyrus SASL utiliza OpenSSL para cifrar los datos.

Para llevar a cabo la instalacion de estos paquetes solo teclee en terminal lo siguiente:

```
[BASH]# yum install -y sendmail sendmail.cf dovecot cyrus-sasl cyrus-sasl-plain cyrus-sasl-md5 make m4
```

9.6 Configuracion Basica de Sendmail

Los ficheros generados a partir de la instalacion del servidor de coreo Sendmail que modificaremos seran los siguientes:

- access
- local-host-names
- **relay-domains ---> (Este fichero sera creado por usted)**
- sendmail.mc

El fichero relay-domains no existe por lo que tendra que ser creado por usted mismo

Estos ficheros los puedes localizar en:

9.6.1 Configuracion del fichero --> /etc/mail/access

En este fichero se definen los dominios o conjunto de direcciones IP que podran hacer uso o no del servidor de correo.

La sintaxis de este fichero es el siguiente

```
Connect:midominio1.net                    [accion]
Connect:midominio2.net                    [accion]
Connect:midominio3.net                    [accion]
Connect:midominio4.net                    [accion]
```

Los valores que puede tomar el parametro **[accion]** son los siguientes:

RELAY	**Permite el envio de correo a travez de nuestro servidor**
REJECT	**Niega el uso de nuestro servidor para la entrega de correo**

Ejemplo:

```
# Check the /usr/share/doc/sendmail/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail/README.cf is part of the sendmail-doc
# package.
#
# If you want to use AuthInfo with "M:PLAIN LOGIN", make sure to have the
# cyrus-sasl-plain package installed.
#
# By default we allow relaying from localhost...
Connect:localhost.localdomain          RELAY
Connect:localhost                      RELAY
Connect:127.0.0.1                       RELAY

#IP Publica de su Servidor de correo
Connect: 207.249.24.30                   RELAY

#Nombre de su Dominio
Connect: midominio.com.mx               RELAY

#Nombre de su Equipo
Connect: correo.midominio.com.mx        RELAY

#IP Local de su Servidor de correo
Connect: 192.168.1.10                    RELAY


#Dominios y direcciones IP a quienes se les negara el envio de correo
Connect:spammers.com.ar                 REJECT
Connect:yourporn.net                    REJECT
Connect:207.46.197.32                    REJECT
Connect:207.46.197.32                    REJECT
```

Como podemos observar, solo permitimos el envio de correo a nuestro propio dominio asi como tambien a la direccion IP publica que tiene asignada nuestro dominio, asi mismo estamos denegando el uso de nuestro servidor de correo a dominios como spammers.com.ar , yourporn.net y a las direcciones IP 207.46.197.32 y 207.46.197.32.

9.6.2 Configuracion del fichero --> /etc/mail/local-host-names

Se suele utilizar para escribir aquellos dominios o equipos de los cuales sendmail va a recibir correo. Por ejemplo, si nuestro servidor de correo va a aceptar correo proveniente del dominio

```
midominio.com.mx
```

y también de la máquina

```
correo.midominio.com.mx
```

nuestro fichero local-host-names debería quedar editado de la siguiente forma

```
correo.midominio.com.mx
midominio.com.mx
```

9.6.3 Configuracion del fichero --> /etc/mail/relay-domains

En este fichero se introduciran los nombres de los equipos, redes o dominios **desde** o **hacia** las que podemos hacer transmisión de correo.

Por ejemplo:

```
midominio.com.mx
correoomidominio.com.mx
```

Como podemos observar estamos permitiendo la transmisión a cualquier correo que **"venga de"** o **"vaya hacia"** el dominio **"midominio.com.mx"** , asi como tambien al dominio **"correo.midominio.com.mx" .**

Practicamente es una copia del fichero /**etc/mail/local-host-names**

9.6.4 Configuracion del fichero --> /etc/mail/sendmail.mc

Este fichero contiene la configuración completa del servidor de correo, es por ello que debe ser cuidadoso al momento de editarlo.

9.6.4.1 Activando interfaces de red

Por defecto sendmail esta configurado para enviar correos desde la interfaz **loopback 127.0.0.1**,esto quiere decir que unicamente el servidor envia correos a si mismo, para cambiar este comportamiento solo deberas ubicar la siguiente linea

```
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
```

y eliminar el parametro

```
Addr=127.0.0.1
```

Al final, la linea debera quedar de la siguiente manera

```
DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl
```

Con esta accion sendmail asumira que podrá enviar correos desde cualquier IP.

Asi mismo tambien podras declar cada una de las direcciones IP por las cuales se podra enviar correo

Ejemplo:

```
DAEMON_OPTIONS(`Port=smtp,Addr=192.168.0.1 Name=MTA')dnl
DAEMON_OPTIONS(`Port=smtp,Addr=172.16.0.10 Name=MTA')dnl
```

9.6.4.2 Filtrado de dominios no validos

Por defecto, Sendmail esta configurado para aceptar correos de dominios no resueltos. Una forma de cambiar este comportamiento es comentando la siguiente linea del fichero /etc/mail/sendmail.mc.

```
FEATURE(`accept_unresolvable_domains')dnl
```

Solo tendra que agregar la palabra

```
dnl
```

al comienzo de la linea

Al finalizar debera quedar de la siguiente forma

```
dnl FEATURE(`accept_unresolvable_domains')dnl
```

Con esta accion usted estara restrigiendo el paso de spam a su servidor de correo

9.6.4.3 Enmascarar dominios

Si tu intencion es enviar correo con solo un dominio lo conveniente es enmascarar todos los correos emitidos desde el servidor con el nombre de tu dominio. Para ello ubica la siguiente linea

```
dnl MASQUERADE_AS(`mydomain.com')dnl
```

descomenta la linea eliminando la palabra

```
dnl
```

que se encuentra al principio de la linea y luego introduce el nombre de tu dominio como se a muestra a continuacion

```
dnl MASQUERADE_AS(`midominio.com.mx')dnl
```

Con esta accion lograras que tus correos salgan con la terminacion

```
@midominio.com.mx
```

Igualmente ubique las siguientes lineas y tambien descomentelas

```
FEATURE(masquerade_envelope)dnl
```

```
FEATURE(masquerade_entire_domain)dnl
```

9.6.4.4 Habilitar el puerto 587 para el envio de correo

Telmex está implementado medidas para ayudar a combatir el spam en sus servicios.

Estó afecta a los usuarios que usan su conectividad, ya que basicamente, están bloqueando el puerto 25 SMTP, el cual comúnmente es utilizado para el envío de correo electrónico.

Si tu cuentas con un servicio Infinitum con IP Dinámica y desea verificar si va a ser afectado por esta medida, le sugerimos realizar lo siguiente:

Revisar la configuración de su cliente de correo para enviar mensajes de forma segura, si confirma que su servicio está siendo bloqueado contacte a su administrador del servicio de correo electrónico sobre las alternativas para enviar correo o bien:

Solicita a TELMEX que elimine la protección del puerto 25 SMTP de su cuenta de acceso a Internet. Una vez que se haya eliminado la protección del puerto 25, por favor desconecte su módem y conéctelo nuevamente. Esta solicitud se puede hacer en línea en:

Asi mismo, recomendamos abrir el puerto alternativo 587 de SMTP para el envio de correo en su servidor.

Para hacerlo, busque la siguiente linea

```
dnl DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
```

descomenta la linea eliminando la palabra

```
dnl
```

que se encuentra al principio de la linea, con eso tendras habilitado el envio por e

```
dnl DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
```

Con esta accion habras habilitado el envio de correo a traves del puerto 587

9.6.4.5 Habilitar la autenticacion de los usuarios de correo

La linea

```
define(`confAUTH_OPTIONS', `A')dnl
```

la cual se encuentra habilitada por defecto permite realizar autenticacion de usuarios por el metodo PLAIN o mediante cifrado.

El metodo PLAIN consiste en autenticacion en texto plano

Dejar esta linea activada presenta cierto riesgo de seguridad ya que todas las contraseñas de los usuarios viajan en texto claro lo cual podria ser aprovechado por algun analizador de protocolos y robar las contraseñas.

Una manera de solucionar este problema seria comentando la anterior linea y en su lugar descomentar la siguiente.

```
define(`confAUTH_OPTIONS', `A p')dnl
```

Esta accion desactiva la autenticación en texto plano y en su lugar activa la autenticacion mediante cifrado, el unico inconveniente es que obligaria a sus clientes o usuarios a utilizar clientes de correo con soporte para autenticacion mediante cifrado

No lo olvide

```
define(`confAUTH_OPTIONS', `A')dnl
```

Autenticacion por metodo PLAIN o mediante Cifrado

```
define(`confAUTH_OPTIONS', `A p')dnl
```

Autenticacion unicamente por el metodo de cifrado

Adicionalmente ubique las siguientes lineas y tambien descomentelas

```
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN
PLAIN')dnl
```

9.7 Configuracion del servidor dovecot

Por defecto,el servidor dovecot tiene deshabilitados los protocolos pop e imap lo cuales son necesarios para la entrega de correo, la forma de habilitar estos protocolos es de la siguiente manera.

Edite el siguiente fichero con la ayuda de cualquier editor de textos

```
/etc/dovecot.conf
```

Ubique la siguiente linea

```
#protocols = imap imaps pop3 pop3s
```

Y solo borre las siguientes palabras asi como tambien la almohadilla de **“#”**

```
imaps pop3s
```

Al final debera lucir de la siguiente manera:

```
protocols = imap pop3
```

Guarde los cambios y salga de la terminal

9.8 Configuracion Avanzada de Sendmail

9.8.1 Limitando el numero de destinatarios de correo

La manera de establecer un numero maximo de destinatarios para un mensaje de correo electronico se hace agregando la siguiente linea

```
define(`confMAX_RCPTS_PER_MESSAGE', `10')dnl
```

justo debajo de la linea

```
dnl define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn,restrictqrun')dnl
```

El numero 10 hace referencia al numero maximo de destinarios para un mensaje de coreo, tu puedes modificar este valor segun tu conveniencia

Al finalizar debera lucir de la sigueinte manera

```
dnl define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn,restrictqrun')dnl
define(`confMAX_RCPTS_PER_MESSAGE', `10')dnl
```

9.8.2 Limitando el tamaño de la cabecera de un correo

La manera de establecer un tamaño maximo de cabecera para un mensaje de correo electronico se hace agregando la siguiente linea

```
define(`confMAX_HEADERS_LENGTH', `10240')dnl
```

justo debajo de la linea

```
define(`confMAX_RCPTS_PER_MESSAGE', `10')dnl
```

El numero 10240 es equivalente a 10Kb (Kilobytes),tu puedes modificar este valor segun tu conveniencia

Al finalizar debera lucir de la sigueinte manera

```
define(`confMAX_RCPTS_PER_MESSAGE', `10')dnl
define(`confMAX_HEADERS_LENGTH', `10240')dnl
```

9.8.3 Limitando el tamaño para un mensaje de correo

La manera de establecer un tamaño maximo para un mensaje de correo electronico se hace agregando la siguiente linea

```
define(`confMAX_MESSAGE_SIZE', `3075000')dnl
```

justo debajo de la linea

```
define(`confMAX_HEADERS_LENGTH', `10240')dnl
```

El numero 3075000 es equivalente a 3Mb (Megabytes),tu puedes modificar este valor segun tu conveniencia

Al finalizar debera lucir de la sigueinte manera

```
define(`confMAX_HEADERS_LENGTH', `10240')dnl
define(`confMAX_MESSAGE_SIZE', `3075000')dnl
```

9.8.4 Limitando el numero de procesos hijos en el servidor de correo

La forma de limitar el numero de procesos hijos que se permitirán simultáneamente en el servidor de correo sera de la siguiente manera:

Agrege la siguiente linea

```
define(`confMAX_DAEMON_CHILDREN', `5')dnl
```

justo debajo de la linea

```
define(`confMAX_MESSAGE_SIZE', `3075000')dnl
```

Al finalizar debera lucir de la sigueinte manera

```
define(`confMAX_MESSAGE_SIZE', `3075000')dnl
define(`confMAX_DAEMON_CHILDREN', `5')dnl
```

9.8.5 Limitando el numero de conexiones

La forma de limitar el numero de conexiones por segundo que se permitirán en el servidor de correo sera de la siguiente manera:

Agrege la siguiente linea

```
define(`confCONNECTION_RATE_THROTTLE', `4')dnl
```

justo debajo de la linea

```
define(`confMAX_DAEMON_CHILDREN', `5')dnl
```

Al finalizar debera lucir de la sigueinte manera

```
define(`confMAX_DAEMON_CHILDREN', `5')dnl
define(`confCONNECTION_RATE_THROTTLE', `4')dnl
```

9.9 Alta de cuentas de correo

La forma en que dara de alta cuentas de correo para sus usuarios sera de la siguiente manera

```
[BASH]# useradd -s /sbin/nologin  nombreDelsuario
```

9.10 Asignando contraseñas a las cuentas de correo

La forma en que asignara contraseñas a las cuentas de correo sera a travez de dos fases.

La primera aplicando el siguiente comando

```
[BASH]# passswd  nombreDelsuario
```

y la segunda aplicando este otro

```
[BASH]# saslpasswd2 nombreDelsuario
```

9.11 Iniciar , detener o reiniciar el servidor de Correo

Para iniciar el servidor de correo por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/sendmail start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el servidor de correo. Estas opciones pueden ser consultadas en la siguiente tabla:

start	Inicia el servicio
stop	Detiene el servicio
restart	Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta
reload	Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.
condrestart	Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.
status	Da a conocer el estado en el que se encuentra el servicio

Como alternativa también podemos ocupar el siguiente comando para iniciar el servidor de correo

```
[root@ localhost ~]# service sendmail start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root.

9.12 Iniciar , detener o reiniciar el servidor Dovecot

Para iniciar el servidor de correo por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/dovecot start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el servidor dovecot. Estas opciones pueden ser consultadas en la siguiente tabla:

start	**Inicia el servicio**
stop	**Detiene el servicio**
restart	**Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta**
reload	**Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.**
condrestart	**Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.**
status	**Da a conocer el estado en el que se encuentra el servicio**

Como alternativa también podemos ocupar el siguiente comando para iniciar el servidor de correo

```
[root@ localhost ~]# service dovecot start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root.

9.13 Iniciar , detener o reiniciar el servicio de autenticacion

Para iniciar el servidor de correo por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/saslauthd start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el servicio de autenticacion saslauthd. Estas opciones pueden ser consultadas en la siguiente tabla:

start	**Inicia el servicio**
stop	**Detiene el servicio**
restart	**Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta**
reload	**Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.**
condrestart	**Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.**
status	**Da a conocer el estado en el que se encuentra el servicio**

Como alternativa también podemos ocupar el siguiente comando para iniciar el servidor de correo

```
[root@ localhost ~]# service saslauthd start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root

Índice de contenido

Información de Derechos reservados de esta publicación.

Tema 11. Instalacion de Antivirus ClamAV

11.1 Sobre ClamAV

El proyecto ClamAv Antivirus fue fundado en el año 2001 por Tomasz Kojm. Actualmente tiene una implementacion superior a los 500 000 servidores en todo el mundo. Asi mismo ClamAV nació como un proyecto Open Source que pretende identificar y bloquear virus en el sistema. El primer objetivo de ClamAv fue combatir el Spam. Como consecuencia de ello ClamAv se está usando en un número elevado de servidores de correo.

Gracias a la colaboración de varias compañías, universidades y otras organizaciones ha posibilitado al proyecto ClamAV poseer una red extensa de distribución rápida y fiable en todo el mundo.

Algunas de las caracteristicas de ClamAV son las siguientes:

- Licenciado bajo GNU General Public License 2
- Detecta alrededor de 320.000 virus, gusanos, troyanos, incluyendo virus programados como macros de Microsoft Office.
- Escaneo de archivos y ficheros comprimidos:
    - ZIP
    - RAR
    - ARJ
    - TAR
    - Gzip
    - Bzip2
    - MS OLE2
    - MS Cabinet File
    - MS CHM
    - MS SZDD
    - BinHex
    - SIS
    - AutoIt
- Soporta formatos especiales como:
    - HTML
    - RTF
    - PDF
    - CryptFF
    - SCREnc
    - uuencode
    - TNEF

11.2 Instalacion ClamAV

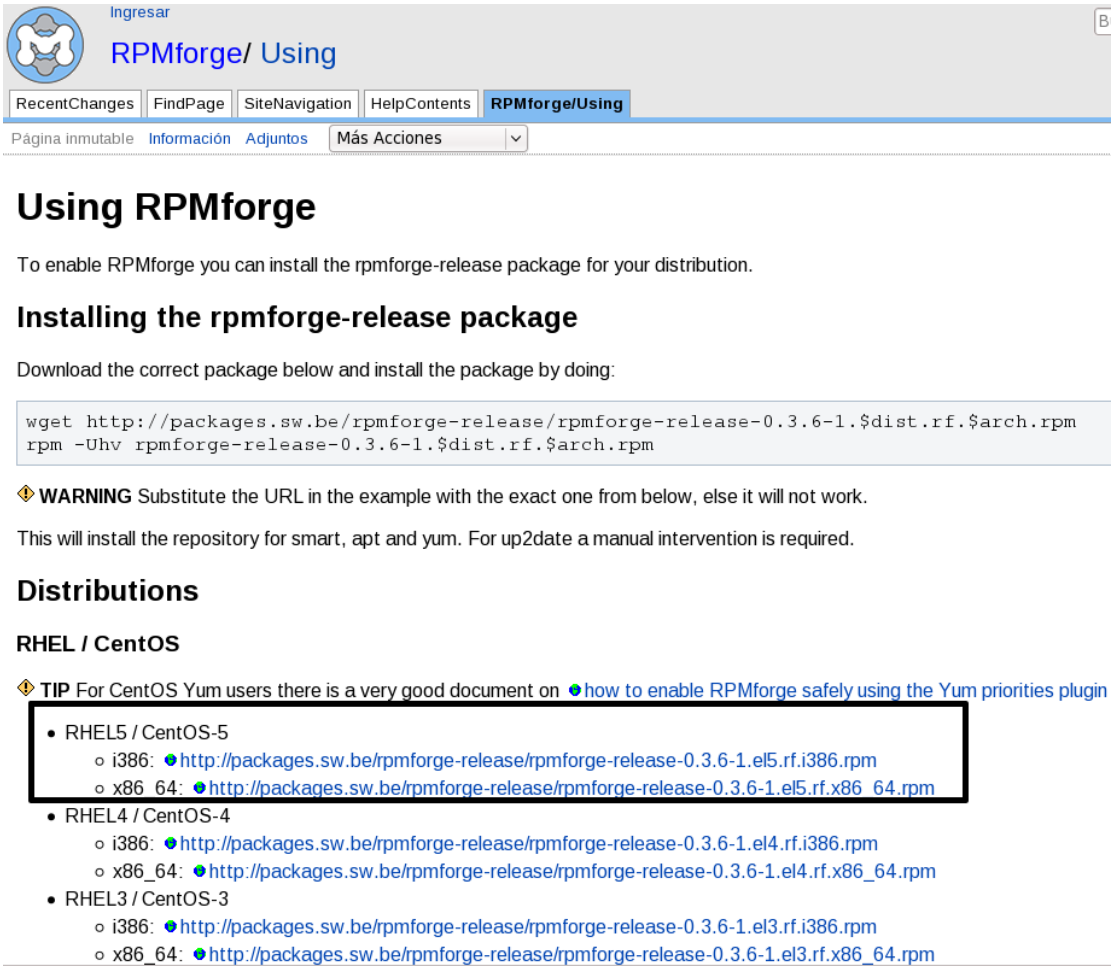
Para poder llevar a cabo la instalacion de ClamAV se deben agregar los repositorios de rpmforge, ya que ClamAV no esta contenido en los repositorios originales de Centos

Los repositorios RMPforge se agregaran de la siguiente manera.

Acceda al portal web de RMPforge -->

```
https://rpmrepo.org/RPMforge/Using
```

La pagina debe lucir muy parecida a esta



Descarge el paquete enmarcado en el recuadro negro, en particular la version para 32 bits (i386).

La razon del porque descargamos este paquete y no los demas es porque nosotros tenemos instalada la version de Centos 5.3.

Al finalizar la descarga abra una terminal, vaya a donde descargo el paquete y posteriormente instale de la siguiente manera:

```
[BASH]# rpm -ivh rpmforge-release-0.3.6-1.$dist.rf.$arch.rpm
```

Una vez concluida esta accion podremos empezar a instalar ClamAV.

Los paquetes que instalaremos seran los siguientes:

● clamav	**El paquete antivirus**
● libclamav	**La API para integrar mas modulos**
● clamtk	**interfaz gráfica basada en GTK**
● clamd	**Métodos para ejecutar el motor en segundo plano (demonio del sistema)**

Instale estos paquetes tecleando en consola lo siguiente:

```
[BASH]# sudo yum install clamav libclamav clamtk clamd
```

11.3 Configuracion de ClamAV

Al concluir la instalacion deberan ser editados los siguientes ficheros:

- /etc/freshclam.conf
- /etc/clamd.conf

11.3.1 Fichero /etc/freshclam.conf

Con la ayuda de algun editor de textos agrege o comente las siguientes lineas.

11.3.1.1 Definiendo la cantidad de actualizaciones que se buscan por dia

Con la ayuda de algun editor de textos edite, busque y agrege la siguiente linea

```
Checks 12
```

El comando

```
Cheks
```

define el intervalo de tiempo en el que ClamAV buscara y descargara las actualizaciones de los virus mas actuales. El numero

```
12
```

Nos indica que cada 2 horas ClamAV buscara y descargara las actualizaciones

11.3.2 Fichero /etc/clamd.conf

Con la ayuda de algun editor de textos agrege o comente las siguientes lineas.

11.3.2.1 Busqueda de fraude mediante firmas

Para habilitar la busqueda de fraude mediante firmas solo debe agregar la siguiente linea

```
PhisingSignatures yes
```

En caso de que el valor tenga asignada la sentencia **"no"** solo habra que cambiarla por **"yes"**

11.3.2.2 Busqueda de fraude mediante analisis de direcciones

Para habilitar la busqueda de fraude mediante analisis de direcciones solo debe agregar la siguiente linea

```
PhishingURLs yes
```

En caso de que el valor tenga asignada la sentencia **"no"** solo habra que cambiarla por **"yes"**

11.3.2.3 Busqueda de fraude haciendo uso de una base de datos

Para habilitar la busqueda de fraudes haciendo uso de una base de datos solo debe agregar la siguiente linea

```
PhishingRestrictedScan yes
```

En caso de que el valor tenga asignada la sentencia **"no"** solo habra que cambiarla por **"yes"**

11.3.2.4 Analizar el contenido HTML

Para habilitar el analisis al contenido HTML solo debe agregar la siguiente linea

```
ScanHTML yes
```

En caso de que el valor tenga asignada la sentencia **"no"** solo habra que cambiarla por **"yes"**

11.3.2.5 Analisis a Ficheros

Para habilitar el analisis a los ficheros solo debe agregar la siguiente linea

```
ScanArchive yes
```

En caso de que el valor tenga asignada la sentencia **"no"** solo habra que cambiarla por **"yes"**

11.3.2.6 Tamaño maximo de archivos a analizar

Para definir el tamaño maximo de archivos a analizar solo debe agregar la siguiente linea

```
ArchiveMaxiFileSize 5M
```

Asi mismo, puede definir una cantidad mayor de bytes ha analizar, solo debe usar la siguiente nomenclatura

```
(m, M = megabytes)
(k, K = kilobytes)
```

11.3.2.7 Tamaño maximo de subcarpetas a analizar

Para definir el tamaño maximo de subcarpetas a analizar solo debe agregar la siguiente linea

```
ArchiveMaxRecursion 10
```

El numero **"10"** se refiere a la cantidad de recursiones que hara sobre cada carpeta, usted puede cambiar este valor a su conveniencia

11.3.2.8 Tamaño maximo de archivos a analizar

Para definir el tamaño maximo de archivos a analizar solo debe agregar la siguiente linea

```
ArchiveMaxFiles 1000
```

El numero **"1000"** se refiere a la cantidad de archivos que analizara ClamAV, usted puede cambiar este valor a su conveniencia

11.4 Activando ClamAV

Para iniciar el Antivirus ClamAV por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/clamd start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el el Antivirus ClamAV. Estas opciones pueden ser consultadas en la siguiente tabla:

start	Inicia el servicio
stop	Detiene el servicio
restart	Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta
reload	Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.
condrestart	Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.
status	Da a conocer el estado en el que se encuentra el servicio

Como alternativa también podemos ocupar el siguiente comando para iniciar el Antivirus ClamAV

```
[root@ localhost ~]# service clamd start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root.

Índice de contenido

Información de Derechos reservados de esta publicación.

Tema 12. Instalacion de MailScanner

12.1 Sobre MailScanner

MailScanner funciona con cualquier sistema basado en Unix y el sistema es compatible con una amplia gama de MTA. Viene con soporte para cualquier combinación de 25 diferentes paquetes antivirus, incluida la de distribución libre ClamAV y su diseño permite el uso de scáner de virus múltiples en paralelo para aumentar el nivel de seguridad.

La protección contra el spam se basa en SpamAssassin y se complementa con las búsquedas rápidas en lista negra que puede ser utilizada para rechazar una gran proporción de mensajes.

La protección contra el malware es proporcionada por una amplia selección de controles y pruebas, que van desde el simple nombre de archivo hasta normas para el contenido basado en la detección de tipos de archivo. También incorpora uno de los más sofisticados detectores de phishing disponible en cualquier lugar.

MailScanner es altamente configurable mediante un sistema de reglas muy intuitivo. Prácticamente cada opción de configuración, por ejemplo, puede ser controlado en un esquema por usuario, por dominio o por IP.

MailScanner es extremadamente fácil de integrar en su actual sistema de transporte de correo, que no requiere modificación de las configuraciones de sendmail. Es utilizado actualmente por una gran selección de organizaciones de todo el mundo, desde las pequeñas empresas y proveedores de servicios de Internet en los EE.UU. y el Gobierno Militar.

12.2 Instalando MailScanner

Uno de los requisitos para poder llevar a cabo la instalacion de MailScanner es actualizar el kernel de nuestro sistema operativo, para hacerlo simplemente teclee lo siguiente en una terminal de BASH.

```
[BASH]# yum update kernel
```

Al terminar reinicie su equipo

Una vez actualizado el kernel del sistema operativo proceda a instalar los siguientes paquetes

```
[BASH]# yum install unrar spamassassin kernel-devel kernel-headers gcc gcc-
c++ rpm-build gmp
```

Por ultimo solo nos restaria instalar MailScanner, desafortunadamente este paquete no existe en los repositorios oficiales de centos por lo que tendremos que descargarlo directamente de la pagina web del proyecto.

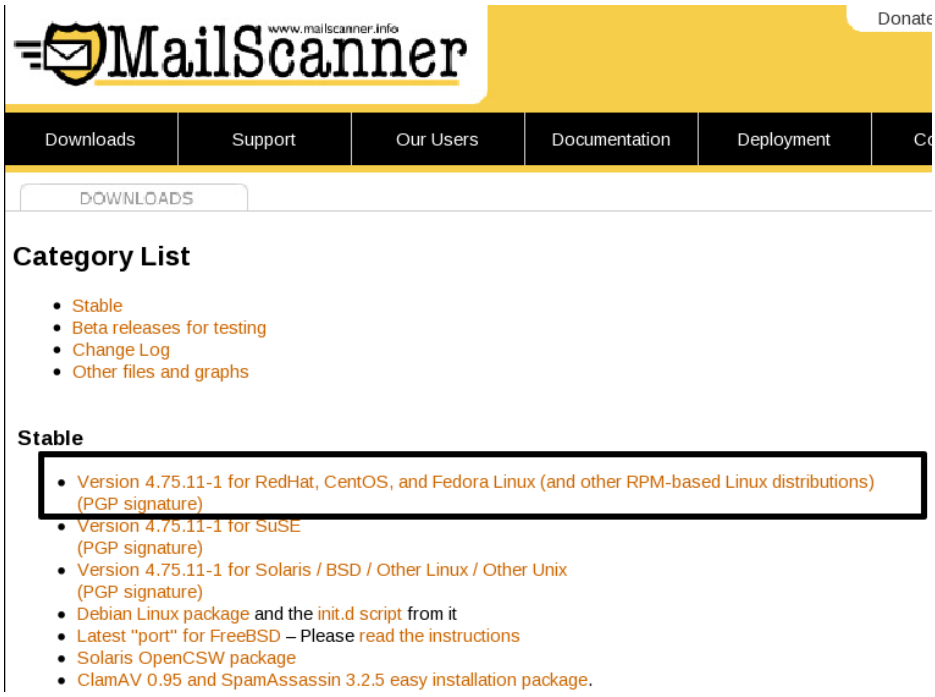
Para descargarlo solo haga lo siguiente:

.-Acceda a la pagina oficial del proyecto MailScanner

```
http://www.mailscanner.info/
```

Y de clic en la seccion de **“downloads”**, esto lo conducira a otra pagina.

Descargue el paquete diseñado para entornos Red Hat , Centos o Fedora.



Descomprime el fichero recién descargado, y cambiate a la carpeta recién creada:

```
[BASH]#. tar -xzvf MailScanner-4.75.11-1.rpm.tar.gz
[BASH]#. cd MailScanner-4.75.11-1/
```

Por ultimo ejecutaremos el script que se encargara del proceso de instalacion

```
[BASH]#./install.sh
```

Este proceso dura aproximadamente entrre 20 y 40 minutos por lo que tendras que ser paciente.

12.3 Configuracion Basica de MailScanner

La configuracion basica de MailScanner se basa en el fichero localizado en:

```
"/etc/MailScanner/MailScanner.conf"
```

12.3.1 Configurando los mensajes del sistema a Español

Con la ayuda de algun editor de textos busque la siguiente linea

```
%report-dir% = /etc/MailScanner/reports/en
```

al haberla ubicado,reemplazela por esta otra

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

Esta accion hara que MailScanner le de los mensajes del sistema en español.

12.3.2 Agregando el nombre de la empresa a MailScanner

Con la ayuda de algun editor de textos busque la siguiente linea

```
%org-name% = yoursite
```

al haberla ubicado,reemplazela por esta otra

```
%org-long-name% = Empresa Irreal S.A de C.V
```

Esta accion hara que MailScanner asigne un remitente a los correos que salgan de nuestro servidor,esto con la finalidad de informar si algun correo infectado salio de nuestro propio servidor o de otro

12.3.3 Agregando la direccion web de la empresa a MailScanner

Con la ayuda de algun editor de textos busque la siguiente linea

```
%web-site%
```

al haberla ubicado,reemplazela por esta otra

```
%web-site% = http://www.suempresa.com.mx
```

Esta accion definira la direccion web asociada nuestra empresa, dicha direccion es incluida en los reportes que se envian a MailScanner

12.3.4 Especificando a MailScanner el antivirus que utilizara

Con la ayuda de algun editor de textos busque la siguiente linea

```
Virus Scanners = none
```

al haberla ubicado,reemplazela por esta otra

```
Virus Scanners = clamav
```

Si nosotros quisieramos especificarle a MailScanner otro antivirus solo deberia anexar el nombre a la linea antes editada. Ejemplo:

```
Virus Scanners = clamav  panda
```

12.3.4 Deshabilitar la cuarentena de los correos infectados y borrarlos del sistema

Con la ayuda de algun editor de textos busque la siguiente linea

```
Quarantine Infections = yes
```

al haberla ubicado,reemplazela por esta otra

```
Quarantine Infections = no
```

Esta accion hara que el sistema en lugar de poner en cuarentena los mensajes infectados los borre inmediatamente del sistema.

11.4 Activando MailScanner

Antes de iniciar el servicio de MailScanner debera detener el servicio de Sendmail, para ello haga lo siguiente:

```
[root@ localhost ~]# /etc/init.d/sendmail stop
[root@ localhost ~]# chkconfig –level35 sendmail off
```

Para iniciar el MailScanner por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/MailScanner start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el el MailScanner. Estas opciones pueden ser consultadas en la siguiente tabla:

start	Inicia el servicio
stop	Detiene el servicio
restart	Reinicia el servicio.–La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta
reload	Recarga el servicio.–La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.
condrestart	Reinicio Condicional.– Solamente se inicia si el servicio se encuentra ejecutándose.
status	Da a conocer el estado en el que se encuentra el servicio

Como alternativa también podemos ocupar el siguiente comando para iniciar el MailScanner

```
[root@ localhost ~]# service MailScanner start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root.

Índice de contenido

Información de Derechos reservados de esta publicación.

Autor del manual: Javier Eduardo Duarte

Tema 10. Instalacion del Cliente de correo OpenWebMail

9.1 Instalando Openwebmail

Tecle en terminal las siguientes instrucciones:

```
[BASH]# cd /etc/yum.repos.d
[BASH]#lftpgethttp://openwebmail.org/openwebmail/download/redhat/rpm/release/openwebmail.repo
[BASH]## yum install openwebmail
```

9.2 Iniciando Openwebmail

Al terminar la instalacion debera ejecutar el script de configuracion de openwebmail, este script se encuentra localizado en:

```
/var/www/cgi-bin/openwebmail
```

La forma de ejecutar este script se hara de la siguiente manera.

```
[BASH]#cd /var/www/cgi-bin/openwebmail

[BASH]#./openwebmail-tool.pl --init
```

Este proceso de configuracion preparara a Openwebmail para su perfecta ejecucion, al terminal, solo debera lanzar Openwebmail de la siguiente manera:

```
http://www.sudominio.com.mx/cgi-bin/openwebmail.pl
```

De igual forma, si usted quisiera cambiar la manera en como accede al correo debera crear un alias en su servidor web apache

9.3 Configurando Openwebmail

Algunas de las recomendaciones para personalizar openwebmail las tendra que hacer sobre el siguiente fichero.

```
/var/www/cgi-bin/openwebmail/etc/openwebmail.conf
```

9.3.1 Agregando el nombre de nuestro dominio a Openwebmail

Con la ayuda de algun editor de textos edite, busque y agrege la siguiente linea

```
domainnames                    sudominio.com.mx
```

9.3.2 Personalizar el idioma

Con la ayuda de algun editor de textos edite, busque y agrege la siguientes lineas

```
##############################################
# Personal Information
default_language                es
default_timeoffset              auto
default_daylightsaving          auto
default_realname                auto
default_fromemails              auto
default_autoreplysubject        This is an autoreply...[Re: $SUBJECT]
```

9.3.3 Personalizar el pie del correo

Con la ayuda de algun editor de textos edite, busque y agrege la siguientes lineas

```
<default_signature>
---------------------------------------
Tu Empresa
La direccion de tu empresa
Telefonos: xxx xx xx

TuEmpresa S.A de C.V
</default_signature>
```

9.3.4 Personalizar el aspecto y la regionalizacion

Con la ayuda de algun editor de textos edite, busque y agrege la siguientes lineas

```
##############################################
# Display Preference
default_style                   Default
default_iconset                 Cool3D.Spanish
default_bgurl                   %ow_htmlurl%/images/backgrounds/Globe.gif
default_bgrepeat                yes
default_fontsize                10pt
default_dateformat              dd/mm/yyyy
default_hourformat              12
```

9.3.5 Seguridad

Con la ayuda de algun editor de textos edite, busque y agrege la siguientes lineas

Para mayor seguridad deberias desactivar la opcion:

```
enable_sshterm
```

para no dar acceso a SSH a través del webmail.

El rootpath es un directorio que se crea dentro de la carpeta del usuario

```
/home/usuario/webdisk
```

en el cual queda enjaulado, es decir, sólo puede dejar archivos en esa carpeta y las subcarpetas que genere.

```
##############################################
# Security Settings
webdisk_rootpath                  /webdisk
webdisk_lsmailfolder              no
webdisk_lshidden                  no
webdisk_lsunixspec                no
webdisk_lssymlink                 yes
webdisk_allow_symlinkout          yes
webdisk_symlinkout_display        @
enable_sshterm                    no
# ps: To completely disable the SSH terminal support, you have to remove
# the file data/openwebmail/applet/mindterm/mindtermfull.jar
```

9.3.6 Opciones de cuota por usuario

Con la ayuda de algun editor de textos edite, busque y agrege la siguientes lineas

```
##############################################
# Quota System (limit in KB and threshold in%)
#            1 MB =     1,024 KB
#           10 MB =    10,240 KB
#          100 MB =   102,400 KB
# 1 GB = 1,024 MB = 1,048,576 KB
# uncomment following lines if you wish to enable Quota System for 10 Mb
quota_module            quota_du.pl
spool_limit             10240
quota_limit             10240
quota_threshold         0
delmail_ifquotahit      yes
delfile_ifquotahit      yes
```