Guía del servidor Ubuntu

Proyecto de documentación Ubuntu <*ubuntu-doc@lists.ubuntu.com*>

Guía del servidor Ubuntu

por Proyecto de documentación Ubuntu <*ubuntu-doc@lists.ubuntu.com*>

Resumen

Introducción a la instalación y configuración de aplicaciones de servidor en Ubuntu.

Créditos y licencias

Los siguientes autores del Equipo de Documentación de Ubuntu mantienen este documento:

- Bhuvaneswaran Arumugam

La Guía del servidor de Ubuntu también está basada en contribuciones de:

- Robert Stoffers
- Brian Shumate
- Rocco Stanzione

Limitación de responsabilidad

Tabla de contenidos

Acerca de esta guía v
1. Convenciones vi
2. Contribuciones y realimentación viii
1. Introducción 9
2. Instalación 10
1. Preparando la Instalación 11
2. Instalando desde CD 13
3. Gestión de paquetes 14
1. Introducción 15
2. Apt-Get 16
3. Aptitude 18
4. Configuración 20
5. Repositorios adicionales 21
4. Red 22
1. Configuración de red 23
2. TCP/IP 26
3. Configuración del Cortafuegos 31
4. Servidor OpenSSH 34
5. Servidor FTP 37
6. Network File System (NFS) 39
7. Dynamic Host Configuration Protocol (DHCP) 41
8. Servicio de nombre de dominio (DNS) 44
9. CUPS - Servidor de Impresión 46
10. HTTPD - Servidor Web Apache2 49
11. Servidor proxy Squid 59
12. Sistema de Control de Versiones 61
13. Bases de Datos 68
14. Servicios de correo electrónico 71
5. Redes Windows 83
1. Introducción 84
2. Instalar Samba 85
3. Configurar SAMBA 86
A. Creative Commons by Attribution-ShareAlike 2.0 92
B. GNU Free Documentation License 98

Lista de tablas

2.1. Requerimientos mínimos recomendados 11
4.1. Métodos de Acceso 62

Acerca de esta guía

1. Convenciones

Se usarán las siguientes notas a lo largo del libro:

Una nota presenta información interesante, a veces técnica, relacionada con la explicación en curso.

Una pista ofrece consejos o una manera más sencilla de hacer algo.

Un aviso de precaución alerta al lector sobre problemas potenciales y ayuda a evitarlos.

Una advertencia avisa al lector del peligro que puede aparecer en un escenario concreto.

Las referencias cruzadas para la impresión se mostrarán de la siguiente forma:

- Los enlaces para otros documentos o sitios web se verán como *así* [http://www.ubuntu.com].

Las versiones PDF, HTML y XHTML de este documento utilizarán hipervínculos para gestionar referencias cruzadas.

Las conveniciones tipográficas se visualizarán de la siguiente forma:

- Los nombres de archivos y las rutas a los directorios se mostrarán en un tipo de letra `monoespaciada`.
- Las órdenes que pueda teclear en una Terminal se mostrarán así:

  ```
  orden a teclear
  ```

- Las opciones sobre las que pulse, seleccione o escoja en una interfaz de usuario se mostrarán en un tipo de letra `monoespaciada`.

Selecciones de menú, acciones de ratón y combinaciones de teclas:

- Una secuencia de selecciones de menú se mostrará de la siguiente manera: Archivo → Abrir
- Las acciones con el ratón asumen una configuración adecuada para usuarios diestros. Los términos “pulsar” y “pulsar dos veces” se refieren al botón izquierdo del ratón. El término “pulsar con el botón derecho” se refiere al botón derecho del ratón. El término “pulsar con el botón central” se refiere al botón central del ratón, apretando la rueda de desplazamiento, o bien pulsando los botones izquierdo y derecho simultáneamente, según el diseño del ratón.
- Las combinaciones de teclas se mostrarán de la siguiente manera: **Ctrl-N**. Donde los convenios para las teclas “Control”, “Mayúsculas” y “Alternativa” serán **Ctrl**, **Mayús** y

Alt, respectivamente, y significa que hay que mantener pulsada la primera tecla mientras se pulsa la segunda.

2. Contribuciones y realimentación

Este libro es desarrollado por el *Equipo Documentación de Ubuntu* [https://wiki.ubuntu.com/DocumentationTeam]. *Usted* puede contribuir con este documento enviando ideas o comentarios a la lista de correo del Equipo de Documentación de Ubuntu. Información acerca del equipo, sus listas de correo, proyectos, etc. puede encontrarse en el *Sitio web del Equipo de Documentación de Ubuntu* [https://wiki.ubuntu.com/DocumentationTeam].

Si usted observa algún problema en este documento, o quisiera hacer alguna sugerencia, usted puede simplemente reportar ese error en el *Seguimiento de Errores de Ubuntu* [https://launchpad.net/products/ubuntu-doc/+bugs]. Su ayuda es de vital importancia para el éxito de nuestra documentación!

Muchas gracias,

-Su Equipo de Documentación de Ubuntu

Capítulo 1. Introducción

Bienvenido a la *Guía del servidor de Ubuntu*.

La *Guía del servidor de Ubuntu* contiene información sobre cómo instalar y configurar varias aplicaciones de servidor en su sistema Ubuntu para satisfacer sus necesidades. Es una guía paso a paso, orientada a tareas, de configuración y personalización de su sistema. Este manual discute muchos temas intermedios como los siguientes:

- Configuración de red
- Configuración de Apache2
- Bases de Datos
- Redes Windows

Este manuel esta dividido en las siguiente categorias principales:

- Instalación
- Gestión de paquetes
- Red
- Redes Windows

Esta guía asume que usted tiene una conocimiento básico del sistema Ubuntu. Si necesita ayuda detallada para la instalación de Ubuntu, revise la Guía de Instalación de Ubuntu.

Las versiones en HTML y PDF de este manual se encuentran disponibles en *La web de la Documentación de Ubuntu* [http://help.ubuntu.com].

Puede comprar esta guía editada en forma de libro en *nuestro almacén Lulu* [http://www.lulu.com/ubuntu-doc]. Sólo tendrá que pagar los gastos de impresión y envío.

Capítulo 2. Instalación

Este capítulo suministra un rápido vistazo a la instalación de Ubuntu 6.06 LTS Edición Servidor. Para unas instrucciones más detalladas, por favor remitase a la Guía de Instalación de Ubuntu.

1. Preparando la Instalación

Esta sección explica varios aspectos a considerar antes de comenzar la instalación.

1.1. Requerimientos de Sistema

Ubuntu 6.06 LTS Edición Servidor soporta tres (3) arquitecturas: Intel x86, AMD64, y PowerPc. La tabla de debajo muestra una lista de las especificaciones de hardware recomendadas. Dependiendo de sus necesidades, puede gestionarlo con menos recursos de los citados. En cualquier caso, muchos usuario podrian resultar frustrados si ignora estas sugerencias.

Tabla 2.1. Requerimientos mínimos recomendados

Tipo de Instalación	RAM	Espacio en Dis
Servidor	64 megabytes	500 megabytes

El perfil por defecto de Ubuntu 6.06 LTS Edición Servidor es mostrado debajo. Una vez más, el tamaño de la instalación puede incrementarse dependiendo de los servicios que usted instale durante la instalación. Para la mayoría de los administradores, los servicios por defecto son suficientes para un uso general del servidor.

Servidor

Existe un perfil de servidor pequeño, que proporciona una base común para todo tipo de aplicaciones de servidor. Es un perfil mínimo diseñado para añadir sobre él los servicios deseados, como servicios de archivos e impresión, alojamiento web, alojamiento de correo electrónico, etc. Para esos servicios, puede ser suficiente contar con al menos 500 MB de espacio en disco, pero sería conveniente añadir más espacio dependiendo de los servicios que desee alojar en su servidor.

Recuerde que tales tamaños no incluyen el resto de materiales que normalmente encontrará, como archivos de usuario, correo, registros y datos. Siempre es mejor ser generoso en cuanto al espacio para sus propios archivos y datos.

1.2. Realizar una copia de seguridad

- Antes de empezar, asegúrese de que ha hecho una copia de seguridad de todos los archivos suyos que haya en su sistema. Si es la primera vez que va a instalar un sistema operativo no nativo en su equipo, probablemente necesitará reparticionar su disco para dejar espacio a Ubuntu. Siempre que vaya a particionar su disco, deberá estar dispuesto a perder todo el contenido del disco por cometer algún error o porque vaya mal algo durante el particionado, como por ejemplo una caída en la corriente eléctrica. Los programas usados durante la instalación son bastante fiables, y muchos se han usado durante años, pero también realizan acciones destructivas, y un error durante su uso puede provocar la pérdida de todos sus valiosos datos.

Si está creando un sistema de arranque múltiple, asegúrese de que tiene a mano los soportes de distribución de todos los demás sistemas operativos. Especialmente si reparticiona su unidad de arranque, probablemente necesitará reinstalar el cargador de arranque de su sistema operativo, o en muchos casos el sistema operativo completo y todos los archivos de la partición afectada.

2. Instalando desde CD

Inserta tu CD de instalación en el Lector de CD y reeinicia el computador. El sistema de instalación comienza inmediatamente al iniciar desde el CD-ROM. Una vez iniciado, aparecerá la primera pantalla

En este punto, lea el texto de la pantalla. Puede leer la pantalla de ayuda proporcionada por el sistema de instalación. Para ello, pulse F1.

Para realizar una instalación predeterminada de servidor, seleccione “Instalar en el disco duro” y pulse **Intro. Empezará el proceso de instalación. Simplemente siga las instrucciones en pantalla, y se instalará su sistema Ubuntu.**

Alternativamente, para instalar un servidor LAMP (Linux, Apache, Mysql, PHP/Perl/Python), selecciona “Instalar servidor LAMP”, y sigue las instrucciones

Capítulo 3. Gestión de paquetes

Ubuntu ofrece un completo sistema de gestión de paquetes para la instalación, actualización, configuración y eliminación de software. Además de proporcionar acceso a una base de más de 17.000 paquetes de software para su ordenador Ubuntu, el gestor de paquetes también ofrece capacidades de resolución de dependencias y comprobación de actualizaciones de software.

Existen algunas herramientas disponibles para interactuar con el sistema de gestión de paquetes de Ubuntu, desde simples utilidades de línea de órdenes fácilmente automatizables por los administradores de sistemas, a sencillas interfaces gráficas fáciles de utilizar por los recién llegados a Ubuntu.

1. Introducción

El sistema de gestión de paquetes de Ubuntu está derivado del mismo sistema utilizado por la distribución Debian GNU/Linux. Los paquetes contienen todos los archivos necesarios, meta-datos e instrucciones para implementar una funcionalidad particular o una aplicación software en un ordenador Ubuntu.

Los paquetes Debian normalmente tienen la extensión '.deb', y normalmente existen en *repositorios* que son colecciones de paquetes que se encuentran en varios soportes, como discos CD-ROM o en línea. Los paquetes normalmente están en un formato binario pre-compilado; su instalación es rápida y no requiere compilar software.

Algunos paquetes complejos utilizan el concepto de *dependencia*. Las dependencias son paquetes adicionales que necesita el paquete principal para funcionar correctamente. Por ejemplo, el paquete para síntesis de voz Festival depende del paquete festvox-kalpc16k, que suministra una de las voces usadas por la aplicación. Para que funcione Festival , deben instalarse todas las dependencias junto con el paquete principal Festival. Las herramientas de gestión de software en Ubuntu hacen esto automáticamente.

2. Apt-Get

La orden apt-get es una potente herramienta de línea de órdenes diseñada para trabajar con el *Advanced Packaging Tool* (APT) de Ubuntu realizando funciones de instalación de nuevos paquetes de software, actualización de paquetes de software, actualización del índice de paquetes, e incluso actualización de todo el sistema Ubuntu.

Siendo como es una simple herramienta de línea de órdenes, apt-get tiene numerosas ventajas frente otras herramientas de gestión de paquetes disponibles para los administradores de sistemas en Ubuntu. Algunas de estas ventajas incluyen facilidad de uso a través de conexiones sencillas de terminal (SSH) y la capacidad de poder usarse en scripts de administración del sistema, que pueden automatizarse en la utilidad de planificación de tareas cron .

Algunos ejemplos de uso populares de la utilidad apt-get:

- **Instalar un paquete**: La instalación de paquetes usando la herramienta apt-get es bastante simple. Por ejemplo, para instalar el analizador de red *nmap*, teclee lo siguiente:

```
sudo apt-get install nmap
```

- **Desinstalar un paquete**: Desinstalar uno o varios paquetes es también un proceso simple y sencillo. Para desinstalar el paquete nmap instalado en el ejemplo anterior, teclee lo siguiente:

```
sudo apt-get remove nmap
```

Múltiples paquetes: Puede especificar multiples paquetes para instalar o desinstalar, separándolos por espacios.

- **Actualizar el índice de paquetes**: El índice de paquetes de APT es esencialmente una base de datos de paquetes disponibles en los repositorios definidos en el archivo `/etc/apt/sources.list`. Para actualizar el índice local de paquetes con los últimos cambios realizados en los repositorios, teclee lo siguiente:

```
sudo apt-get update
```

- **Actualizar paquetes**: Con el tiempo, ciertos paquetes instalados en su ordenador pueden tener disponibles versiones suyas más actualizadas en el repositorio de paquetes (por ejemplo actualizaciones de seguridad). Para actualizar su sistema, primero actualice su índice de paquetes como se mostraba antes, y despúes teclee:

```
sudo apt-get upgrade
```

Si un paquete necesita instalar o desinstalar nuevas dependencias durante su actualización, no se podrá actualizar con la orden *upgrade*. Para esta actualización, es necesario que use la orden *dist-upgrade* .

Además, usted puede actualizar su sistema Ubuntu de una revisión a otro con dist-upgrade. Por ejemplo, para actualizar de la versión Ubuntu 5.10 a la versión 6.06 LTS, primero debe asegurarse que reemplaza los repositorios de la versión 5.10 existente por los de la 6.06 LTS en su ordenador `/etc/apt/sources.list`, después simplemente introduzca el comando apt-get update como se detalla anteriormente, y finalmente, ejecute la actualización:

```
#
sudo apt-get dist-upgrade#
```

Después de una considerable cantidad de tiempo, su ordenador estará actualizado con la nueva versión. Normalmente, se pueden requerir algunos pasos posteriores a la instalación como se detalla en las notas de actualización de la versión a la que usted se está actualizando.

Las acciones realizadas por la orden apt-get , como la instalación o desinstalación de paquetes, son registradas en el archivo de registro «/var/log/dpkg.log».

Para más información sobre el uso de APT, lea el completo *Manual de Usuario de Debian APT* [http://www.debian.org/doc/user-manuals#apt-howto] o teclee:

```
apt-get help
```

3. Aptitude

Aptitude es una interfaz del sistema *APT (Advanced Packaging Tool)* basada en texto y que se maneja por menús. Muchas de las funciones típicas de gestión de paquetes, como la instalación, desinstalación y actualización, se realizan con Aptitude mediante órdenes de una sola tecla, normalmente letras minúsculas.

Aptitude es conveniente usarlo sobre todo en entornos de terminales no gráficas para garantizar el correcto funcionamiento de las teclas de órdenes. Puede iniciar Aptitude como un usuario normal con la siguiente orden en la línea de órdenes de una terminal:

```
sudo aptitude
```

Cuando inicie Aptitude , usted podrá ver una barra de menú en la parte de arriba de la pantalla y dos paneles debajo de esta barra. El panel superior contiene las categorías de los paquetes, tal como *Nuevos Paquetes* y *Paquetes No Instalados*. El panel inferior contiene información relativa a los paquetes y categorías de paquetes.

Usar Aptitude para el manejo de paquetes es relativamente sencillo, y el interface de usuario hace que las tareas comunes sean fáciles de realizar. Lo siguiente son ejemplos de funciones de manejo de paquetes como se realizan en Aptitude:

- **Instalar paquetes**: Para instalar un paquete, localícelo en la categoría «Paquetes no instalados», por ejemplo usando las teclas del cursor del teclado y la tecla **INTRO**, y seleccionando el paquete que desee instalar. Una vez haya seleccionado el paquete deseado, pulse la tecla **+**, y la entrada del paquete se pondrá de color *verde*, indicando así que el paquete ha sido marcado para su instalación. Entonces pulse la tecla **g** y se le presentará un resumen de las acciones que se van a realizar. Pulse **g** otra vez, y entonces se le solicitará convertirse en superusuario para completar la instalación. Pulse **INTRO** para que se le solicite la contraseña. Introduzca su contraseña para obtener privilegios de superusuario. Finalmente, pulse **g** una vez más y se le pedirá permiso para descargar el paquete. Pulse **INTRO** sobre el botón *Continuar*, y comenzará la descarga y posterior instalación del paquete.
- **Desinstalar paquetes**: Para desinstalar un paquete, localícelo en la categoría de paquetes «Paquetes instalados», por ejemplo usando las teclas del cursor y la tecla **Intro**, seleccione el paquete que desea desinstalar. A continuación pulse la tecla **-** y la entrada del paquete se volverá *rosa*, indicando así que se ha marcado para su desinstalación. Ahora pulse la tecla **g** y se le presentará un resumen de las acciones a realizar sobre los paquetes. Pulse de nuevo la tecla **g**, y se le pedirá que se convierta en administrador para completar la instalación. Pulse **Intro** y se le pedirá la contraseña. Introduzca su contraseña de usuario para convertirse en administrador. Finalmente, pulse una vez más la tecla **g** y se le preguntará si quiere descargar el paquete. Pulse **Intro** sobre el botón*Continuar*, y dará comienzo la desinstalación del paquete.

- **Actualizar el índice de paquetes**: Para actualizar el índice de paquetes, simplemente pulse la tecla **u** y se le pedirá que se convierta en administrador para finalizar la instalación. Pulse **Intro**, tras lo cual se le pedirá una contraseña. Introduzca su contraseña de usuario para convertirse en administrador. Comenzará la actualización del índice de los paquetes. Pulse **Intro** sobre el botón Aceptar cuando aparezca la ventana de descarga para completar el proceso.
- **Actualizar paquetes**: Para actualizar paquetes, realice la actualización del índice de los paquetes como se detalla más arriba, y después pulse la tecla **U** (mayúscula) para marcar todos los paquetes actualizables. Ahora pulse **g** lo que le presentará un resumen de las acciones a realizar sobre los paquetes. Pulse **g** nuevamente, y se le pedirá que se convierta en administrador para completar la instalación. Pulse **Intro**, tras lo cual se le pedirá una contraseña. Introduzca su contraseña de usuario para convertirse en administrador. Finalmente, pulse **g** una vez más, y se le preguntará si desea descargar los paquetes. Pulse **Intro** en el botón *Continuar* para comenzar la actualización de los paquetes.

La primera columna de información mostrada en la lista de paquetes en el panel superior refleja el estado actual de cada paquete, y para describir dicho estado se usa la siguiente leyenda:

- **i**: Paquete instalado.
- **c**: Paquete no instalado, pero la configuración del paquete permanece en el sistema
- **p**: Eliminado del sistema
- **v**: Paquete virtual
- **B**: Paquete roto
- **u**: Archivos desempaquetados, pero el paquete esta sin configurar
- **C**: A medio configurar- La configuración falló y requiere ser reparada
- **H**: A medio configurar- Falló la eliminación y requiere ser reparada

Para cerrar Aptitude, simplemente presione la tecla **q** y confirme que desea salir. Muchas otras funciones del menú de Aptitude estan disponibles presionando la tecla **F10** .

4. Configuración

La configuración de los repositorios del sistema *Advanced Packaging Tool* (APT) se guarda en el archivo de configuración /etc/apt/sources.list. Un ejemplo de este archivo está referenciado aquí, junto con información sobre añadir o eliminar referencias a repositorios en este archivo.

Aquí [../sample/sources.list] tiene un sencillo ejemplo de un archivo `/etc/apt/sources.list` típico.

Usted puede editar el fichero para habilitar o desabilitar repositorios. Por ejemplo, para desabilitar el requerimiento de insertar el CD-ROM de Ubuntu al operar con paquetes, simplemente comente la línea apropiada para el CD-ROM, que aparece al principio del archivo.

```
# no more prompting for CD-ROM please
# deb cdrom:[Ubuntu 6.06 _Dapper Drake_ - Release i386 (20060329.1)]/ dapper main restrict
```

5. Repositorios adicionales

Además de los repositorios disponibles de paquetes soportados oficialmente por Ubuntu, existen otros repositorios mantenidos por la comunidad que añaden miles de paquetes potenciales para su instalación. Dos de esos repositorios adicionales son los más populares, y son los repositorios *Universe* y *Multiverse*. Esos repositorios no están soportados oficialmente por Ubuntu, por lo que no están activados de forma predeterminada, pero generalmente proporcionan paquetes que usted podrá usar de forma segura en su equipo Ubuntu.

Los paquetes en el repositorio Multiverse suelen tener asuntos en la licencia que les impiden ser incluidos en las distribuciones con un sistema operativo libre, y pueden ser ilegales en su localidad.

Debe saber que los repositorios *Universe* o *Multiverse* nunca contienen paquetes soportados oficialmente. En particular, no habrá actualizaciones de seguridad para estos paquetes.

Hay muchas otras fuentes de paquetes disponibles, algunas de ellas solo ofrecen un paquete, como en el caso de paquetes suministrados por el desarrollador de una sola aplicación. Usted siempre debe ser muy precavido cuando use fuentes de paquetes no-standard. Investigue la fuente y los paquetes cuidadosamente antes de realizar ninguna instalación, algunas fuentes de paquetes y sus paquetes pueden volver algo inestable o no funcional su sistema en algunos casos.

Para habilitar los repositorios *Universe* y *Multiverse* , edite el archivo `/etc/apt/sources.list` y descomente las líneas apropiadas:

```
# We want Multiverse and Universe repositories, please

deb http://archive.ubuntu.com/ubuntu dapper universe multiverse
deb-src http://archive.ubuntu.com/ubuntu dapper universe multiverse
```

5.1. Referencias

Cómo añadir repositorios (Ubuntu Wiki)
[https://wiki.ubuntu.com/AddingRepositoriesHowto]

Capítulo 4. Red

La red consiste en dos o más dispositivos, como ordenadores, impresoras y equipamiento relacionado que están conectados por cables o enlaces wireless con el proposito de compartir y distribuir información a través de los dispositios conectados.

Esta seccion de la Guía del servidor Ubuntu proporciona información general y específica sobre las redes, incluyendo un vistazo a conceptos de red y detalladas discusiones sobre protocolos de red y aplicaciones de servidor.

1. Configuración de red

Ubuntu viene con varias utilidades gráficas para configurar sus dispositivos de red. Este documento es una herramienta para los administradores de servidores y esta enfocada para manejar su red en línea de comandos.

1.1. Ethernet

La mayoría de la configuración de Ethernet está centralizada en un único archivo, `/etc/network/interfaces`. Si usted no tiene dispositivos Ethernet, en este archivo sólo aparecerá el dispositivo loopback, y tendrá un aspecto parecido a éste:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback
address 127.0.0.1
netmask 255.0.0.0
```

Si tiene sólo un dispositivo Ethernet, eth0, y éste obtiene su configuración desde un servidor DHCP, y se debe activar automáticamente durante el arranque del sistema, sólo se deben añadir dos líneas adicionales:

```
auto eth0
iface eth0 inet dhcp
```

La primera línea especifica que el dispositivo eth0 debe activarse automáticamente durante el arranque del equipo. La segunda línea significa que la interfaz (“iface”) eth0 debe tener un espacio de direcciones IPv4 (sustituya “inet” por “inet6” en un dispositivo IPv6) y que debe obtener su configuración automáticamente desde un servidor DHCP. Suponiendo que tanto su red como su servidor DHCP están correctamente configurados, la red de este equipo no necesitaría más configuración adicional para poder funcionar. El servidor DHCP le proporcionará la pasarela (gateway) predeterminada (implementada mediante la orden route), la dirección IP del dispositivo (implementada mediante la orden ifconfig), y los servidores DNS usados en la red (implementados en el archivo `/etc/resolv.conf`.)

Para configurar su dispositivo Ethernet con una dirección IP estática y una configuración personalizada, se requiere más información. Suponga que desea asignar la dirección IP 192.168.0.2 al dispositivo eth1, con la clásica máscara de red 255.255.255.0. La dirección IP de su pasarela predeterminada es 192.168.0.1. En tal caso, podría poner algo semejante a ésto en `/etc/network/interfaces`:

```
iface eth1 inet static
 address 192.168.0.2
 netmask 255.255.255.0
 gateway 192.168.0.1
```

En este caso, necesitará especificar sus servidores DNS manualmente en `/etc/resolv.conf`, que tendría entonces el siguiente aspecto:

```
search midominio.com
nameserver 192.168.0.1
nameserver 4.2.2.2
```

La directiva *search* añadirá midominio.com a todas las consultas de nombres de host para intentar resolver nombres en su red. Por ejemplo, si el dominio de su red es midominio.com e intenta hacer un ping al host “mipc”, la consulta DNS se transformará en una consulta a “mipc.midominio.com” para su resolución. Las directivas *nameserver* especifican los servidores DNS que se usarán para resolver nombres de hosts en direcciones IP. Si usa su propio servidor de nombres, introdúzcalo aquí. En caso contrario, pregunte a su proveedor de Internet qué servidores DNS primario y secundario debe utilizar, e introdúzcalos en `/etc/resolv.conf` como se acaba de explicar.

Es posible realizar muchas más configuraciones, incluyendo interfaces de marcación analógica PPP, redes IPv6, dispositivos VPN, etc. Acuda a man 5 interfaces para obtener más información y las opciones soportadas. Recuerde que los scripts ifup/ifdown usan `/etc/network/interfaces` como un esquema de configuración de más alto nivel que el utilizado en otras distribuciones de Linux, y que las tradicionales utilidades de más bajo nivel como ifconfig, route y dhclient todavía se encuentran disponibles para realizar configuraciones más puntuales.

1.2. Gestionar entradas DNS

Esta sección explica cómo configurar el servidor de nombres que se usará para resolver direcciones IP en nombres de host, y viceversa. No explica cómo configurar el sistema como un servidor de nombres.

Para administrar los DNS, puedes agregar, editar o eliminar los servidores DNS desde el archivo `/etc/resolv.conf`. Un *archivo de ejemplo* [../sample/resolv.conf] se muestra a continuación:

```
search com
nameserver 204.11.126.131
nameserver 64.125.134.133
nameserver 64.125.134.132
nameserver 208.185.179.218
```

La clave search especifica la cadena que se añadirá a un nombre incompleto de host. Aquí se ha especificado como com. Por tanto, cuando se ejecute la orden: **ping ubuntu** ésta se interpretará como **ping ubuntu.com**.

La clave nameserver especifica la dirección IP del servidor de nombres. Se usará para resolver las direcciones IP o los nombres de host dados. Este archivo puede tener varias

entradas de servidores de nombres. Las consultas de la red usarán los servidores de nombres en el mismo orden en el que aparezcan en el archivo.

Si los nombres de los servidores DNS se recogen dinámicamente mediante DHCP o PPPOE (desde su proveedor de Internet), no añada ninguna entrada de servidor de nombres a este archivo. Se actualizará automáticamente.

1.3. Gestionar los hosts

Para gestionar los hosts, puede añadir, editar, o borrar hosts del archivo `/etc/hosts`. Este archivo contiene direcciones IP y sus correspondientes nombres de host. Cuando su sistema intenta resolver un nombre de host en una dirección IP, o determinar el nombre del host a partir de su dirección IP, busca en el archivo `/etc/hosts` antes de usar los servidores de nombres. Si la dirección IP se encuentra en el archivo `/etc/hosts`, no se usarán los servidores de nombres. Este comportamiento se puede modificar cambiando el archivo `/etc/nsswitch.conf` para adaptarlo a sus necesidades.

Si su red contiene ordenadores cuya dirección IP no este listada en el DNS, es recomendable que los añada en el archivo `/etc/hosts`.

2. TCP/IP

El Protocolo de Control de Transmisión y Protocolo Internet (Transmission Control Protocol and Internet Protocol, TCP/IP) es un juego de protocolos estandard desarrollados a finales de los 70 por el Defense Advanced Research Projects Agency (DARPA) como una forma de comunicarse entre diferentes tipo de ordenadores y redes. TCP/IP es el impulsor de Internet, y es el más popular juego de protocolos de red de la Tierra.

2.1. Introducción a TCP/IP

Los dos protocolos componentes del TCP/IP se encargan de aspectos diferentes en las redes de ordenadores. El *Protocolo Internet* (Internet Protocol), el «IP» del TCP/IP, es un protocolo sin conexión que se ocupa únicamente del encaminamiento de los paquetes a través de la red usando el *datagrama IP* como unidad básica de información en la red. Los datagramas IP constan de una cabecera seguida de un mensaje. El *Protocolo de Control de Transmisión* (Transmission Control Protocol) es el «TCP» del TCP/IP y permite que los hosts de la red puedan establecer conexiones que se utilizarán para intercambiar flujos de datos. El TCP también garantiza la entrega de los datos a través de las conexiones y que éstos llegarán al host de destino en el mismo orden en que fueron enviados desde el host de origen.

2.2. Configuración de TCP/IP

La configuración del protocolo TCP/IP consta de varios elementos que deben establecerse editando los archivos de configuración apropiados, o utilizando soluciones como el servidor de Protocolo de Configuración Dinámica de Hosts (Dynamic Host Configuration Protocol, DHCP) que, de hecho, puede configurarse para proporcionar automáticamente las opciones de configuración TCP/IP adecuadas para los clientes de la red. Esos valores de configuración deben establecerse adecuadamente para poder facilitar el correcto funcionamiento de la red en su sistema Ubuntu.

Los elementos de configuración comunes del TCP/IP y sus propositos son los siguientes:

- **Dirección IP** La dirección IP es una cadena de identificación única expresada como cuatro números decimales que van desde 0 hasta 255, separados por puntos, donde cada uno de los cuatro números representan 8 bits de la dirección, de un total de 32 bits para la dirección completa. Este formato se denomina *notación cuádruple con puntos*.
- **Máscara de red** La máscara de red (o máscara de subred) es una máscara local de bits, o conjunto de indicadores, que separan, en una dirección IP, la parte correspondiente a la red de la parte correspondiente a la *subred*. Por ejemplo, en una red de Clase C, la máscara de red estándar es 255.255.255.0, lo que enmascara los tres primeros bytes de la dirección IP y deja disponible el último byte de la dirección IP para poder especificar hosts en la subred.

- **Dirección de red** La dirección de red representa los bytes que componen la porción de red de una dirección IP. Por ejemplo, el host 12.128.1.2 en una red de Clase A debe usar 12.0.0.0 como dirección de red, en el que el doce (12) representa el primer byte de la dirección IP, (la parte de red) y los ceros (0) en los restantes tres bytes representan los posibles valores de host. Los hosts de una red que use direcciones IP privadas no enrutables tan comunes como 192.168.1.100 deberán usar la dirección de red 192.168.1.0, que especifica los tres primeros bytes de la red de clase C 192.168.1 y el cero (0) para todos los posibles hosts de la red.
- **Dirección de difusión (broadcast)** La dirección de difusión es una dirección IP que permite enviar datos a todos los hosts de una misma subred simultáneamente, en lugar de especificar uno por uno cada host de la red. La dirección de difusión general estándar para las redes IP es 255.255.255.255, pero esta dirección de difusión no se puede usar para enviar un mensaje de difusión a todos los hosts de Internet porque los routers lo bloquean. Se puede establecer una dirección de difusión más apropiada cuadrándola con una subred específica. Por ejemplo, en la populare rede IP privada de Clase C, 192.168.1.0, la dirección de difusión debería configurarse como 192.168.1.255. Los mensajes de difusión son producidos normalmente por los protocolos de red como el Protocolo de Resolución de Direcciones (Address Resolution Protocol, ARP), y el Protocolo de Información de Encaminamiento (Routing Information Protocol, RIP).
- **Dirección de pasarela o «puerta de enlace» (gateway)** Una dirección de pasarela es la dirección IP a través de la cual se puede alcanzar una red, o un host concreto dentro de una red. Si el host de una determinada red desea comunicarse con otro host, y éste host no está en la misma red que el primero, se deberá usar una *pasarela*. En muchos casos, la dirección de pasarela será la dirección de un router de la red, que será el encargado de pasar el tráfico a otras redes o hosts, como por ejemplo los hosts de Internet. El valor de la dirección de pasarela debe ser correcto, o de lo contrario su sistema no será capaz de alcanzar ningún host que esté fuera de su red.
- **Dirección del servidor de nombres (nameserver)** Las direcciones de los servidores de nombres representan direcciones IP de sistemas DNS (Domain Name Service, Servicio de Nombre de Dominio), encargados de convertir («resolver») nombres de hosts en direcciones IP. Hay tres niveles de direcciones de servidores de nombres, que se especifican por orden de preferencia: el servidor de nombres *primario*, el servidor de nombres *secundario* y el servidor de nombres *terciario*. Para que su sistema sea capaz de resolver nombres de hosts en sus correspondientes direcciones IP, debe especificar en la configuración TCP/IP de su sistema las direcciones válidas de servidores de nombre que usted esté autorizado a usar. En muchos casos, esas direcciones pueden y deben ser proporcionadas por su proveedor de servicios de red (o su proveedor de Internet), aunque existen muchos servidores de nombre gratuitos y accesibles públicamente disponibles para su uso, como por ejemplo los servidores de Level3 (Verizon), cuyas direcciones IP van del 4.2.2.1 al 4.2.2.6.

La dirección IP, la máscara de red, la dirección de red, la dirección de broadcast (difusión) y la dirección de gateway (pasarela) se especifican normalmente por medio de las directivas apropiadas en el archivo `/etc/network/interfaces`. Las direcciones de los servidores de nombres se especifican normalmente por medio de las directivas *nameserver* en el archivo `/etc/resolv.conf`. Para más información, vea la página de manual para `interfaces` o `resolv.conf`, respectivamente, con las siguientes órdenes tecleadas en la línea de órdenes de una terminal:

Acceda a la página del manual de `interfaces` con el siguiente comando:

```
man interfaces
```

Acceda a la página del manual de `resolv.conf` con el siguiente comando:

```
man resolv.conf
```

2.3. Encaminamiento IP

El encaminamiento IP es una manera de especificar y descubrir caminos en una red TCP/IP por los cuales se pueden enviar datos dentro de la red. El encaminamiento usa un conjunto de *tablas de enrutamiento* (routing tables) para dirigir el envío de los paquetes de datos desde su origen hasta su destino, a menudo usando muchos nodos intermedios conocidos como *encaminadores* o «routers». El encaminamiento IP es la forma principal de descubrir caminos dentro de Internet. Hay dos formas básicas de encaminamiento IP: *encaminamiento estático* y *encaminamiento dinámico*.

El encaminamiento estático supone añadir manualmente las rutas IP en la tabla de encaminamiento del sistema, y esto se hace normalmente manipulando la tabla de encaminamiento con la orden route. El encaminamiento estático tiene muchas ventajas sobre el encaminamiento dinámico, como la simplicidad de implementación sobre redes pequeñas, la predecibilidad (la tabla de encaminamiento siempre se calcula por adelantado, y por tanto la ruta siempre es la misma cada vez que se usa), y la baja sobrecarga en otros routers y enlaces de red por la inexistencia de un protocolo de encaminamiento dinámico. Sin embargo, el encaminamiento estático también presenta algunos inconvenientes. Por ejemplo, está limitado a redes pequeñas y no escala adecuadamente. El encaminamiento estático también fracasa completamente al intentar adaptarse a pérdidas de la red y a fallos a lo largo de la ruta debido a la naturaleza inmutable de la misma.

El encaminamiento dinámico depende de redes grandes con muchas rutas IP posibles desde un origen hacia un destino, y hace uso de protocolos especiales de encaminamiento, como el Protocolo de Información del Router (Router Information Protocol, RIP), que gestina los ajustes automáticos en las tablas de encaminamiento que hacen posible el encaminamiento dinámico. El encaminamiento dinámico tiene varias ventajas sobre el encaminamiento

estático, como su superior escalabilidad y la capacidad de adaptarse a los fallos y las pérdidas producidos a lo largo de las rutas de la red. Además, tiene una configuración menos manual de las tablas de encaminamiento, puesto que los routers aprenden unos de otros sobre la existencia y la disponibilidad de las rutas. Esta característica también elimina la posibilidad de introducir fallos en las tablas de encaminamiento provocadas por un error humano. El encaminamiento dinámico no es perfecto, sin embargo, y presenta inconvenientes como su mayor complejidad y la sobrecarga adicional de la red debida a las comunicaciones entre los routers, que no benefician inmediatamente a los usuarios finales, y que además consume ancho de banda de la red.

2.4. TCP y UDP

El TCP es un protocolo orientado a conexión, que ofrece corrección de errores y garantiza la entrega de los datos mediante el denominado *control de flujo*. El control de flujo determina cuándo se tiene que parar el flujo de una corriente de datos, y cuándo se deben reenviar los datos enviados previamente debido a problemas tales como *colisiones*, por ejemplo, asegurando así la entrega completa y precisa de los datos. El TCP se usa habitualmente en el intercambio de información importante, como transacciones de bases de datos.

El Protocolo de Datagramas de Usuario (User Datagram Protocol, UDP), por otro lado, es un protocolo *sin conexión* que raramente se usa en la transmisión ed datos importantes ya que carece de control de flujo o de cualquier otro método para garantizar la fiabilidad en la entrega de los datos. El UDP se usa habitualmente en aplicaciones de «streaming» de audio y vídeo, donde resulta considerablemente más rápido que el TCP por carecer de corrección de errores y control de flujo, y donde la pérdida de unos cuantos paquetes no suele resultar catastrófico.

2.5. ICMP

El Protocolo de Mensajería de Control de Internet (Internet Control Messaging Protocol, ICMP), es una extensión del Protocolo de Internet (Internet Protocol, IP) definida en el documento Request For Comments (RFC) #792, y que soporta paquetes de red que contienen mensajes de control, error e información. El ICMP se usa en aplicaciones de red como la utilidad ping, que comprueba la disponibilidad de un host o dispositivo en la red. Como ejemplos de mensajes error devueltos por el ICMP que resultan de utilidad en hosts de red y dispositivos como routers, tenemos *Destination Unreachable* (Destino Inalcanzable) y *Time Exceeded* (Tiempo Excedido).

2.6. Demonios

Los demonios (daemons) son aplicaciones especiales del sistema que normalmente se ejecutan continuamente en segundo plano esperando peticiones provenientes de otras aplicaciones que deseen usar las funciones que proporcionan. Muchos demonios están

centrados en la red; es decir, muchos de los demonios que se ejecutan en segundo plano en un sistema Ubuntu pueden proporcionar funcionalidades relacionadas con la red. Algunos ejemplos de tales demonios de red incluyen el *demonio de protocolo de transporte de hipertexto* (httpd), que proporciona funcionalidades de servidor web; el *demonio de intérprete seguro* (sshd), que proporciona capacidades seguras de sesiones interactivas remotas y transferencia de archivos; y el *demonio de protocolo de acceso a mensajes de Internet* (imapd), que proporcona servicios de correo electrónico.

3. Configuración del Cortafuegos

El kernel Linux incluye el subsistema *Netfilter* , que es usado para manipular o decidir el destino del tráfico de red entre o a través de su red. Todas las soluciones firewall Linux modernas utilizan este sistema para el filtrado de paquetes.

3.1. Introducción al Cortafuegos

El sistema de filtrado de paquetes del kernet sirve de ayuda a los administradores sin interface de usuario para manejarlo. Este es el proposito de iptables. Cuando un paquete llegue a su servidor, será manejado por el subsistema Netfilter para aceptarlo, manipularlo, o rechazarlo basandose en las reglas suministradas a este via iptables. Así, iptables es todo lo que necesita para manejar su cortafuegos si está familiarizado con el, pero existen muchos interfaces de usuario disponibles para simplificar esta tarea.

3.2. Enmascaramiento IP

El propósito del Enmascaramiento IP (IP Masquerading) es permitir que máquinas con direcciones IP privadas no enrutables de una red accedan a Internet a través de la máquina que realiza el enmascaramiento. Se debe manipular el tráfico que va de su red privada con destino a Internet, para que las respuestas puedan encaminarse adecuadamente a la máquina que hizo la petición. Para ello, el núcleo debe modificar la dirección IP *fuente* de cada paquete de forma que las respuestas se encaminen hacia ella, en lugar de encaminarla hacia la dirección IP privada que hizo la petición, lo que resulta imposible en Internet. Linux usa Seguimiento de Conexión (*Connection Tracking, conntrack)* para llevar la cuenta de qué conexiones pertenencen a qué máquinas, y reencaminar adecuadamente cada paquete de retorno. El tráfico que sale de su red privada es, por consiguiente, «enmascarada» dando la sensación de que se ha originado en la máquina Ubuntu que hace de pasarela. Este proceso se denomina Compartición de Conexiones de Internet (Internet Connection Sharing) en la documentación de Microsoft.

Esto se puede conseguir con una sóla regla de iptables, que puede variar ligeramente en función de la configuración de su red:

```
sudo iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o ppp0 -j MASQUERADE
```

La orden anterior supone que su espacio de direcciones privadas es 192.168.0.0/16 y que el dispositivo que conecta con Internet es ppp0. La sintaxis se descompone de la siguiente forma:

- -t nat -- la regla es para ir a la tabla nat
- -A POSTROUTING -- la regla es para añadir (-A) a la cadena POSTROUTING
- -s 192.168.0.0/16 -- la regla se aplica al tráfico originado desde la dirección específica
- -o ppp0 -- la regla se aplica al tráfico programado para ser enrutado a través del dispositivo de red especificado

- -j MASQUERADE -- el tráfico que se ajuste a esta regla «saltará» («jump», -j) al destino MASQUERADE para ser manipulado como se describió anteriormente

Cada cadena en la tabla de filtrado (la tabla predeterminada, y donde ocurren la mayoría de los filtrados de paquetes) tiene una *política* predeterminada de ACCEPT, pero si está creando un firewall además de un dispositivo de pasarela, debería establecer las políticas a DROP o REJECT, en cuyo caso necesitará habilitar su tráfico enmascarado a través de la cadena FORWARD para que la regla anterior funcione:

```
sudo iptables -A FORWARD -s 192.168.0.0/16 -o ppp0 -j ACCEPT
sudo iptables -A FORWARD -d 192.168.0.0/16 -m state --state ESTABLISHED,RELATED -i ppp0 -j
```

Las órdenes anteriores permitirán todas las conexiones que vayan de su red local a Internet, así como el retorno a la máquina que las inició de todo el tráfico relacionado con esas conexiones.

3.3. Herramientas

Hay muchas herramientas disponibles que pueden ayudarle a construir un completo firewall sin necesidad de conocer iptables en profundidad. Para los que se inclinan por una solución gráfica, Firestarter es muy popular y fácil de usar, y fwbuilder es muy potente y tiene un aspecto familiar para aquellos administradores que hayan usado herramientas comerciales de firewall como Checkpoint FireWall-1. Si prefiere una utilidad de línea de órdenes con archivos de configuración en texto plano, Shorewall es una solución muy potente para ayudarle a configurar un firewall avanzado para cualquier red. Si su red es relativamente simple, o no dispone de red, ipkungfu le proporcionará un firewall funcional con desde el principio sin necesidad de configuración, y le permitirá crear fácilmente un firewall más avanzado editando archivos de configuración sencillos y bien documentados. Otra herramienta interesante es fireflier, diseñado para ser una aplicación firewall de escritorio. Está formada por un servidor (fireflier-server) y una selección de clientes GUI (GTK o QT), y se comporta de manera muy similar a muchas aplicaciones interactivas de firewall para Windows.

3.4. Logs

Los registros del firewall son esenciales para reconocer ataques, corregir problemas en las reglas de su firewall, y observar actividades inusuales en su red. Debe incluir reglas de registro en su firewall para poder activarlos, y las reglas de registro deben aparecer antes de cualquier otra regla final aplicable (una regla con un objetivo que decide el destino del paquete, como ACCEPT, DROP o REJECT). Por ejemplo,

```
sudo iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j LOG --log-prefix "NEW_HTT
```

Una petición al puerto 80 desde la máquina local, por tanto, podría generar un registro en dmesg con el siguiente aspecto:

```
[4304885.870000] NEW_HTTP_CONN: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 S
```

El registro anterior también aparecerá en `/var/log/messages`, `/var/log/syslog` y `/var/log/kern.log`. Este comportamiento se puede cambiar editando apropiadamente el archivo `/etc/syslog.conf`, o instalando y configurando ulogd y utilizando el objetivo ULOG en lugar del LOG. El demonio ulogd es un servidor en espacio de usuario, que escucha las instrucciones de registro que provienen del núcleo y que sean específicamente para firewalls, y puede registrar cualquier archivo que desee, o incluso a una base de datos PostgreSQL o MySQL. Se puede simplificar la interpretación del significado de los registros del firewall usando una herramienta de análisis de registros como fwanalog, fwlogwatch o lire.

4. Servidor OpenSSH

4.1. Introducción

Esta sección de la Guía de Servidores de Ubuntu introduce una potente colección de herramientas para el control remoto y la transferencia de datos de ordenadores en red, llamados *OpenSSH*. También pruede aprender algo sobre los parámetros de configuración posibles del servidor OpenSSH y como cambiarlos en un sistema Ubuntu.

OpenSSH es una versión libre del protocolo Secure Shell (SSH) que es una familia de herramientas para control remoto o transferencia de ficheros entre ordenadores. Las herramientas utilizadas para realizar estas funciones, eran el telnet o el rcp, que son inseguras y transmiten el password de los usuarios en texto plano cuando son usadas. OpenSSH provee un demonio y clientes para facilitar un seguro y encriptado control remoto y operaciones de transferencia de fichero, reemplaza efectivamente las herramientas heredadas.

El componente servidor OpenSSH , sshd, escucha continuamente a la espera de conexiones de clientes desde cualquiera de las herramientas cliente. Cuando aparece una petición conexión, sshd establece la conexión correcta dependiendo del tipo de herramienta cliente que está conectándose. Por ejemplo, si el equipo remoto se está conectando con la aplicación cliente ssh, el servidor OpenSSH establecerá una sesión de control remoto tras la autenticación. Si el usuario remoto se conecta al servidor OpenSSH con scp, el demonio del servidor OpenSSH iniciará una copia segura de archivos entre el servidor y el cliente tras la autenticación. OpenSSH puede usar muchos métodos de autenticación, incluyendo contraseñas planas, claves públicas y tickets de Kerberos

4.2. Instalación

La instalación de cliente y servidor OpenSSH es simple. Para instalar las aplicaciones cliente de OpenSSH en su sistema ubuntu, use el siguiente comando en la línea de comandos:

```
sudo apt-get install openssh-client
```

Para instalar la aplicación servidor de OpenSSH, y los archivos de soporte relacionados, use en una línea de comandos la siguiente instrucción:

```
sudo apt-get install openssh-server
```

4.3. Configuración

Puede configurar el comportamiento predeterminado del servidor OpenSSH, sshd, editando el archivo `/etc/ssh/sshd_config`. Para más información sobre las directivas

de configuración usadas en este archivo, puede ver la página del manual apropiada con la siguiente orden, introducida en una terminal:

```
man sshd_config
```

Existen muchas directivas en el archivo de configuración de sshd que controlan cosas como los parámetros de comunicaciones y modos de autentificación. Los siguientes son ejemplos de directivas de configuración que pueden ser cambiadas editando el archivo `/etc/ssh/ssh_config` .

Antes de cambiar el archivo de configuración, debe hacer una copia del archivo original y protegerlo contra escritura así tendrá la configuración original como referencia y podrá reusarla si es necesario.

Copie el archivo `/etc/ssh/sshd_config` y protejalo contra escritura con los siguientes comandos, introduzcalos en el prompt:

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
sudo chmod a-w /etc/ssh/sshd_config.original
```

Lo siguiente son ejemplos de directivas de configuración que usted puede cambiar:

- Para hacer que su OpenSSH escuche por el puerto TCP 2222 en lugar del puerto TCP 22 por defecto, cambie la directiva Port como sigue:

  Port 2222

- Para hacer que sshd permita credenciales de inicio de sesión basados en clave pública, simplemente añada o modifique la línea:

  PubkeyAuthentication yes

  en el archivo `/etc/ssh/sshd_config`, si está presente, asegúrese que la línea no está comentada.

- Para hacer que su servidor OpenSSH muestre el contenido del archivo `/etc/issue.net` como banner antes del login, simplemente añada o modifique la línea:

  Banner /etc/issue.net

  en el archivo `/etc/ssh/sshd_config`.

Después de hacer los cambios en el archivo `/etc/ssh/sshd_config`, guarde este, y reinicie el servidor sshd para que los cambios tengan efecto usando la siguiente orden en una terminal:

```
sudo /etc/init.d/ssh restart
```

Existen muchas otras directivas de configuración disponibles para sshd que cambian el comportamiento de la aplicación servidor para ajustarlo a sus necesidades. No obstante, si su único método de acceso a un servidor es ssh, y comete un error al configurar sshd por medio del archivo `/etc/ssh/sshd_config`, puede conseguir que el servidor se cierre durante el reinicio del mismo, o que el servidor sshd no quiera iniciarse debido a una directiva de configuración incorrecta, por lo que debe ser extremadamente cuidadoso cuando edite este fichero desde un servidor remoto.

4.4. Referencias

Sitio web de OpenSSH [http://www.openssh.org/]

Página Wiki Avanzada de OpenSSH [https://wiki.ubuntu.com/AdvancedOpenSSH]

5. Servidor FTP

El Protocolo de Transferencia de Archivos (FTP) es un protocolo TCP para subir y descargar archivos entre ordenadores. El FTP funciona con el modelo cliente/servidor. El componente servidor es llamado *demonio FTP*. Está continuamente escuchando peticiones FTP de clientes remotos. Cuando se recibe una petición, gestiona la creación de la sesión y establece la conexión. Durante la duración de la sesión ejecuta las órdenes enviadas por el cliente FTP.

El acceso a un servidor FTP puede hacerse de dos maneras:

- Anónimo
- Autenticado

En el modo Anónimo, los clientes remotos pueden acceder al servidor FTP usando la cuenta de usuario por defecto llamada «anonymous» o "ftp" y enviando una dirección de correo como contraseña. En el modo Autenticado los usuario deben poseer una cuenta y su contraseña. El acceso del usuario a los directorios u ficheros del servidor FTP dependerá de los permisos definidos para la cuenta utilizada. Como regla general, el demonio FTP oculta el directorio raíz del servidor FTP y lo cambia por el directorio de inicio del FTP. Esto oculta el resto del sistema de archivos en las sesiones remotas.

5.1. vsftpd - Instalación del Servidor FTP

vsftpd es un demonio FTP disponible en Ubuntu. Es fácil de intalar, configurar y mantener. Para instalar vsftpd puede ejecutar el siguiente comando:

```
sudo apt-get install vsftpd
```

5.2. vsftpd - Configuración del Servidor FTP

You can edit the vsftpd configuration file, `/etc/vsftpd.conf`, to change the default settings. By default only anonymous FTP is allowed. If you wish to disable this option, you should change the following line:

```
anonymous_enable=YES
```

to

```
anonymous_enable=NO
```

By default, local system users are not allowed to login to FTP server. To change this setting, you should uncomment the following line:

```
#local_enable=YES
```

By default, users are allowed to download files from FTP server. They are not allowed to upload files to FTP server. To change this setting, you should uncomment the following line:

```
#write_enable=YES
```

Similarly, by default, the anonymous users are not allowed to upload files to FTP server. To change this setting, you should uncomment the following line:

```
#anon_upload_enable=YES
```

The configuration file consists of many configuration parameters. The information about each parameter is available in the configuration file. Alternatively, you can refer to the man page, **man 5 vsftpd.conf** for details of each parameter.

Una vez que haya configurado vsftpd puede ejecutar el demonio. Puede ejecutar el siguiente comando para lanzar el demonio vsftpd :

```
sudo /etc/init.d/vsftpd start
```

Por favor note que las configuración por defecto del archivo de configuración estan así por razones de seguridad. Cada uno de los cambios de arriba hacen el sistema un poco menos seguro, por lo tanto haga estos cambios solo si son necesarios.

6. Network File System (NFS)

NFS permite a un sistema compartir directorios y archivos con otros sistemas a través de la red. Usando NFS, los usuarios y los programas pueden acceder a archivos en sistemas remotos casi como si fueran archivos locales.

Algunos de los beneficios más notables que el NFS suministra son:

- Las estaciones de trabajo locales utilizan menos espacio en disco porque los datos usados de forma común pueden ser guardados en una sola máquina y permanecerán accesibles a todas las de la red.
- No es necesario que los usuarios tengan directorios de inicio separados en cada máquina de la red. Los directorios de inicio pueden estar configurados en un servidor NFS y estar disponibles a través de la red.
- Los dispositivos de almacenamiento como disquetes, unidades de CDROM, y dispositivos USB pueden ser usados por otras máquinas a través de la red. Esto reduce el número de dispositivos removibles en la red.

6.1. Instalación

Ejecute la siguiente orden en una terminal para instalar el Servidor NFS:

```
sudo apt-get install nfs-kernel-server
```

6.2. Configuración

Puede configurar los directorios a exportar añadiendolos al archivo `/etc/exports` . Por ejemplo:

```
/ubuntu *(ro,sync,no_root_squash)
/home *(rw,sync,no_root_squash)
```

Puede reemplazar * con uno de los formatos de nombres de máquina. Haciendo la declaración del nombre de máquina tan específica como sea posible para evitar que sistemas no deseados accedan al punto de montaje NFS.

Para iniciar el servidor NFS, ejecute la siguiente orden en una terminal:

```
sudo /etc/init.d/nfs-kernel-server start
```

6.3. Configuración del cliente NFS

Use la orden mount para montar directorios NFS compartidos por otra máquina, tecleando una orden similar a ésta en la terminal:

```
sudo mount ejemplo.hostname.com:/ubuntu /local/ubuntu
```

El directorio del punto de montaje `/local/ubuntu` debe existir. No deben haber archivos ni directorios dentro de `/local/ubuntu`.

Una forma alternativa de montar un recurso compartido desde otra máquina es añadiendo una línea en el archivo `/etc/fstab` . La línea debe contener el nombre de máquina del servidor NFS, el directorio que esta siendo exportado en el servidor, y el directorio en la máquina local donde el recurso NFS será montado.

La sintaxis general para el archivo `/etc/fstab` es la siguiente:

```
example.hostname.com:/ubuntu /local/ubuntu nfs rsize=8192,wsize=8192,timeo=14,intr
```

6.4. Referencias

FAQ de NFS en Linux [http://nfs.sourceforge.net/]

7. Dynamic Host Configuration Protocol (DHCP)

El Protocolo de Configuración Dinámica de Hosts (DHCP, en inglés), es un servicio de red que permite que los ordenadores hosts sean configurados automáticamente desde un servidor en lugar de tener que configurar manualmente cada host de la red. Los ordenadores configurados para ser clientes DHCP no tienen control sobre la configuración que reciben del servidor DHCP, y la configuración es transparente para el usuario del ordenador.

Las opciones de configuración más comunes suministradas por un servidor DHCP a los clientes DHCP incluyen:

- Dirección IP y máscara de red
- DNS
- WINS

Además, un servidor DHCP puede suministrar propiedades de configuración como:

- Nombre del host
- Nombre de dominio
- Puerta de enlace predeterminada
- Servidor horario
- Servidor de impresión

La ventaja de usar DHCP es que un cambio en la red (por ejemplo, un cambio en la dirección del servidor DNS), sólo supone un cambio en el servidor DHCP, ya que todos los hosts de la red se reconfigurarán automáticamente la próxima vez que sus clientes DHCP soliciten la configuración al servidor DHCP. Como una ventaja añadida, también es más fácil integrar nuevos ordenadores en la red, ya que no es necesario comprobar la disponibilidad de la dirección IP. Los conflictos de direcciones IP también se reducen.

Un servidor DHCP puede proporcionar parámetros de configuración usando dos métodos:

Dirección MAC
: Este método supone el uso de DHCP para identificar el hardware único de cada tarjeta de red conectada a la red y continuar suministrando una configuración constante cada vez que el cliente DHCP hace una petición usando ese dispositivo de red.

Depósito de direcciones
: Este método define un depósito (también llamado a veces rango o ámbito) de direcciones IP que serán suministradas a los clientes DHCP de forma dinámica como parte de sus opciones de configuración, y en una política de «primero en llegar, primero en ser servido». Cuando un cliente DHCP deja de estar en la red durante un periodo de tiempo especificado, la configuración expira y retorna al depósito de direcciones para que pueda ser utilizada por otros clientes DHCP.

Ubuntu viene equipado con un cliente DHCP y un servidor DHCP. El servidor es dhcpd (dynamic host configuration protocol daemon). El cliente suministrado por Ubuntu es dhclient y se debe instalar en los equipos que necesiten ser configurados automáticamente. Ambos programas son fáciles de instalar y de configurar, y deberían iniciarse automáticamente durante el arranque del sistema.

7.1. Instalación

En un terminal, introduzca el siguiente comando para instalar el dhcpd:

```
sudo apt-get install dhcpd
```

Usted podrá ver la siguiente salida, que explica que hacer después:

```
Por favor, tenga en cuenta que si está instalando el servidor DHCP por
primera vez, necesitará configurarlo. Por favor, detenga el demonio
del servidor DHCP (/etc/init.d/dhcp stop), edite /etc/dhcpd.conf para
adaptarlo a sus necesidades, y reinice el demonio del servidor DHCP
(/etc/init.d/dhcp start).

También necesitará editar /etc/default/dhcp para especificar las
interfaces que dhcpd deberá escuchar. De forma predeterminada,
escucha en eth0.

NOTA: Los mensajes de dhcpd se enviarán a syslog. Localice allí los
mensajes de diagnóstico.

Starting DHCP server: dhcpd failed to start - check syslog for diagnostics.
```

7.2. Configuración

El mensaje final de error de la instalación puede resultar un poco confuso, pero los siguientes pasos pueden ayudarle a configurar el servicio:

Lo más común, que usted quisiera hacer es asignar una dirección IP de forma aleatoria. Esto puede ser hecho con las siguientes configuraciones:

```
# Sample /etc/dhcpd.conf
# (add your comments here)
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "mydomain.org";

subnet 192.168.1.0 netmask 255.255.255.0 {
```

```
range 192.168.1.10 192.168.1.100;
range 192.168.1.150 192.168.1.200;
}
```

Esto hará que el servidor DHCP proporcione a un cliente una dirección IP dentro del rango 192.168.1.10 - 192.168.1.100 ó 192.168.1.150 - 192.168.1.200. La concesión de la dirección IP durará 600 segundos, si el cliente no ha solicitado un intervalo de tiempo específico. En caso contrario, la concesión máxima permitida será de 7200 segundos. El servidor también «aconsejará» al cliente que use 255.255.255.0 como su máscara de subred, 192.168.1.255 como su dirección de difusión, 192.168.1.254 como la dirección del router/pasarela, y 192.168.1.1 y 192.168.1.2 como sus servidores DNS.

Si necesita especificar un servidor WINS para sus clientes Windows, necesitará incluir la opción netbios-name-servers option, p.e.

```
option netbios-name-servers 192.168.1.1;
```

Los parámetros de configuración de dhcpd son tomados del DHCP mini-HOWTO, que se puede encontrar *aquí* [http://www.tldp.org/HOWTO/DHCP/index.html].

7.3. Referencias

FAQ de DHCP [http://www.dhcp-handbook.com/dhcp_faq.html]

8. Servicio de nombre de dominio (DNS)

El Servicio de Nombres de Dominio (Domain Name Service, DNS) es un servicio de Internet que hace corresponder direcciones IP con nombres de dominio totalmente cualificados (FQDN). De esta forma, DNS nos evita tener que recordar direcciones IP. Los ordenadores que relizan DNS se denominan *servidores de nombres*. Ubuntu viene equipado con BIND (Berkley Internet Naming Daemon, Demonio de Nombres de Internet de Berkley), el programa usado más comúnmente para gestionar un servidor de nombres en GNU/Linux.

8.1. Instalación

En un terminal, introduzca el siguiente comando para instalar dns:

```
sudo apt-get install bind
```

8.2. Configuración

Los archivos de configuración del DNS están guardados en el directorio `/etc/bind` . El archivo de configuración principal es `/etc/bind/named.conf`. El contenido del archivo de configuración por defecto se muestra debajo:

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind/README.Debian for information on the
// structure of BIND configuration files in Debian for BIND versions 8.2.1
// and later, *BEFORE* you customize this configuration file.
//

include "/etc/bind/named.conf.options";

// reduce log verbosity on issues outside our control#
logging {
 category lame-servers { null; };
 category cname { null; };
};

// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
```

```
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

// add local zone definitions here
include "/etc/bind/named.conf.local";
```

La línea include especifica el archivo que contiene las opciones del DNS. La línea directory en el archivo de opciones de dice al DNS donde buscar los archivos. Todos los archivos usados por BIND serán relativos a ese directorio.

El fichero llamado `/etc/bind/db.root` describe los servidores de nombres raiz en el mundo. Los servidores cambian con el tiempo y deben de ser mantenidos.

The zone section defines a master server, and it is stored in a file mentioned against file tag. Every zone file contains 3 resource records (RRs): an SOA RR, an NS RR and a PTR RR. SOA is short of Start of Authority. The "@" is a special notation meaning the origin. NS is the Name Server RR. PTR is Domain Name Pointer. To start the DNS server, run the following command from a terminal prompt:

```
sudo /etc/init.d/bind start
```

Para más detalles puede accedar a la documentación mencionada en la sección de referencias.

8.3. Referencias

DNS HOWTO [http://www.tldp.org/HOWTO/DNS-HOWTO.html]

9. CUPS - Servidor de Impresión

El mecanismo principal de impresión y de servicios de impresión en Ubuntu es el *Sistema de Impresión Común de UNIX* (Common UNIX Printing System, CUPS). Este sistema de impresión es una capa de impresión libre y portable que se ha convertido en el nuevo estándar de impresión en la mayoría de las distribuciones ed GNU/Linux.

CUPS gestiona los trabajos y tareas de impresión, y proporciona impresión de red utilizando el Protocolo estándar de Impresión en Internet (IPP), que dispone de soporte para una gran gama de impresoras, desde matriciales hasta láser. CUPS también soporta PostScript Printer Description (PPD) y autodetección de impresoras de red, y dispone de una sencilla herramienta basada en web para la configuración y administración.

9.1. Instalación

Para instalar CUPS en su equipo Ubuntu, simplemente use sudo con la orden apt-get y proporcione como primer parámtro el nombre de los paquetes a instalar. Una instalación completa de CUPS tiene muchas dependencias de paquetes, pero pueden especificarse todas ellas en la misma línea de órdenes. Introduzca lo siguiente en la línea de órdenes de una terminal para instalar CUPS:

```
sudo apt-get install cupsys cupsys-client
```

Tras autenticarse con su contraseña de usuario, los paquetes se descargarán y se instalarán sin errores. Tras finalizar la instalación, el servidor CUPS se iniciará automáticamente. Con el propósito de ayudar a la resolución de posibles problemas, puede acceder a los errores del servidor CUPS consultando el archivo de registro de errores en: `/var/log/cups/error_log`. Si el registro de errores no mostrara información suficiente para resolver los problemas encontrados, se podría incrementar el detalle del registro de CUPS cambiando la directiva **LogLevel** en el archivo de configuración (como se indicó antes) del valor predeterminado «info» al valor «debug», o incluso «debug2», lo que registrará todo. Si hace este cambio, recuerde volverlo a su valor original una vez haya resuelto su problem, para evitar que el archivo de registro crezca demasiado.

9.2. Configuración

El comportamiento del servidor CUPS se configura a través de las directivas contenidas en el archivo `/etc/cups/cupsd.conf`. El archivo de configuración de CUPS tiene la misma sintaxis que el archivo principal de configuración del servidor HTTP Apache, por lo que los usuarios acostumbrados a editar el archivo de configuración de Apache se sentirán como en su casa cuando editen el archivo de configuración de CUPS. Se presentarán aquí algunos ejemplos de opciones que usted puede desear cambiar inicialmente.

Antes de editar un fichero de configuración, debe hacer una copia del archivo original y protegerla contra escritura, así tendrá la configuración original como referencia, y podrá reusarla si fuera necesario.

Copie el archivo `/etc/cups/cupsd.conf` y protejalo contra escritura con los siguientes comandos, introduzcalos en un terminal:

```
sudo cp /etc/cups/cupsd.conf /etc/cups/cupsd.conf.original
sudo chmod a-w /etc/cups/cupsd.conf.original
```

- **ServerAdmin**: To configure the email address of the designated administrator of the CUPS server, simply edit the `/etc/cups/cupsd.conf` configuration file with your preferred text editor, and modify the *ServerAdmin* line accordingly. For example, if you are the Administrator for the CUPS server, and your e-mail address is 'bjoy@somebigco.com', then you would modify the ServerAdmin line to appear as such:

  ```
  ServerAdmin bjoy@somebigco.com
  ```

Para más ejemplos de directivas de configuración en el archivo de configuración del servidor CUPS, vea la página de manual asociada introduciendo el siguiente comando en un terminal:

```
man cupsd.conf
```

Una vez haya realizado cambios en el archivo de configuración `/etc/cups/cupsd.conf`, necesitará reiniciar el servidor CUPS tecleando la siguiente orden en la línea de órdenes de una terminal:

```
sudo /etc/init.d/cupsys restart
```

Otras opciones de configuración para el servidor CUPS se encuentran en el archivo `/etc/cups/cups.d/ports.conf`:

- **Listen**: De forma predeterminada, en Ubuntu la instalación del servidor CUPS escucha sólo por la interfaz loopback en la dirección IP *127.0.0.1*. Para hacer que el servidor CUPS escuche en la dirección IP del verdadero adaptador de red, debe especificar un nombre de host, una dirección IP, o bien, un par dirección IP/puerto, y para ello debe añadir una directiva Listen. Por ejemplo, si su servidor CUPS reside en una red local con la dirección IP *192.168.10.250* y desea que sea accesible para los demás sistemas de esta subred, debe editar el archivo `/etc/cups/cups.d/ports.conf` y añadir una directiva Listen, de esta forma:

  ```
  Listen 127.0.0.1:631 # existing loopback Listen
  Listen /var/run/cups/cups.sock # existing socket Listen
  ```

```
Listen 192.168.10.250:631 # Listen on the LAN interface, Port 631 (IPP)
```

En el ejemplo anterior, debe comentar o borrar la referencia a la dirección de loopback (127.0.0.1) si no desea que cupsd escuche por esa interfaz, sino sólo por la interfaz Ethernet de la red local (LAN). Para activar la escucha por todas las interfases de red en las que se haya establecido un nombre de host, incluyendo el loopback, debería crear una entrada listen para el nombre de host *socrates* así:

```
Listen·socrates:631··#·Escuchando en todos los interfaces para la máquina·'socrates'
```

o omitiendo la directiva Listen y usando *Port* en su lugar, como en:

```
Port 631 # Escuchando en el puerto 631 en todos los interfaces
```

9.3. Referencias

Sitio Web de CUPS [http://www.cups.org/]

10. HTTPD - Servidor Web Apache2

Apache es el Servidor Web mas comunmente utilizado en sistemas GNU/Linux. Los Servidores Web son usados para servir Páginas Web solicitadas por ordenadores clientes. Los clientes típicamente solicitan ver Páginas Web usando un Navegador como Firefox, Opera, o Mozilla.

Los usuarios introducen un Localizador de Recursos Uniforme (Uniform Resource Locator, URL) para señalar a un servidor web por medio de su Nombre de Dominio Totalmente Cualificado (Fully Qualified Domain Name, FQDN) y de una ruta al recurso solicitado. Por ejemplo, para ver la página web del *sitio web de Ubuntu* [http://www.ubuntu.com], un usuario debería introducir únicamente el FQDN. Para solicitar información específica acerca del *soporte de pago* [http://www.ubuntu.com/support/supportoptions/paidsupport], un usuario deberá introducir el FQDN seguido de una ruta.

El protocolo más comunmente utilizado para ver páginas Web es el Hyper Text Transfer Protocol (HTTP). Protocolos como el Hyper Text Transfer Protocol sobre Secure Sockets Layer (HTTPS), y File Transfer Protocol (FTP), un protocolo para subir y descargar archivos, también son soportados.

Los servidores web Apache a menudo se usan en combinación con el motor de bases de datos MySQL, el lenguaje de scripting PHP, y otros lenguajes de scripting populares como Python y Perl. Esta configuración se denomina LAMP (Linux, Apache, MySQL y Perl/Python/PHP) y conforma una potente y robusta plataforma para el desarrollo y distribución de aplicaciones basadas en la web.

10.1. Instalación

El servidor web Apache2 esta disponible en Ubuntu Linux. Para instalar Apache2:

- Introduzca el siguiente comando en un terminal:

```
#
sudo apt-get install apache2#
```

10.2. Configuración

Apache se configura colocando *directivas* en archivos de configuración de texto plano. El archivo principal de configuración se llama `apache2.conf`. Además, se pueden añadir otros archivos de configuración mediante la directiva *Include*, y se pueden usar comodines para incluir muchos archivos de configuración. Todas las directivas deben colocarse en alguno de esos archivos de configuración. Apache2 sólo reconocerá los cambios realizados en los archivos principales de configuración cuando se inicie o se reinicie.

El servidor también lee un fichero que contiene los tipos mime de los documentos; el nombre de ese fichero lo establece la directiva *TypesConfig*, y es `mime.types` por omisión.

El archivo de configuración predeterminado de Apache2 es `/etc/apache2/apache2.conf`. Puede editar este archivo para configurar el servidor Apache2. Podrá configurar el número de puerto, la raíz de documentos, los módulos, los archivos de registros, los hosts virtuales, etc.

10.2.1. Opciones básicas

Esta sección explica los parámetros de configuración esenciales para el servidor Apache2. Remitase a la *Documentación de Apache2 Documentation* [http://httpd.apache.org/docs/2.0/] para más detalles.

- Apache2 ships with a virtual-host-friendly default configuration. That is, it is configured with a single default virtual host (using the *VirtualHost* directive) which can modified or used as-is if you have a single site, or used as a template for additional virtual hosts if you have multiple sites. If left alone, the default virtual host will serve as your default site, or the site users will see if the URL they enter does not match the *ServerName* directive of any of your custom sites. To modify the default virtual host, edit the file `/etc/apache2/sites-available/default`. If you wish to configure a new virtual host or site, copy that file into the same directory with a name you choose. For example, **sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/mynewsite** Edit the new file to configure the new site using some of the directives described below.
- La directiva *ServerAdmin* especifica la dirección de correo del administrador del servidor. El valor por omisión es webmaster@localhost. Cambie esta dirección por alguna a la que le puedan llegar los mensajes que se le envíen (si ud. es el administrador del servicio). Si su sitio web tiene algún problema, Apache2 mostrará un mensaje de error con en la que aparecerá esta dirección de correo para que la gente pueda enviar un informe del error. La directiva se encuentra en el fichero de configuración de su sitio en /etc/apache2/sites-available.
- The *Listen* directive specifies the port, and optionally the IP address, Apache2 should listen on. If the IP address is not specified, Apache2 will listen on all IP addresses assigned to the machine it runs on. The default value for the Listen directive is 80. Change this to 127.0.0.1:80 to cause Apache2 to listen only on your loopback interface so that it will not be available to the Internet, to (for example) 81 to change the port that it listens on, or leave it as is for normal operation. This directive can be found and changed in its own file, `/etc/apache2/ports.conf`
- The *ServerName* directive is optional and specifies what FQDN your site should answer to. The default virtual host has no ServerName directive specified, so it will respond to all requests that do not match a ServerName directive in another virtual host. If you have just acquired the domain name ubunturocks.com and wish to host it on your Ubuntu server, the value of the ServerName directive in your virtual host configuration file should be ubunturocks.com. Add this directive to the new virtual host file you created earlier (`/etc/apache2/sites-available/mynewsite`).

También puede desear que su sitio responda a www.ubunturocks.com, ya que muchos usuarios asumen que el prefijo www es apropiado. Para ello, use la directiva *ServerAlias*. Puede usar comodines en la directiva ServerAlias. Por ejemplo, **ServerAlias *.ubunturocks.com** hará que su sitio responda a cualquier solicitud de dominio que termine en .ubunturocks.com.

- La directiva *DocumentRoot* especifica dónde debe buscar Apache los archivos que forman el sitio. El valor predeterminado es /var/www. No hay ningún sitio configurado allí, pero si descomenta la directiva *RedirectMatch* en `/etc/apache2/apache2.conf`, las peticiones se redirigirán a /var/www/apache2-default, que es donde reside el sitio predeterminado de Apache2. Cambie este valor en el archivo de host virtual de su sitio, y recuerde crear ese directorio si fuese necesario.

Apache2 **no** procesa el directorio /etc/apache2/sites-available. Los enlaces simbólicos en /etc/apache2/sites-enabled apuntan a los sitios «disponibles». Use la utilidad a2ensite (Apache2 Enable Site) para crear esos enlaces simbólicos, así: **sudo a2ensite minuevositio** donde el archivo de cofiguración de su sitio es `/etc/apache2/sites-available/minuevositio`. Igualmente, se debe usar la utilidad a2dissite para deshabilitar sitios.

10.2.2. Opciones predeterminadas

Esta sección explica la configuración de las opciones predeterminadas del servidor Apache2. Por ejemplo, si desea añadir un host virtual, las opciones que usted configura para el host virtual tienen prioridad para ese host virtual. Para las directivas no definidas dentro de las opciones del host virtual, se usan los valores predeterminados.

- El *DirectoryIndex* es la página servida por defecto por el servidor cuando un usuario solicita el índice de un directorio añadiendo la barra de división (/) al final del nombre del directorio.

  For example, when a user requests the page http://www.example.com/this_directory/, he or she will get either the DirectoryIndex page if it exists, a server-generated directory list if it does not and the Indexes option is specified, or a Permission Denied page if neither is true. The server will try to find one of the files listed in the DirectoryIndex directive and will return the first one it finds. If it does not find any of these files and if Options Indexes is set for that directory, the server will generate and return a list, in HTML format, of the subdirectories and files in the directory. The default value, found in `/etc/apache2/apache2.conf` is " index.html index.cgi index.pl index.php index.xhtml". Thus, if Apache2 finds a file in a requested directory matching any of these names, the first will be displayed.

- The *ErrorDocument* directive allows you to specify a file for Apache to use for specific error events. For example, if a user requests a resource that does not exist, a 404 error will occur, and per Apache2's default configuration, the file

`/usr/share/apache2/error/HTTP_NOT_FOUND.html.var` will be displayed. That file is not in the server's DocumentRoot, but there is an Alias directive in `/etc/apache2/apache2.conf` that redirects requests to the /error directory to /usr/share/apache2/error/. To see a list of the default ErrorDocument directives, use this command: **grep ErrorDocument /etc/apache2/apache2.conf**

- By default, the server writes the transfer log to the file /var/log/apache2/access.log. You can change this on a per-site basis in your virtual host configuration files with the *CustomLog* directive, or omit it to accept the default, specified in `/etc/apache2/apache2.conf`. You may also specify the file to which errors are logged, via the *ErrorLog* directive, whose default is `/var/log/apache2/error.log`. These are kept separate from the transfer logs to aid in troubleshooting problems with your Apache2 server. You may also specify the *LogLevel* (the default value is "warn") and the *LogFormat* (see `/etc/apache2/apache2.conf` for the default value).
- Algunas opciones son especificadas por directorio en lugar de por servidor. Una de estas directivas es Option. Un parrafo Directory es encerrado entre etiquetas XML, como estas:

```
<Directory /var/www/mynewsite>#
    ...#
  </Directory>
```

La directiva Options dentro del parrafo Directory acepta un o más de los siguientes valores (entre otros), separados por espacios:

- **ExecCGI** - Permite la ejecución de scripts CGI. Los scripts CGI no serán ejecutados si esta opción no fue escojida.

  

  Muchos archivos no deberían ser ejecutados como scripts CGI. Esto podría resultar muy peligroso. Los scripts CGI deberían mantenerse en un directorio separado fuera de su DocumentRoot, y dicho directorio debería ser el único que tuviese activada la opción ExecCGI. Así está establecido desde el principio, y la ubicación predeterminada para los scripts CGI es /usr/lib/cgi-bin.
- **Includes** - Permite «server-side includes». Éstos, permiten a un fichero HTML *incluir* otros ficheros. No es una opción muy común, consulte el *Cómo - Apache2 SSI* [http://httpd.apache.org/docs/2.0/howto/ssi.html] para más información.
- **IncludesNOEXEC** - Permite «server-side includes», pero deshabilita los #exec y #include en los scripts CGI.
- **Indexes** - Muestra una lista formateada del contenido de los directorios, si no existe el DirectoryIndex (como el index.html) en el directorio solicitado.

  

  For security reasons, this should usually not be set, and certainly should not be set on your DocumentRoot directory. Enable this option carefully on a per-directory basis only if you are certain you want users to see the entire contents of the directory.

- **Multiview** - Support content-negotiated multiviews; this option is disabled by default for security reasons. See the *Apache2 documentation on this option* [http://httpd.apache.org/docs/2.0/mod/mod_negotiation.html#multiviews].
- **SymLinksIfOwnerMatch** - Solo seguirá enlaces simbólicos si el directorio de destino es del mismo usuario que el enlace.

10.2.3. Configuración de Servidores Virtuales

Virtual hosts allow you to run different servers for different IP addresses, different host names, or different ports on the same machine. For example, you can run the website for http://www.example.com and http://www.anotherexample.com on the same Web server using virtual hosts. This option corresponds to the <VirtualHost> directive for the default virtual host and IP-based virtual hosts. It corresponds to the <NameVirtualHost> directive for a name-based virtual host.

The directives set for a virtual host only apply to that particular virtual host. If a directive is set server-wide and not defined within the virtual host settings, the default setting is used. For example, you can define a Webmaster email address and not define individual email addresses for each virtual host.

Establezca la directiva DocumentRoot apuntando al directorio que contenga el documento raíz (como el index.html) para el host virtual. El DocumentRoot por defecto es `/var/www`.

La directiva ServerAdmin, dentro de una estrofa VirtualHost, es la dirección de correo usada en el pie de página de las páginas de error (si es que eligió mostrar un pie de página con la dirección de correo en las páginas de error).

10.2.4. Configuración del Servidor

Esta sección explica como configurar básicamente un servidor.

LockFile - The LockFile directive sets the path to the lockfile used when the server is compiled with either USE_FCNTL_SERIALIZED_ACCEPT or USE_FLOCK_SERIALIZED_ACCEPT. It must be stored on the local disk. It should be left to the default value unless the logs directory is located on an NFS share. If this is the case, the default value should be changed to a location on the local disk and to a directory that is readable only by root.

PidFile - The PidFile directive sets the file in which the server records its process ID (pid). This file should only be readable by root. In most cases, it should be left to the default value.

User - The User directive sets the userid used by the server to answer requests. This setting determines the server's access. Any files inaccessible to this user will also be inaccessible to your website's visitors. The default value for User is www-data.

Hasta que no sepa exactamente lo que esta haciendo, no ponga en la directiva User al root. Usar el root como usuario puede crear grandes agujeros de seguridad en su servidor Web.

La directiva Group es similar a la directiva User. Group establece el grupo sobre el que el servidor aceptará las peticiones. El grupo por defecto es también www-data.

10.2.5. Módulos de Apache

Apache es un servidor modular. Esto supone que en el núcleo del servidor sólo está incluida la funcionalidad más básica. Las características extendidas están disponibles a través de módulos que se pueden cargar en Apache. De forma predeterminada, durante la compilación se incluye un juego básico de módulos en el servidor. Si el servidor se compila para que use módulos cargables dinámicamente, los módulos se podrán compilar por separado y se podrán añadir posteriormente usando la directiva LoadModule. En caso contrario, habrá que recompilar Apache para añadir o quitar módulos. Ubuntu compila Apache2 para que permita la carga dinámica de módulos. Las directivas de configuración ser pueden incluir condicionalmente en base a la presencia de un módulo en particular, encerrándolas en un bloque <IfModule>. Puede instalar módulos adicionales de Apache2 y usarlos con su servidor web. Puede instalar los módulos de Apache2 usando la orden apt-get. Por ejemplo, para instalar el módulo de Apache2 que proporciona autenticación por MySQL, puede ejecutar lo siguiente en la línea de órdenes de una terminal:

```
sudo apt-get install libapache2-mod-auth-mysql
```

Una vez instalado el módulo, este estará disponible en el directorio `/etc/apache2/mods-available`. Puede utilizar el comando a2enmod para activar el módulo. Puede utilizar el comando a2dismod para desactivar el módulo. Una vez que active el módulo, este estará disponible en el directorio `/etc/apache2/mods-enabled`.

10.3. Configuración HTTPS

El módulo mod_ssl añade una importante característica al servidor Apache2 - la habilidad de encriptar las comunicaciones. De esta forma, cuando su navegador se esta comunicando utilizando la encriptación SSL, se utilizará el prefijo https:// al principio del Localizador de Recursos Uniformes (URL) en la barra de direcciones del navegador.

El módulo mod_ssl esta disponible en el paquete apache2-common. Si tiene instalado este paquete, podrá ejecutar el siguiente comando en un terminal para activar el módulo mod_ssl:

```
sudo a2enmod ssl
```

10.3.1. Certificados y Seguridad

Para configurar un servidor seguro, utilice criptografía de clave pública para crear un par de claves pública y privada. En la mayoría de los casos, usted envía su solicitud de certificado (incluyendo su clave pública), una prueba de la identidad de su compañía, y el pago correspondiente, a una Autoridad de Certificación (Certificate Authority, CA). La CA verifica la solicitud de certificado y su identidad, y posteriormente le envía un certificado para su servidor seguro.

También puede crear su propio certificado auto-firmado. Tenga en cuenta, no obstante, que los certificados auto-firmados no deben usarse en la mayoría de los entornos de producción. Los certificados auto-firmados no son aceptados automáticamente por los navegadores de los usuarios. Los navegadores solicitarán al usuario que acepte el certificado para crear la conexión segura.

Cuando tenga un certificado auto-firmado, o un certificado firmado por una CA de su elección, necesitará instalarlo en su servidor seguro.

10.3.2. Tipos de Certificados

Necesita una clave y un certificado para trabajar con su servidor seguro, lo que significa que deberá generar su propio certificado firmado por usted mismo, o comprar un certificado firmado por una CA. Un certificado firmado por una CA proporciona dos capacidades importantes para su servidor:

- Los navegadores (habitualmente) reconocen automáticamente el certificado y permiten establecer una conexión segura sin preguntar al usuario.
- Cuando una CA envía un certificado firmado, está garantizando la identidad de la organización que está suministrando las páginas web al navegador.

Muchos navegadores web que soportan SSL tienen una lista de CAs cuyos certificados aceptan automáticamente. Si un navegador encuentra un certificado autorizado por una CA que no está en su lista, el navegador le preguntará al usuario si desea aceptar o denegar la conexión.

Puede generar un certificado firmado por usted mismo para su servidor seguro, pero tenga en cuenta que un certificado auto-firmado no proporciona la misma funcionalidad que un certificado firmado por una CA. La mayoría de los navegadores web no reconocen automáticamente los certificados auto-firmados, y éstos además no proporcionan ninguna garantía acerca de la identidad de la organización que está proporcionando el sitio web. Un certificado firmado por una CA proporciona estas dos importantes características a un servidor seguro. El proceso para obtener un certificado de una CA es realmente fácil. A grandes rasgos, consta de:

1. Crear dos llaves encriptadas pública y privada.

2. Crear una solicitud de certificado basado en la clave pública. La solicitud de certificado contiene información sobre su servidor y la compañía que lo aloja.
3. Enviar la solicitud de certificado, junto con los documentos que prueban su identidad, a una CA. No podemos decirle qué autoridad de certificación elegir. Su decisión debe basarse en sus experiencias pasadas, o en las experiencias de sus amigos o colegas, o simplemente en factores económicos.

   Una vez se haya decidido por una CA, necesita seguir las instrucciones que ésta le proporcione para obtener un certificado proveniente de ella.
4. Cuando la CA esté segura de que tiene todo lo que necesita de usted, le enviará un certificado digital.
5. Instalar este certificado en su servidor seguro, y soportar transacciones seguras.

Cuando obtenga un certificado de una CA, o genere su propio certificado auto-firmado, el primer paso es generar una clave.

10.3.3. Generar una Petición de Firma de Certificado (Certificate Signing Request, CSR)

Para generar la Solicitud de Firma de Certificado (Certificate Signing Request, CSR), deberá crear su propia clave. Para ello, puede ejecutar la siguiente orden en la línea de órdenes de una terminal:

```
openssl genrsa -des3 -out server.key 1024
```

```
#
Generating RSA private key, 1024 bit long modulus#
.....................++++++#
.................++++++#
unable to write 'random state'#
e is 65537 (0x10001)#
Enter pass phrase for server.key:#
```

Ahora puede introducir su frase de paso. Para mayor seguridad, ésta debería contener, al menos, ocho caracteres. La longitud mínima al especificar -des3 es de cuatro caracteres. Debe incluir números y/o signos de puntuación, y no debería ser una palabra que se pudiera encontrar en un diccionario. Además, recuerde que su frase de paso distingue mayúsculas de minúsculas.

Vuelva a escribir la frase de paso para verificarla. Cuando la haya vuelto a escribir correctamente, se generará la clave del servidor y se almacenará en el archivo `server.key`.

También puede ejecutar su servidor web seguro sin una frase de paso. Esto puede ser conveniente porque así no tendrá que introducir la frase de paso cada vez que vaya a arrancar su servidor web seguro. Pero también resulta altamente inseguro y comprometer la clave significa también comprometer al servidor.

En todo caso, puede escoger ejecutar su servidor web seguro sin frase de paso quitando la opción -des3 en la fase de generación, o ejecutando la siguiente orden en una terminal:

```
openssl rsa -in server.key -out server.key.insecure
```

Una vez haya ejecutado la orden anterior, la clave insegura se almacenará en el archivo `server.key.insecure`. Puede usar este archivo para generar el CSR sin frase de paso.

Para crear el CSR, ejecute el siguiente comando en un terminal:

```
openssl req -new -key server.key -out server.csr
```

Se le pedirá que introduzca la frase de paso. Si la introduce correctamente, se le solicitará que introduzca el nombre de la empresa, el nombre del sitio, la dirección de correo electrónico, etc. Cuando haya introducido todos esos detalles, se creará su CSR y se almacenará en el archivo `server.csr`. Puede enviar ese archivo CSR a una AC para que lo procese. La AC usará ese archivo CSR y emitirá el certificado. Por otra parte, también puede crear un certificado auto-firmado usando este CSR.

10.3.4. Creación de un certificado auto-firmado

Para crear un certificado auto-firmado, ejecute la siguiente orden en una terminal:

```
openssl·x509·-req·-days·365·-in·server.csr·-signkey·server.key·-out·server.crt
```

La orden anterior le solicitará que introduzca la frase de paso. Cuando la haya introducido, se creará su certificado y se almacenará en el archivo `server.crt`.

Si su servidor seguro se va a usar en un entorno de producción, probablemente necesitará un certificado firmado por una CA. No se recomienda el uso de certificados auto-firmados.

10.3.5. Instalar el Certificado

Puede instalar el archivo de la clave `server.key` y el archivo del certificado `server.crt` o el archivo de certificado enviado por su CA ejecutando las siguientes órdenes en la línea de órdenes de una terminal:

```
sudo cp server.crt /etc/ssl/certs
sudo cp server.key /etc/ssl/private
```

You should add the following four lines to the `/etc/apache2/sites-available/default` file or the configuration file for your secure virtual host. You should place them in the *VirtualHost* section. They should be placed under the *DocumentRoot* line:

```
#
SSLEngine on#
#
SSLOptions +FakeBasicAuth +ExportCertData +CompatEnvVars +StrictRequire#
#
SSLCertificateFile /etc/ssl/certs/server.crt#
SSLCertificateKeyFile /etc/ssl/private/server.key#
```

El HTTPS suele escuchar en el puerto número 443. Podría añadir la siguiente línea al archivo `/etc/apache2/ports.conf`:

```
#
Listen 443#
```

10.3.6. Accediendo al Servidor

Una vez haya instalado su certificado, debería reiniciar su servidor web. Puede ejecutar la siguiente orden en la línea de órdenes de una terminal para reiniciar su servidor web.

```
sudo /etc/init.d/apache2 restart
```

Debería memorizar e introducir su contraseña cada vez que inicie una sesión segura en su navegador.

Se le pedirá que introduzca la frase de paso. Cuando haya introducido la frase de paso correcta, se arrancará el servidor web seguro. Puede acceder a las páginas del servidor seguro tecleando https://su_equipo/url en la barra de direcciones de su navegador.

10.4. Referencias

Documentación de Apache2 [http://httpd.apache.org/docs/2.0/]

Documentación de Mod SSL [http://www.modssl.org/docs/]

11. Servidor proxy Squid

Squid es una completa aplicación servidor proxy caché web que proporciona servicios de proxy y caché para Hyper Text Transport Protocol (HTTP), File Transfer Protocol (FTP) y otros protocolos populares de red. Squid puede servir de caché y de proxy para las peticiones Secure Sockets Layer (SSL) y de caché para las consultas de Domain Name Server (DNS), y proporciona servicios de caché transparente. Squid también soporta una amplia variedad de protocolos de caché, como el Internet Cache Protocol (ICP), el Hyper Text Caching Protocol (HTCP), el Cache Array Routing Protocol (CARP), y el Web Cache Coordination Protocol (WCCP).

El servidor proxy caché Squid es una solución excelente para una amplia variedad de necesidades de proxy y de caché, y escala desde redes de oficina hasta redes a nivel empresarial al tiempo que proporciona extensos y granulares mecanismos de control de acceso y monitorización de parámetros críticos a través del Simple Network Management Protocol (SNMP). Cuando elija un ordenador para su uso como proxy Squid dedicado, o como servidor de caché, asegúrese de que su sistema dispone de una gran cantidad de memoria física, puesto que Squid mantiene una caché en memoria para mejorar el rendimiento.

11.1. Instalación

En un terminal, introduzca el siguiente comando para instalar el servidor Squid:

```
sudo apt-get install squid squid-common
```

11.2. Configuración

Squid se configura editando las directivas contenidas en el archivo de configuración `/etc/squid/squid.conf`. Los siguientes ejemplos ilustran algunas de las directivas que puede modificar para alterar el comportamiento del servidor Squid. Para una configuración más en profundidad, consulte la sección Referencias.

Antes de editar el archivo de configuración, debería hacer una copia del archivo original y protegerlo contra escritura de forma que tenga las opciones originales como referencia y pueda reutilizarlas si fuese necesario.

Copie el archivo·`/etc/squid/squid.conf`·y protejalo contra escritura introduciendo el siguiente comando en un terminal:

```
sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.original
sudo chmod a-w /etc/squid/squid.conf.original
```

- Para que su servidor Squid escuche en el puerto TCP 8888 en lugar del puerto TCP 3128 que usa por defecto, cambie la directiva http_port como sigue:

http_port·8888

- Cambie la directiva visible_hostname para hacer que el servidor Squid tenga un nombre de host específico. Este nombre de host no tiene por qué ser necesariamente el nombre de host del equipo. En este ejemplo se ha establecido a *weezie*

  visible_hostname·weezie

- De nuevo, usando el control de acceso de Squid, puede configurar que el uso de los servicios de Internet delegados por Squid esté sólo disponible para aquellos usuarios que tengan unas determinadas direcciones IP. Por ejemplo, ilustraremos el acceso sólo de aquellos usuarios que pertenezcan a la subred 192.168.42.0/24:

  Añada lo siguiente al **final** de la sección ACL de su archivo `/etc/squid/squid.conf`:

  acl fortytwo_network src 192.168.42.0/24

  Después, añada lo siguiente al **principio** de la sección http_access de su archivo `/etc/squid/squid.conf`:

  http_access allow fortytwo_network

- Usando las excelentes capacidades de control de acceso de Squid, puede configurar el uso de los servicios de Internet delegados por Squid para que sólo estén disponibles durante las horas normales de trabajo. Por ejemplo, ilustraremos el acceso de los empleados de un negocio que opera entre las 9 de la mañana y las 5 de la tarde, de lunes a viernes, y que usan la subred 10.1.42.0/42:

  Añada lo siguiente al **final** de la sección ACL de su archivo `/etc/squid/squid.conf`:

  acl biz_network src 10.1.42.0/24 acl biz_hours time M T W T F 9:00-17:00

  Después, añada lo siguiente al **principio** de la sección http_access de su archivo `/etc/squid/squid.conf`:

  http_access allow biz_network biz_hours

Después de hacer los cambios en el archivo `/etc/squid/squid.conf`, guarde el archivo y reinicie el servidor squid para que los cambios surtan efecto, usando la siguiente orden que deberá introducir en la línea de órdenes de una terminal:

```
sudo /etc/init.d/squid restart
```

11.3. Referencias

Web de Squid [http://www.squid-cache.org/]

12. Sistema de Control de Versiones

Version control is the art of managing changes to information. It has long been a critical tool for programmers, who typically spend their time making small changes to software and then undoing those changes the next day. But the usefulness of version control software extends far beyond the bounds of the software development world. Anywhere you can find people using computers to manage information that changes often, there is room for version control.

12.1. Subversion

Subversion is an open source version control system. Using Subversion, you can record the history of source files and documents. It manages files and directories over time. A tree of files is placed into a central repository. The repository is much like an ordinary file server, except that it remembers every change ever made to files and directories.

12.1.1. Instalación

Para acceder a un repositorio de Subversion mediante el protocolo HTTP, debe instalar y configurar un servidor web. Apache2 ha demostrado funcionar bien con Subversion (para instalar y configurar Apache2, consulte la sub-sección HTTP de la sección de Apache2). Para acceder al repositorio de Subversion repository mediante el protocolo HTTPS, debe instalar y configurar un certificado digital en su servidor web Apache 2 (para ello, consulte la sub-sección HTTPS de la sección de Apache2).

Para instalar Subversion, ejecute la siguiente orden en la línea de órdenes de una terminal:

```
sudo apt-get install subversion libapache2-svn
```

12.1.2. Configuración del servidor

Este paso asume que ya tiene instalados los paquetes mencionados en su sistema. Esta sección le explica cómo crear un repositorio de Subversion y acceder al proyecto.

12.1.2.1. Crear un repositorio de Subversion

El repositorio de Subversion puede ser creado usando la siguiente orden en la línea de órdenes de una terminal

```
svnadmin create /path/to/repos/project
```

12.1.3. Métodos de Acceso

Subversion repositories can be accessed (checked out) through many different methods --on local disk, or through various network protocols. A repository location, however, is

always a URL. The table describes how different URL schemas map to the available access methods.

Tabla 4.1. Métodos de Acceso

Proyecto	Método de Acceso
file://	acceso directo al repositorio (en disco local)
http://	Access via WebDAV protocol to Subversion-aware Apache2 web server
https://	Igual que http://, pero con cifrado SSL
svn://	Acceso al servidor svnserve via el protocolo por defecto
svn+ssh://	Lo mismo que svn://, pero a través de un tunel SSH

In this section, we will see how to configure Subversion for all these access methods. Here, we cover the basics. For more advanced usage details, refer to the *svn book* [http://svnbook.red-bean.com/].

12.1.3.1. Acceso directo al repositorio (file://)

This is the simplest of all access methods. It does not require any Subversion server process to be running. This access method is used to access Subversion from the same machine. The syntax of the command, entered at a terminal prompt, is as follows:

```
svn co file:///path/to/repos/project
```

o

```
svn co file://localhost/path/to/repos/project
```

Si no especifica el nombre del host, ha de usar tres barras (///) -- dos para el protocolo (file, en este caso) más la barra que indica la raíz de la ruta. Si especifica el nombre del host, debe usar dos barras (//).

Los permisos del repositorio dependen de los permisos del sistema de archivos. Si el usuario tiene permisos de lectura/escritura, puede hacer «checkout» y «commit» sobre el repositorio.

12.1.3.2. Acceso·via·protocolo WebDAV·(http://)

To access the Subversion repository via WebDAV protocol, you must configure your Apache 2 web server. You must add the following snippet in your `/etc/apache2/apache2.conf` file:

```
<Location /svn>
 DAV svn
 SVNPath /path/to/repos
 AuthType Basic
 AuthName "El nombre de su repositorio"
 AuthUserFile /etc/subversion/passwd
 <LimitExcept GET PROPFIND OPTIONS REPORT>
 Require valid-user
 </LimitExcept>
 </Location>
```

Ahora, debe crear el fichero `/etc/subversion/passwd`, el cual contiene los detalles de autenticación del usuario. Para añadir una entrada, p.e. para añadir un usuario, puede ejecutar esta orden en una terminal:

```
htpasswd2·/etc/subversion/passwd·user_name
```

Ésta orden le pedirá que introduzca su contraseña. Cuando lo haga, se añadirá el usuario. Entonces, para acceder al repositorio puede ejecutar esto:

```
svn co http://servername/svn
```

La contraseña se transmite como texto plano. Si le preocupa que puedan interceptar su contraseña, se le recomienda que use cifrado SSL. Para más detalles, consulte la siguiente sección.

12.1.3.3. Acceso vía protocolo WebDAV con encriptación SSL (https://)

Accessing Subversion repository via WebDAV protocol with SSL encryption (https://) is similar to http:// except that you must install and configure the digital certificate in your Apache2 web server.

Puede instalar un certificado digital emitido por una autoridad de certificación como Verisign. También puede instalar su propio certificado auto-firmado.

This step assumes you have installed and configured a digital certificate in your Apache 2 web server. Now, to access the Subversion repository, please refer to the above section! The access methods are exactly the same, except the protocol. You must use https:// to access the Subversion repository.

12.1.3.4. Acceso vía protocolo personalizado (svn://)

Once the Subversion repository is created, you can configure the access control. You can edit the `/path/to/repos/project/conf/svnserve.conf` file to configure the access control. For example, to set up authentication, you can uncomment the following lines in the configuration file:

```
# [general]#
```

```
# password-db = passwd
```

After uncommenting the above lines, you can maintain the user list in the passwd file. So, edit the file `passwd` in the same directory and add the new user. The syntax is as follows:

```
username·=·password
```

Para más detalles, por favor consulte el archivo.

Now, to access Subversion via the svn:// custom protocol, either from the same machine or a different machine, you can run svnserver using svnserve command. The syntax is as follows:

```
$ svnserve -d --foreground -r /path/to/repos
# -d -- daemon mode
# --foreground -- run in foreground (useful for debugging)
# -r -- root of directory to serve

For more usage details, please refer to:
$ svnserve --help
```

Once you run this command, Subversion starts listening on default port (3690). To access the project repository, you must run the following command from a terminal prompt:

```
svn co svn://hostname/project project --username user_name
```

Based on server configuration, it prompts for password. Once you are authenticated, it checks out the code from Subversion repository. To synchronize the project repository with the local copy, you can run the **update** sub-command. The syntax of the command, entered at a terminal prompt, is as follows:

```
cd project_dir ; svn update
```

For more details about using each Subversion sub-command, you can refer to the manual. For example, to learn more about the co (checkout) command, please run the following command from a terminal prompt:

```
svn co help
```

12.1.3.5. Acceso vía protocolo personalizado con encriptación SSL (svn+ssh://)

The configuration and server process is same as in the svn:// method. For details, please refer to the above section. This step assumes you have followed the above step and started the#Subversion server using svnserve command.

It is also assumed that the ssh server is running on that machine and that it is allowing incoming connections. To confirm, please try to login to that machine using ssh. If you can login, everything is perfect. If you cannot login, please address it before continuing further.

The svn+ssh:// protocol is used to access the Subversion repository using SSL encryption. The data transfer is encrypted using this method. To access the project repository (for example with a checkout), you must use the following command syntax:

```
svn co svn+ssh://hostname/var/svn/repos/project
```

You must use the full path (/path/to/repos/project) to access the Subversion repository using this access method.

Based on server configuration, it prompts for password. You must enter the password you use to login via ssh. Once you are authenticated, it checks out the code from the Subversion repository.

12.2. Servidor CVS

CVS es un sistema de control de versiones. Puede usarlo para grabar el historial de un fichero fuente.

12.2.1. Instalación

At a terminal prompt, enter the following command to install cvs:

```
sudo apt-get install cvs
```

After you install cvs, you should install xinetd to start/stop the cvs server. At the prompt, enter the following command to install xinetd:

```
sudo apt-get install xinetd
```

12.2.2. Configuración

Once you install cvs, the repository will be automatically initialized. By default, the repository resides under the /var/lib/cvs directory. You can change this path by running following command:

```
cvs -d /your/new/cvs/repo init
```

Once the initial repository is set up, you can configure xinetd to start the CVS server. You can copy the following lines to the `/etc/xinetd/cvspserver` file.

```
#
service cvspserver#
{#
     port = 2401#
     socket_type = stream#
     protocol = tcp#
     user = root#
```

```
    wait = no#
    type = UNLISTED#
    server = /usr/bin/cvs#
    server_args = -f --allow-root /var/lib/cvs pserver#
    disable = no#
}#
```

Be sure to edit the repository if you have changed the default repository (/var/lib/cvs) directory.

Once you have configured xinetd you can start the cvs server by running following command:

```
sudo /etc/init.d/xinetd start
```

Puede confirmar que el servidor CVS se está ejecutando introduciendo la siguiente orden:

```
sudo netstat -tap | grep cvs
```

Cuando ejecute este comando, deberá ver la siguiente línea o algo similar:

```
#
tcp 0 0 *:cvspserver *:* LISTEN #
```

Desde aquí puede continuar añadiendo usuarios, nuevos proyectos, y manejando el servidor CVS.

CVS allows the user to add users independently of the underlying OS installation. Probably the easiest way is to use the Linux Users for CVS, although it has potential security issues. Please refer to the CVS manual for details.

12.2.3. Añadir proyectos

Esta sección explica cómo añadir un nuevo proyecto al repositorio CVS. Cree el directorio y meta en él los documentos y códigos fuente necesarios. Después, ejecute la siguiente orden para añadir el proyecto al repositorio CVS:

```
cd su/proyecto
cvs import -d :pserver:nombreusuario@nombrehost.com:/var/lib/cvs -m "Importando mi proyect
```

Puede usar la variable de entorno CVSROOT para guardar el directorio raíz CVS. Una vez haya exportado la variable de entorno CVSROOT, podrá evitar usar la opción -d en las órdenes cvs de arriba.

La cadena *nuevo_proyecto* es una etiqueta de vendedor, y *start* es una etiqueta de publicación. No tienen importancia en este contexto, pero como CVS los requiere, deben estar presentes.

Cuando añada un nuevo proyecto, el usuario CVS que utilice deberá tener acceso de escritura al repositorio CVS (/var/lib/cvs). De forma predeterminada, el grupo src tiene acceso de escritura al repositorio CVS. Por tanto, puede añadir el usuario a este grupo, y así él podrá añadir y gestionar proyectos en el repositorio CVS.

12.3. Referencias

Página web de Subversion [http://subversion.tigris.org/]

Libro de Subversion [http://svnbook.red-bean.com/]

Manual de CVS [http://ximbiot.com/cvs/manual/cvs-1.11.21/cvs_toc.html]

13. Bases de Datos

Ubuntu proporciona dos servidores de bases de datos. Son:

- MySQL™
- PostgreSQL

Están disponibles en el repositorio Main. Esta sección explica cómo instalar y configurar estos servidores de bases de datos.

13.1. MySQL

MySQL es un rápido y robusto servidor de bases de datos SQL multi-hilo y multi-usuario.

13.1.1. Instalación

Para instalar MySQL, ejecute el siguiente comando en un terminal:

```
sudo apt-get install mysql-server mysql-client
```

Cuando se complete la instalación, el servidor MySQL deberá iniciarse automáticamente. Puede ejecutar la siguiente orden en la línea de órdenes de una terminal para comprobar si se está funcionando el servidor MySQL:

```
sudo netstat -tap | grep mysql
```

Cuando ejecute este comando, deberá ver la siguiente línea o algo similar:

```
tcp 0 0 localhost.localdomain:mysql *:* LISTEN -
```

Si el servidor no se está ejecutando correctamente, puede teclear la siguiente orden para arrancarlo:

```
sudo /etc/init.d/mysql restart
```

13.1.2. Configuración

La contraseña del administrador no está establecida de forma predeterminada. Una vez que haya instalado MySQL, lo primero que debe hacer es establecer la contraseña del administrador de MySQL. Para ello, ejecute las siguientes órdenes:

```
sudo mysqladmin -u root contraseña nuevacontraseñasqlderoot
```

```
sudo mysqladmin -u root -h localhost password newrootsqlpassword
```

Puede cambiar el archivo `/etc/mysql/my.cnf` para configurar las opciones básicas -- archivo de registro, número de puerto, etc. Diríjase al archivo `/etc/mysql/my.cnf` para más detalles.

13.2. PostgreSQL

PostgreSQL es un sistema de bases de datos objeto-relacional que combina las características de un sistema de gestión de bases de datos comercial tradicional con las mejoras que se suelen encontrar en sistemas de gestión de bases de datos de nueva generación.

13.2.1. Instalación

Para instalar PostgreSQL, ejecute la siguiente orden en la línea de órdenes de una terminal:

```
sudo apt-get install postgresql
```

Cuando se haya completado la instalación, podrá configurar el servidor PostgreSQL en base a sus necesidades, aunque la configuración predeterminada es viable.

13.2.2. Configuración

Las conexiones TCP/IP están deshabilitadas de forma predeterminada. PostgreSQL soporta varios métodos de autenticación del cliente. El método de autenticación predeterminado es IDENT. Por favor, para más información lea *la Guía del administrador de PostgreSQL* [http://www.postgresql.org/docs/8.1/static/admin.html].

La siguiente explicación asume que desa activar las conexiones TCP/IP y que usa el método de autenticación MD5 para la autenticación del cliente. Los archivos de configuración de PostgreSQL se almacenan en el directorio `/etc/postgresql/<version>/main`. Por ejemplo, si instala PostgreSQL 7.4, los archivos de configuración se guardarán en el directorio `/etc/postgresql/7.4/main`.

Para configurar la autenticación ident, debe añadir unas entradas al archvivo de configuración `/etc/postgresql/7.4/main/pg_ident.conf`.

Para habilitar las conexiones TCP/IP, debe editar el archivo `/etc/postgresql/7.4/main/postgresql.conf`.

Busque la línea *#tcpip_socket = false* y cámbiela por *tcpip_socket = true*. También puede editar todos los demás parámetros, si sabe lo que está haciendo. Para más detalles, recurra al archivo de configuración o a la documentación de PostgreSQL.

De forma predeterminada, las credenciales del usuario no están establecidas para autenticación de cliente *MD5*. Por ello, primero es necesario configurar el servidor PostgreSQL para que use la autenticación de cliente *trust*, conectarse a la base de

datos, establecer la contraseña, y revertir la configuración de nuevo autenticación de cliente *MD5*. Para habilitar la autenticación de cliente *trust*, edite el archivo `/etc/postgresql/7.4/main/pg_hba.conf`

Comente todas las líneas que usen las autenticaciones de cliente *ident* y *MD5*, y añada la siguiente línea:

```
#
local all postgres trust sameuser#
```

Después, ejecute el siguiente comando para arrancar el servidor PostgreSQL:

```
sudo /etc/init.d/postgresql start
```

Una vez que haya iniciando con éxito el servidor PostgreSQL, ejecute la siguiente orden en la línea de órdenes de una terminal para conectar con la base de datos plantilla predeterminada de PostgreSQL

```
psql -U postgres -d template1
```

La orden anterior conecta con la base de datos de PostgreSQL *template1* como usuario *postgres*. Una vez haya conectado con el servidor PostgreSQL, se encontrará en una línea de órdenes SQL. Puede ejecutar la siguiente orden SQL en la línea de órdenes de psql para establecer la contraseña del usuario *postgres*.

```
template1=# ALTER USER postgres with encrypted password 'su_contraseña';
```

Cuando haya establecido la contraseña, edite el archivo `/etc/postgresql/7.4/main/pg_hba.conf` para usar la autenticación *MD5*:

Comente la línea *trust* añadida recientemente, y añada la siguiente línea:

```
local all postgres md5 sameuser
```

La configuración anterior no está completa de ningún modo.
Por favor, consulte la *Guía del administrador de PostgreSQL* [http://www.postgresql.org/docs/8.1/static/admin.html] para configurar más parámetros.

14. Servicios de correo electrónico

El proceso de enviar un correo electrónico de una persona a otra a través de una red o de Internet involucra muchos sistemas trabajando juntos. Todos esos sistemas deben estar configurados correctamente para que el proceso funcione. El remitente usa un *Agente de Usuario de Correo* (Mail User Agent, MUA), o cliente de correo, para enviar el mensaje a través de uno o varios *Agentes de Transferencia de Correo* (Mail Transport Agent, MTA), el último de los cuales actuará de *Agente de Entrega de Correo* (Mail Delivery Agent, MDA) para entregarlo en el buzón del destinatario, y que luego pueda ser recuperado usando el cliente de correo del destinatario, normalmente por medio de un servidor POP3 o IMAP.

14.1. Postfix

Postfix es el Agente de Transferencia de Correo (Mail Transfer Agent, MTA) predeterminado en Ubuntu. Su objetivo es ser rápido, seguro y fácil de administrar. Es compatible con el MTA sendmail. Esta sección explica cómo instalar y configurar postfix. También explica cómo configurar un servidor SMTP usando una conexión segura (para enviar correos electrónicos de forma segura).

14.1.1. Instalación

Para instalar postfix con SMTP-AUTH y Transport Layer Security (TLS), ejecute la siguiente orden:

```
sudo apt-get install postfix
```

Cuando el proceso de instalación le haga preguntas, simplemente pulse Intro; la configuración se hará con más detalle en la siguiente etapa.

14.1.2. Configuración Básica

Para configurar postfix, ejecute la siguiente orden:

```
sudo dpkg-reconfigure postfix
```

Se mostrará la interfaz de usuario. En cada pantalla, seleccione los siguientes valores:

- Ok
- Sitio de Internet
- NONE
- mail.example.com
- mail.example.com, localhost.localdomain, localhost
- No
- 127.0.0.0/8

- Sí
- 0
- +
- todo

Reemplace mail.example.com con el nombre de máquina de su servidor de correo.

14.1.3. Autentificación SMTP

El siguiente paso es configurar postfix para que use SASL con SMTP AUTH. En lugar de editar directamente el archivo de configuración, puede usar la orden **postconf** para configurar todos los parámetros de postfix. Los parámetros de configuración se almacenarán en el archivo `/etc/postfix/main.cf`. Posteriormente, si desea reconfigurar un parámetro en particular, podrá ejecutar la misma orden o cambiar el parámetro manualmente en el archivo.

1. Configurar Postfix para hacer SMTP AUTH usando SASL (saslauthd):

```
#
postconf -e 'smtpd_sasl_local_domain ='#
postconf -e 'smtpd_sasl_auth_enable = yes'#
postconf -e 'smtpd_sasl_security_options = noanonymous'#
postconf -e 'broken_sasl_auth_clients = yes'#
postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetwork
postconf -e 'inet_interfaces = all'#
echo 'pwcheck_method: saslauthd' >> /etc/postfix/sasl/smtpd.conf#
echo 'mech_list: plain login' >> /etc/postfix/sasl/smtpd.conf#
```

2. A continuación, configure el certificado digital para TLS. Cuando se le pregunte, siga las instrucciones y responda adecuadamente.

```
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
chmod 600 smtpd.key
openssl req -new -key smtpd.key -out smtpd.csr
openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt
openssl rsa -in smtpd.key -out smtpd.key.unencrypted
mv -f smtpd.key.unencrypted smtpd.key
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
mv smtpd.key /etc/ssl/private/
mv smtpd.crt /etc/ssl/certs/
mv cakey.pem /etc/ssl/private/
mv cacert.pem /etc/ssl/certs/
```

Puede conseguir el certificado digital solicitándosela a una autoridad de certificación. También puede crear el certificado usted mismo. Vea *Sección 10.3.4, “Creación de un certificado auto-firmado” [57]* para más detalles.

3. Configurar Postfix para hacer cifrado TLS con el correo entrante y saliente:

```
postconf -e 'smtpd_tls_auth_only = no'
postconf -e 'smtp_use_tls = yes'
postconf -e 'smtpd_use_tls = yes'
postconf -e 'smtp_tls_note_starttls_offer = yes'
postconf -e 'smtpd_tls_key_file = /etc/ssl/private/smtpd.key'
postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt'
postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'
postconf -e 'smtpd_tls_loglevel = 1'
postconf -e 'smtpd_tls_received_header = yes'
postconf -e 'smtpd_tls_session_cache_timeout = 3600s'
postconf -e 'tls_random_source = dev:/dev/urandom'
postconf -e 'myhostname = mail.ejemplo.com'
```

Una vez que haya ejecutado todas las órdenes, tendrá configurado el SMTP AUTH en postfix. El certificado auto-firmado se crea para el TLS y se configura con postfix.

Ahora,·el archivo·`/etc/postfix/main.cf`·debería parecerse a

La configuración inicial de postfix se ha completado. Ejecute la siguiente orden para arrancar el demonio de postfix:

```
sudo /etc/init.d/postfix start
```

Ahora, el demonio postfix está instalado y configurado, y se está ejecutando con éxito. Postfix soporta SMTP AUTH como se define en *RFC2554* [ftp://ftp.isi.edu/in-notes/rfc2554.txt]. Está basado en *SASL* [ftp://ftp.isi.edu/in-notes/rfc2222.txt]. Sin embargo, todavía es necesario configurar la autenticación SASL para poder usar SMTP.

14.1.4. Configuración de SASL

Los paquetes libsasl2, sasl2-bin y libsasl2-modules son necesarios para habilitar el SMTP AUTH usando SASL. Puede instalar estas aplicaciones si no las tenía ya instaladas.

```
apt-get install libsasl2 sasl2-bin
```

Se necesitan unos pocos cambios para hacer que funcione apropiadamente. Como Postfix se ejecuta «enjaulado» con chroot en `/var/spool/postfix`, es necesario configurar SASL para ejecutarlo en un raíz falso (`/var/run/saslauthd` se convierte en `/var/spool/postfix/var/run/saslauthd`):

```
mkdir -p /var/spool/postfix/var/run/saslauthd
rm -rf /var/run/saslauthd
```

Para activar saslauthd, edite el archivo `/etc/default/saslauthd` y cambie o añada la variable START. Con idea de configurar saslauthd para que se pueda ejecutar en un falso

raíz, añada las variables PWDIR, PIDFILE y PARAMS. Finalmente, configure la variable MECHANISMS a su gusto. El archivo debe tener el siguiente aspecto:

```
#
# This needs to be uncommented before saslauthd will be run#
# automatically#
START=yes#
#
PWDIR="/var/spool/postfix/var/run/saslauthd"#
PARAMS="-m ${PWDIR}"#
PIDFILE="${PWDIR}/saslauthd.pid"#
#
# You must specify the authentication mechanisms you wish to use.#
# This defaults to "pam" for PAM support, but may also include#
# "shadow" or "sasldb", like this:#
# MECHANISMS="pam shadow"#
#
MECHANISMS="pam"#
```

Si lo prefiere, puede usar **shadow** en lugar de **pam**. De esta forma, se transferirán contraseñas cifradas con MD5, lo que resultará más seguro. El nombre de usuario y la contraseña que haya que autenticar serán los de los usuarios del sistema que esté usando en el servidor.

A continuación, actualice el «estado» de dpkg de `/var/spool/portfix/var/run/saslauthd`. El script de inicialización de saslauthd usa esta opción para crear el directorio que falta con los permisos y propietario adecuados:

```
dpkg-statoverride --force --update --add root sasl 755 /var/spool/postfix/var/run/saslauth
```

14.1.5. Comprobando

La configuración del SMTP AUTH está ya completa. Ahora es el momento de iniciar y probar la configuración. Puede ejecutar la siguiente orden para arrancar el demonio SASL:

```
sudo /etc/init.d/saslauthd start
```

Para ver si el SMTP-AUTH y el TLS funcionan correctamente, ejecute la siguiente orden:

```
telnet mail.example.com 25
```

Una vez que haya establecido la conexión con el servidor de correo postfix, teclee:

```
ehlo mail.ejemplo.com
```

Si ve aparecer las siguientes líneas (entre otras), es que todo funciona correctamente. Teclee **quit** para salir.

```
#
```

```
250-STARTTLS#
250-AUTH LOGIN PLAIN#
250-AUTH=LOGIN PLAIN#
250 8BITMIME#
```

14.2. Exim4

Exim4 is is another Message Transfer Agent (MTA) developed at the University of Cambridge for use on Unix systems connected to the internet. Exim can be installed in place of sendmail, although the configuration of exim is quite different to that of sendmail.

14.2.1. Instalación

Para instalar exim4, ejecute el siguiente comando:

```
#
sudo apt-get install exim4 exim4-base exim4-config#
```

14.2.2. Configuración

To configure exim4, run the following command:

```
sudo dpkg-reconfigure exim4-config
```

The user interface will be displayed. The user interface lets you configure many parameters. For example, In exim4 the configuration files are split among multiple files. If you wish to have them in one file you can configure accordingly in this user interface.

All the parameters you configure in the user interface are stored in `/etc/exim4/update-exim4.conf.conf` file. If you wish to re-configure, either you re-run the configuration wizard or manually edit this file using your favourite editor. Once you configure, you can run the following command to generate the master configuration file:

```
sudo update-exim4.conf
```

The master configuration file, is generated and it is stored in `/var/lib/exim4/config.autogenerated`.

At any time, you should not edit the master configuration file, `/var/lib/exim4/config.autogenerated` manually. It is updated automatically every time you run **update-exim4.conf**

You can run the following command to start exim4 daemon.

```
sudo /etc/init.d/exim4 start
```

TODO: This section should cover configuring SMTP AUTH with exim4.

14.3. Servidor Dovecot

Dovecot is a Mail Delivery Agent, written with security primarily in mind. It supports the major mailbox formats: mbox or Maildir. This section explain how to set it up as an imap or pop3 server.

14.3.1. Instalación

To install dovecot, run the following command in the command prompt:

```
sudo apt-get install dovecot-common dovecot-imapd dovecot-pop3d
```

14.3.2. Configuración

To configure dovecot, you can edit the file `/etc/dovecot/dovecot.conf`. You can choose the protocol you use. It could be pop3, pop3s (pop3 secure), imap and imaps (imap secure). A description of these protocols is beyond the scope of this guide. For further information, refer to the wikipedia articles on *POP3* [http://en.wikipedia.org/wiki/POP3] and *IMAP* [http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol].

IMAPS and POP3S are more secure that the simple IMAP and POP3 because they use SSL encryption to connect. Once you have chosen the protocol, amend the following line in the file `/etc/dovecot/dovecot.conf`:

```
#
protocols = pop3 pop3s imap imaps#
```

It enables the protocols when dovecot is started. Next, add the following line in pop3 section in the file `/etc/dovecot/dovecot.conf`:

```
#
pop3_uidl_format = %08Xu%08Xv#
```

Next, choose the mailbox you use. Dovecot supports **maildir** and **mbox** formats. These are the most commonly used mailbox formats. They both have their own benefits and they are discussed on *the dovecot website* [http://dovecot.org/doc/configuration.txt].

Once you have chosen your mailbox type, edit the file `/etc/dovecot/dovecot.conf` and change the following line:

```
#
default_mail_env = maildir:~/Maildir # (for maildir)#
or#
default_mail_env = mbox:~/mail:INBOX=/var/spool/mail/%u # (for mbox)#
```

You should configure your Mail Trasport Agent (MTA) to transfer the incoming mail to this type of mailbox if it is different from the one you have configured.

Once you have configured dovecot, start the dovecot daemon in order to test your setup:

```
sudo /etc/init.d/dovecot start
```

If you have enabled imap, or pop3, you can also try to log in with the commands **telnet localhost pop3** or **telnet localhost** imap2. If you see something like the following, the installation has been successful:

```
#
bhuvan@rainbow:~$ telnet localhost pop3#
Trying 127.0.0.1...#
Connected to localhost.localdomain.#
Escape character is '^]'.#
+OK Dovecot ready.#
```

14.3.3. Configuración Dovecot SSL

To configure dovecot to use SSL, you can edit the file `/etc/dovecot/dovecot.conf` and amend following lines:

```
#
ssl_cert_file = /etc/ssl/certs/dovecot.pem#
ssl_key_file = /etc/ssl/private/dovecot.pem#
ssl_disable = no#
disable_plaintext_auth = no#
```

The **cert** and **key** files are created automatically by dovecot when you install it. Please note that these keys are not signed and will give "bad signature" errors when connecting from a client. To avoid this, you can use commercial certificates, or even better, you can use your own SSL certificates.

14.3.4. Configuración del firewall para un servidor de correo

Para acceder a su servidor de correo desde otro equipo, deberá configurar su firewall para que permita conexiones al servidor a través de los puertos necesarios.

- IMAP - 143
- IMAPS - 993
- POP3 - 110
- POP3S - 995

14.4. Mailman

Mailman is an open source program for managing electronic mail discussions and e-newsletter lists. Many open source mailing lists (including all the *Ubuntu mailing lists* [http://lists.ubuntu.com]) use Mailman as their mailing list software. It is powerful and easy to install and maintain.

14.4.1. Instalación

Mailman suministra un interface web para administradores y usuarios. Por lo tanto, requiere apache con soporte mod_perl. Mailman usa un servidor de correo externo para enviar y recibir emails. Funciona perfectamente con los siguientes servidores de correo:

- Postfix
- Exim
- Sendmail
- Qmail

Veremos como instalar mailman, el servidor web apache y el servidor de correo Exim. Si desea instalar mailman con un servidor de correo diferente, remitase a las secciones que lo referencian.

14.4.1.1. Apache2

Para instalar apache2 remitase a *Sección 10.1, “Instalación” [49]*.

14.4.1.2. Exim4

Para instalar Exim4 ejecute los siguiente comandos en un terminal:

```
#
sudo apt-get install exim4#
sudo apt-get install exim4-base#
sudo apt-get install exim4-config#
```

Una vez que exim4 este instalado, los archivos de configuración son guardados en el directorio `/etc/exim4`. En ubuntu, por defecto, los archivos de configuración de exim4 son divididos en distintos archivos. Puede cambiar este comportamiento cambiando la siguiente variable en el archivo `/etc/exim4/update-exim4.conf`:

- dc_use_split_config='true'

14.4.1.3. Mailman

Para instalar Mailman, ejecute esta orden en una terminal:

```
sudo apt-get install mailman
```

Eso copia los archivos de instalación en el directorio /var/lib/mailman, instala los scripts CGI en el directorio /usr/lib/cgi-bin/mailman, crea una *lista* de usuarios de linux y la *lista* de grupos de linux. El proceso mailman será propiedad de este usuario.

14.4.2. Configuración

Esta sección asume que instaló con éxito mailman, apache2, y exim4. Ahora solo necesita configurarlos.

14.4.2.1. Apache2

Once apache2 is installed, you can add the following lines in the `/etc/apache2/apache2.conf` file:

```
#
Alias /images/mailman/ "/usr/share/images/mailman/"#
Alias /pipermail/ "/var/lib/mailman/archives/public/"#
```

Mailman uses apache2 to render its CGI scripts. The mailman CGI scripts are installed in the /usr/lib/cgi-bin/mailman directory. So, the mailman url will be http://hostname/cgi-bin/mailman/. You can make changes to the `/etc/apache2/apache2.conf` file if you wish to change this behavior.

14.4.2.2. Exim4

Una vez que Exim4 este instalado, puede ejecutar el servidor Exim usando el siguiente comando en un terminal:

```
#
sudo apt-get /etc/init.d/exim4 start#
```

Para hacer que mailman mailman funcione con exim4, necesita configurar exim4. Como se menciono antes, por defecto, exim4 usa multiples archivos de configuración de diferentes tipos. Para más detalles, remitase al sitio web de *Exim* [http://www.exim.org]. Para ejecutar mailman, deberiamos de añadir un archivo de configuración con el siguiente tipo de configuración:

- Principal
- Transporte
- Enrutamiento

Exim crea un archivo principal de configuración ordenando todos los miniarchivos de configuración. Por lo tanto, el orden de estos archivos de configuración es muy importante.

14.4.2.3. Principal

Todos los archivos de configuración pertenecientes al tipo principal son guardados en el directorio `/etc/exim4/conf.d/main/`. Puede añadir el contenido siguiente a un archivo nuevo, llamado `04_exim4-config_mailman`:

```
#
# start#
# Home dir for your Mailman installation -- aka Mailman's prefix#
# directory.#
# On Ubuntu this should be "/var/lib/mailman"#
# This is normally the same as ~mailman#
MM_HOME=/var/lib/mailman#
##
```

```
# User and group for Mailman, should match your --with-mail-gid#
# switch to Mailman's configure script. Value is normally "mailman"#
MM_UID=list#
MM_GID=list#
##
# Domains that your lists are in - colon separated list#
# you may wish to add these into local_domains as well#
domainlist mm_domains=hostname.com#
##
# -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=#
##
# These values are derived from the ones above and should not need#
# editing unless you have munged your mailman installation#
##
# The path of the Mailman mail wrapper script#
MM_WRAP=MM_HOME/mail/mailman#
##
# The path of the list config file (used as a required file when#
# verifying list addresses)#
MM_LISTCHK=MM_HOME/lists/${lc::$local_part}/config.pck#
# end#
```

14.4.2.4. Transporte

All the configuration files belonging to transport type are stored in the `/etc/exim4/conf.d/transport/` directory. You can add the following content to a new file named `40_exim4-config_mailman`:

```
#
mailman_transport:#
 driver = pipe#
 command = MM_WRAP \#
             '${if def:local_part_suffix \#
                   {${sg{$local_part_suffix}{-(\\w+)(\\+.*)?}{\$1}}} \#
                   {post}}' \#
             $local_part#
  current_directory = MM_HOME#
  home_directory = MM_HOME#
  user = MM_UID#
  group = MM_GID#
```

14.4.2.5. Enrutamiento

All the configuration files belonging to router type are stored in the `/etc/exim4/conf.d/router/` directory. You can add the following content in to a new file named `101_exim4-config_mailman`:

```
#
mailman_router:#
 driver = accept#
```

```
  require_files = MM_HOME/lists/$local_part/config.pck#
  local_part_suffix_optional#
  local_part_suffix = -bounces : -bounces+* : \#
                      -confirm+* : -join : -leave : \#
                      -owner : -request : -admin#
  transport = mailman_transport#
```

The order of main and transport configuration files can be in any order. But, the order of router configuration files must be the same. This particular file must appear before the 200_exim4-config_primary file. These two configuration files contain same type of information. The first file takes the precedence. For more details, please refer to the references section.

14.4.2.6. Mailman

Una vez que mailman esta instalado, puede ejecutarlo usantdo el comando:

```
#
sudo /etc/init.d/mailman start#
```

Una vez que mailman esta instalado, puede crear la lista de correo por defecto. Ejecute el siguiente comando para crear esta lista:

```
#
sudo /usr/sbin/newlist mailman#
```

```
  #
  Enter the email address of the person running the list: bhuvan at ubuntu.com#
  Initial mailman password:#
  To finish creating your mailing list, you must edit your /etc/aliases (or#
  equivalent) file by adding the following lines, and possibly running the#
  `newaliases' program:#
#
  ## mailman mailing list#
  mailman: "|/var/lib/mailman/mail/mailman post mailman"#
  mailman-admin: "|/var/lib/mailman/mail/mailman admin mailman"#
  mailman-bounces: "|/var/lib/mailman/mail/mailman bounces mailman"#
  mailman-confirm: "|/var/lib/mailman/mail/mailman confirm mailman"#
  mailman-join: "|/var/lib/mailman/mail/mailman join mailman"#
  mailman-leave: "|/var/lib/mailman/mail/mailman leave mailman"#
  mailman-owner: "|/var/lib/mailman/mail/mailman owner mailman"#
  mailman-request: "|/var/lib/mailman/mail/mailman request mailman"#
  mailman-subscribe: "|/var/lib/mailman/mail/mailman subscribe mailman"#
  mailman-unsubscribe: "|/var/lib/mailman/mail/mailman unsubscribe mailman"#
#
  Hit enter to notify mailman owner...#
#
  # #
```

Hemos configurado exim para que reconozca todos los emails del mailman. Por lo tanto, no es obligatorio que introduzca nuevas entradas en `/etc/aliases`. Si usted hace algún

cambio en los archivos de configuración, asegurese que reinicia esos servicios antes de continuar con la siguiente sección.

14.4.3. Administración

Asumimos que tiene una instalación por defecto. El cgi script del mailman todavía esta en el directorio /usr/lib/cgi-bin/mailman/. Mailman tiene la facilidad de poder administrase por web. Para acceder a esta página, introduzca la siguiente url en su navegador:

http://nombrehost/cgi-bin/mailman/admin

La lista de correo por defecto, *mailman*, aparecerá en su pantalla. Si hace click en el nombre de la lista, se le preguntará la password de autentificación. Si introduce la password correcta, será capaz de cambiar las configuraciones administrativas de la lista de correo. Puede crear una nueva lista usando una utilidad de la línea de comandos (**/usr/sbin/newlist**). Adicionalmente, puede crear nuevas listas de correo usando el interface web.

14.4.4. Usuarios

Mailman posee un interface de usuario web. Para acceder a esta página, introduzca la siguiente url en su navegador:

http://nombrehost/cgi-bin/mailman/listinfo

La lista de correo por defecto, *mailman*, aparecerá en esta pantalla. Si hace click sobre el nombre, se le mostrará un formulario de suscripción. Puede introducir su dirección de correo, nombre (opcional), y password para suscribirse. Le será enviado un email de invitación. Puede seguir las instrucciones de este email para suscribirse.

14.4.5. Referencias

GNU Mailman - Manual de Instalación [http://www.list.org/mailman-install/index.html]

COMO - Usando juntos Exim4 y Mailman 2.1
[http://www.exim.org/howto/mailman21.html]

Capítulo 5. Redes Windows

Las redes de ordenadores se componen a menudo de sistemas diversos, y aunque trabajar con una red compuesta enteramente de ordenadores de escritorio Ubuntu y servidores Ubuntu puede ser realmente divertido, algunos entornos de red poseen sistemas Ubuntu y Microsoft® Windows® trabajando juntos en armonía. Esta sección de la Guía de Servidor de Ubuntu introduce los principios y las herramientas utilizadas para configurar su servidor Ubuntu para que pueda compartir recursos en red con ordenadores Windows.

1. Introducción

El trabajo en red con su sistema Ubuntu junto con clientes Windows implica la provisión e integración de los servicios comunes a los entornos Windows. Estos servicios ayudan en la compartición de datos e información acerca de los ordenadores y usuarios implicados en la red, y puedenn clasificarse en tres grandes categorías de funcionalidad:

- **Compartir impresoras y archivos**. Se utiliza el protocolo Server Message Block (SMB) para facilitar la compartición de archivos, directorios, volúmenes e impresoras a través de la red.
- **Servicios de Directorio**. Comparten información vital de los ordenadores y usuarios de la red con las tecnologías Lightweight Directory Access Protocol (LDAP) y Microsoft Active Directory®.
- **Autenticación y acceso**. Establecen la identidad de un ordenador o usuario de la red y determinan la información a la que el ordenador o el usuario está autorizado a acceder usando principios y tecnologías como permisos de archivos, políticas de grupos y el servicio de autentificación Kerberos.

Afortunadamente, su sistema Ubuntu proporciona facilidades semejantes a las de los clientes Windows, y compartir recursos de red es una de ellas. Una de las principales piezas de software que su sistema Ubuntu trae para trabajar en grupo con Windows es SAMBA, la suite de heramientas y aplicaciones de servidor SMB. Esta sección de la Guía del servidor Ubuntu le introducirá brevemente en la instalación y configuración limitada de la suite de heramientas y aplicaciones de servidor SMB SAMBA. La documentación e información detallada sobre SAMBA está fuera del alcance de esta documentación, pero existe en la *web de SAMBA* [http://www.samba.org].

2. Instalar Samba

Introduzca la siguiente orden en la línea de órdenes para instalar las aplicaciones del servidor SAMBA:

```
sudo apt-get install samba
```

3. Configurar SAMBA

Puede configurar el servidor SAMBA editando el archivo `/etc/samba/smb.conf` para cambiar las configuraciones por defecto o añadir algunas nuevas. Puede ver más información sobre cada entrada de este archivo en los comentarios del archivo `/etc/samba/smb.conf` o en la página del manual de `/etc/samba/smb.conf` usando la siguiente orden en una terminal:

```
man smb.conf
```

Antes de editar el archivo de configuración, debería hacer una copia del original y protegerla contra escritura para tener las configuraciones originales como referencia y reutilizarlas si fuese necesario.

Haga una copia de seguridad del archivo `/etc/samba/smb.conf` :

```
sudo cp /etc/samba/smb.conf  /etc/samba/smb.conf.original
```

Ahora, edite el archivo `/etc/samba/smb.conf` y haga los cambios que necesite.

3.1. Servidor

Además del paquete SAMBA de aplicaciones de servidor para compartir archivos e impresoras, Ubuntu también incluye otras potentes aplicaciones de red diseñadas para proporcionar funcionalidad adicional de servidor de red a los clientes Windows, similar a la funcionalidad proporcionada por los servidores Windows reales. Por ejemplo, Ubuntu proporciona una gestión centralizada de los recursos de red (como p.ej. ordenadores y usuarios) a través de los Servicios de Directorio, y facilita la identificación y la autorización de ordenadores y usuarios a través de los Servicios de Autenticación.

Las siguientes secciones discutirán con mayor detalle SAMBA y las tecnologías de soporte, como el servidor LDAP (Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios), y el servidor de autenticación Kerberos. También conocerá algunas de las directivas de configuración disponibles en el archivo de configuración de SAMBA, lo que le facilitará la integración en la red con clientes y servidores Windows.

3.1.1. Active Directory

Active Directory es una implementación propietaria (creada por Microsoft) de los Servicios de Directorio, y proporciona una manera de compartir información entre recursos y usuarios de la red. Además de proporcionar una fuente centralizada para esa información, Active Directory también funciona como autoridad de seguridad centralizada de autenticación para la red. Active Directory combina capacidades que tradicionalmente se hallaban en sistemas separados y especializados de directorio, como integración

simplificada, gestión y seguridad de los recursos de la red. El paquete SAMBA puede configurarse para usar los servicios de Active Directory desde un controlador de dominio de Windows.

3.1.1.1. LDAP

La aplicación de servidor LDAP proporciona funcionalidad de Servicios de Directorio a ordenadores Windows de una forma muy similar a los servicios de Microsoft Active Directory. Tales servicios incluyen gestionar las identidades y las relaciones entre los ordenadores, usuarios y grupos de ordenadores o usuarios que participan en la red, y proporcionan una forma consistente de describir, localizar y gestionar esos recursos. La implementación de libre distribución disponible en su sistema Ubuntu se llama *OpenLDAP*. Los demonios de servidor responsables de gestionar las peticiones de directorio OpenLDAP, y la propagación de datos de directorio entre un servidor LDAP y otro en Ubuntu, son slapd y slurpd. OpenLDAP puede usarse junto con SAMBA para proporcionar servicios de Archivo, Impresión y Directorio prácticamente de la misma forma que un Controlador de Dominio de Windows, si se compila SAMBA con soporte LDAP.

3.1.1.2. Kerberos

El sistema de autenticación de seguridad Kerberos es un servicio estandarizado que proporciona autenticación a ordenadores y usuarios por medio de un servidor centralizado que concede tickets de autorización cifrados aceptados para la autorización por cualquier otro ordenador que use Kerberos. Los beneficios de la autenticación Kerberos incluyen autenticación mutua, autenticación delegada, interoperabilidad y gestion simplificada de confianzas. Los demonios de servidor primarios para gestionar la autenticación y la administración de la base de datos Kerberos en Ubuntu son krb5kdc y kadmin. SAMBA puede usar Kerberos como mecanismo de autenticación de ordenadores y usuarios contra un Controlador de Dominio de Windows. Para ello, el sistema Ubuntu debe tener instalado Kerberos, y se debe modificar el `/etc/samba/smb.conf` para seleccionar el *reino* adecuado y el modo de *seguridad*. Por ejemplo, edite el archivo `/etc/samba/smb.conf` y añada los valores:

realm = NOMBRE_DE_DOMINIO

secutiry = ADS

en el archivo, y guarde el archivo.

Asegúrese de sustituir el NOMBRE_DE_DOMINIO del ejemplo de arriba con el nombre real de su Dominio Windows.

Necesitará reiniciar los demonios de SAMBA para hacer efectivos estos cambios. Reinicie los demonios de SAMBA introduciendo los siguientes comandos en una linea de comandos:

```
sudo /etc/init.d/samba restart
```

3.1.2. Cuentas de ordenador

Los Servicios de Directorio usan las Cuentas de Ordenador para identificar de forma única a los ordenadores que participan en una red, e incluso las tratan de la misma manera que a los usuarios en términos de seguridad. Las cuentas de ordenador pueden tener contraseñas como las cuentas de usuario, y están sujetas a autorización sobre los recursos de red de la misma forma que las cuentas de usuario. Por ejemplo, si un usuario de la red, con una cuenta válida para una red en particular, intenta autenticarse sobre un recurso de red desde un ordenador que no tiene una cuenta de ordenador válida, dependiendo de las políticas aplicadas en la red, al usuario se le puede denegar el acceso al recurso si el ordenador desde el que usuario está intentando autenticar se considera un ordenador no autorizado.

Las cuentas de ordenador pueden añadirse al archivo de contraseñas de SAMBA, siempre que el nombre del ordenador que se está añadiendo exista como una cuenta de usuario válida en la base de datos local de contraseñas. La sintaxis para añadir una cuenta de ordenador o máquina al archivo de contraseñas de SAMBA es usar la orden smbpasswd desde la línea de órdenes de una terminal de la siguiente forma:

```
sudo smbpasswd -a -m NOMBRE_ORDENADOR
```

Asegurese de reemplazar el NOMBRE_ORDENADOR de muestra en el ejemplo superior con el nombre actual del ordenador al que usted desea crear una cuenta.

3.1.3. Permisos de archivo

Los Permisos de Archivo definen los derechos explícitos que un ordenador o usuario tiene sobre un directorio, archivo o conjunto de archivos particular. Tales permisos puden definirse editando el archivo `/etc/samba/smb.conf` y especificando los permisos explícitos de un recurso compartido dado. Por ejemplo, si tiene definido un recurso compartido SAMBA llamado *sourcedocs* y desea conceder sobre él permisos de *sólo lectura (read-only)* al grupo de usuarios llamado *planning*, pero al mismo tiempo quiere permitir la escritura sobre el recurso al grupo llamado *autores* y al usuario llamado *ricardo*, entonces podría editar el archivo `/etc/samba/smb.conf` y añadir las siguientes entradas bajo la entrada *[sourcedocs]*:

read list = @planning

write list = @authors, richard

Guardar los cambios de `/etc/samba/smb.conf` para que los cambios surtan efecto.

Otro posible permiso consiste en declarar permisos *administrativos* sobre un recurso compartido en particular. Los usuarios que posean permisos administrativos podrán

leer, escribir o modificar cualquier información contenida en el recurso sobre el que el usuario tenga concedidos los permisos administrativos. Por ejemplo, si desea que el usuario *melissa* posea permisos administrativos al recurso compartido *sourcedocs*, puede editar el archivo `/etc/samba/smb.conf` y añadir la siguiente línea debajo de la entrada *[sourcedocs]*:

admin users = melissa

Guardar los cambios de `/etc/samba/smb.conf` para que los cambios surtan efecto.

3.2. Clientes

Ubuntu incluye aplicaciones cliente y la capacidad de acceder a recursos compartidos de red con el protocolo SMB. Por ejemplo, la utilidad llamada smbclient permite el acceso a sistemas de archivos remotos compartidos, de una manera similar al cliente para el Protocolo de Transferencia de Ficheros (FTP). Para acceder a una carpeta compartida llamada *documentos* proporcionado por un ordenador Windows llamado *bill* usando por ejemplo smbclient, uno debería introducir una orden similar a la siguiente en la línea de órdenes:

```
smbclient //bill/documentos -U <nombredeusuario>
```

Se le solicitará la contraseña del usuario especificado en la opción -U, y si la autenticación tiene éxto, se le presentará un intérprete donde podrá introducir órdenes para manipular y transferir archivos en un contexto similar al usado por clientes FTP no-gráficos. Para más información sobre la herramienta smbclient, lea la página del manual de la herramienta con la orden:

```
man smbclient
```

El montaje local de recursos remotos de red usando el protocolo SMB también es posible utilizando la orden mount. Por ejemplo, para montar una carpeta compartida llamada *codigo-proyecto* en un servidor Windows llamado *desarrollo* con el usuario *dlightman* en el punto de montaje /mnt/pcode de su sistema Ubuntu, usted debe introducir la siguiente orden en la línea de órdenes:

```
mount -t smbfs -o username=dlightman //desarrollo/codigo-proyecto /mnt/pcode
```

Después se le solicitará la contraseña del usuario, y después de una autenticación satisfactoria, el contenido del recurso compartido estará disponible localmente por medio del punto de montaje especificado como último argumento en la orden mount. Para desconectarse del recurso compartido, simplemente use la orden umount como usted haría con otros puntos de montaje de su sistema de archivos. Por ejemplo:

```
umount /mnt/pcode
```

3.2.1. Cuentas de usuario

Las Cuentas de usuario definen las personas que tienen algún nivel de autorización para usar ciertos ordenadores y recursos de red. Normalmente, en un entorno de red se le proporciona una cuenta de usuario a cada persona a la que se le permite el acceso a un ordenador o red, donde las políticas y los permisos definen qué a derechos específicos tiene acceso la cuenta de usuario. Para definir usuarios de una red SAMBA en su sistema Ubuntu, debe usar la orden smbpasswd. Por ejemplo, para añadir un usuario SAMBA a su sistema Ubuntu con el nombre de usuario *jseinfeld*, debe introducir lo siguiente en la línea de órdenes:

```
smbpasswd -a jseinfeld
```

La aplicación smbpasswd le pedirá que introduzca una contraseña para el usuario:

```
Nueva contraseña SMB:
```

Introduzca la contraseña que desea asignarle al usuario, y la aplicación smbpasswd le pedirá que la confirme:

```
Vuelva a escribir la nueva contraseña SMB:
```

Confirme la contraseña, y smbpasswd añadirá la entrada para el usuario en el archivo de contraseñas de SAMBA.

3.2.2. Grupos

Los grupos definen una colección de ordenadores o usuarios que tienen un nivel común de acceso a recursos de red particulares, y proporcionan un nivel de granularidad para controlar el acceso a tales recursos. Por ejemplo, si se define un grupo *qa* que contiene los usuarios *freda*, *danika* y *rob*, y se define un segundo grupo *soporte* con los usuarios *danika*, *jeremy* y *vincent*, entonces los recursos de red configurados para permitir el acceso al grupo *qa* habilitarán en consecuencia el acceso a los usuarios freda, danika y rob, pero no a jeremy ni a vincent. Como el usuario *danika* pertenece a los dos grupos *qa* y *support* simultáneamente, podrá acceder a los recursos configurados para poder ser accedidos desde ambos grupos, mientras que los demás usuarios sólo tendrán acceso a los recursos para los que explícitamente tengan acceso los grupos a los que pertenecen tales usuarios.

Al definir grupos en el archivo de configuración de SAMBA, `/etc/samba/smb.conf`, la sintaxis reconocida es anteponer al nombre del grupo el símbolo «@». Por ejemplo, si desea definir un grupo llamado *sysadmin* en alguna sección del archivo `/etc/samba/smb.conf`, lo podrá hacer introduciendo el nombre del grupo como **@sysadmin**.

3.2.3. Políticas de grupo

Las Políticas de grupo definen ciertas configuraciones SAMBA para el Dominio o Grupo de Trabajo al que pertenecen las cuentas de usuario, y otras configuraciones globales para el servidor SAMBA. Por ejemplo, si el servidor SAMBA pertenece a un Grupo de Trabajo de ordenadores Windows llamado *NIVELUNO*, se debe editar el archivo `/etc/samba/smb.conf` y cambiar el siguiente valor de acuerdo a esto:

workgroup = NIVELUNO

Guarde el archivo y reinicie el demonio SAMBA para que los cambios tengan efecto.

Entre otras opciones importantes de política global está *server string*, que define el nombre de servidor NETBIOS que su sistema Ubuntu proporciona a las demás máquinas de la red basada en Windows. Este es el nombre por el que su sistema Ubuntu será reconocido por los clientes Windows y los demás equipos capaces de examinar la red con el protocolo SMB. Además, también puede especificar el nombre y la ubicación del archivo de registro del servidor SAMBA usando la directiva *log file* en el archivo `/etc/samba/smb.conf`.

Algunas de las directivas adicionales que gobiernan la política global del grupo incluyen la especificación de la naturaleza global de todos los recursos compartidos. Por ejemplo, si se colocan ciertas directivas bajo la cabecera *[global]* del archivo `/etc/samba/smb.conf`, éstas afectarán a todos los recursos compartidos a menos que se coloque alguna directiva contradictoria que sustituya a la global en la cabecera particular de algún recurso compartido. Puede especificar que todos los recursos compartidos sean navegables por todos los clientes de la red colocando la directiva *browseable*, que recibe un argumento booleano, bajo la cabecera *[global]* del archivo `/etc/samba/smb.conf`. Es decir: si edita el archivo y añade la línea:

browseable = true

bajo la sección *[global]* del archivo `/etc/samba/smb.conf`, entonces todos los recursos compartidos suministrados por su sistema Ubuntu a través de SAMBA serán navegables por todos los clientes autorizados, a menos que exista algún recurso compartido específico que contenga una directiva *browseable = false*, lo que cancelaría la directiva global.

Otros ejemplos que funcionan de una manera similar son las directivas *public* y *writeable*. La directiva *public* acepta un valor booleano y decide si un recurso compartido en particular será visible por todos los clientes, autorizados o no. La directiva *writeable* también acepta un valor booleano y define si un determinado recurso compartido podrá ser accedido para escritura por todos los clientes de la red.

Apéndice A. Creative Commons by Attribution-ShareAlike 2.0

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE.

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. **Definitions.**
   a. **"Collective Work"** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.
   b. **"Derivative Work"** means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.
   c. **"Licensor"** means the individual or entity that offers the Work under the terms of this License.

d. **"Original Author"** means the individual or entity who created the Work.

e. **"Work"** means the copyrightable work of authorship offered under the terms of this License.

f. **"You"** means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

g. **"License Elements"** means the following high-level license attributes as selected by Licensor and indicated in the title of this License: Attribution, ShareAlike.

2. **Fair Use Rights.** Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. **License Grant.** Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

   a. to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

   b. to create and reproduce Derivative Works;

   c. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works;

   d. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission Derivative Works.

   e. For the avoidance of doubt, where the work is a musical composition:

      i. **"Performance Royalties Under Blanket Licenses."** Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g. webcast) of the Work.

      ii. **"Mechanical Rights and Statutory Royalties."** Licensor waives the exclusive right to collect, whether individually or via a music rights society or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

   f. **"Webcasting Rights and Statutory Royalties."** For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the

compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4. **Restrictions.** The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:
   a. You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested. If You create a Derivative Work, upon notice from any Licensor You must, to the extent practicable, remove from the Derivative Work any reference to such Licensor or the Original Author, as requested.
   b. You may distribute, publicly display, publicly perform, or publicly digitally perform a Derivative Work only under the terms of this License, a later version of this License with the same License Elements as this License, or a Creative Commons iCommons license that contains the same License Elements as this License (e.g. Attribution-ShareAlike 2.0 Japan). You must include a copy of, or the Uniform Resource Identifier for, this License or other license specified in the previous sentence with every copy or phonorecord of each Derivative Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Derivative Works that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder, and You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Derivative Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Derivative Work as incorporated in a Collective Work, but

this does not require the Collective Work apart from the Derivative Work itself to be made subject to the terms of this License.

c. If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Derivative Works or Collective Works, You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied; to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and in the case of a Derivative Work, a credit identifying the use of the Work in the Derivative Work (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Derivative Work or Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. **Representations, Warranties and Disclaimer**

   UNLESS OTHERWISE AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE MATERIALS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. **Limitation on Liability.** EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **Termination**

   a. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Derivative Works or Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in

full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

b. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. **Miscellaneous**

a. Each time You distribute or publicly digitally perform the Work or a Collective Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

b. Each time You distribute or publicly digitally perform a Derivative Work, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

c. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

d. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

e. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, neither party will use the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative

Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time.

Creative Commons may be contacted at *http://creativecommons.org/*.

Apéndice B. GNU Free Documentation License

Version 1.2, November 2002

Free Software Foundation, Inc.
51 Franklin St, Fifth Floor,
Boston,
MA
02110-1301
USA

Version 1.2, November 2002

PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such

manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally

available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with

changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

GNU FDL Modification Conditions

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the *Addendum [105]* below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified

Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in *section 4 [10]1* above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an

"aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified

version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> ### Sample Invariant Sections list
>
> Copyright (c) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

> ### Sample Invariant Sections list
>
> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.