L. Muga

Administrador Servidores Linux

Administración Servidores Linux

Paso a Paso

Instalación y Configuración de un Servidor Multifunción,
VMware Server 2 + Clonezilla Server

(Ver. 1.0)

Administración Servidores Linux

Paso a Paso

L. Muga
Linux Registered User # 487284
Versión 1.0

Software: Debian 4 Linux, VMware Server 2.0, Microsoft Windows XP.

Composición: LaTeX

Índice general

1. Instalación y configuración de un servidor multifunción **5**
- 1.1. Requisitos de hardware . . . 5
- 1.2. Instalando Debian . . . 7
- 1.3. Configuración de red . . . 8
- 1.4. Configuración básica de repositorios . . . 9
- 1.5. Instalando paquetes: Dpkg-dev, Ntp, Dhcp, Samba, NFS, Squid, Squidguard, Sarg, LAMP, Webmin, VMware Server 2, Module Assistant, Proftpd 9

2. Generación de repositorio local **11**

3. Servicio SSH **13**

4. Servicio NTP **15**

5. Servicio DHCP **19**

6. Servicio Proxy - Cache **21**
- 6.1. ACL: Listas de Control de Acceso . . . 26
- 6.2. Squidguard Squid . . . 26
- 6.3. Sarg Squid . . . 32
- 6.4. Bloqueo de Advertising . . . 32
- 6.5. Squid Transparente . . . 33

7. Servicio LAMP **35**
- 7.1. Apache 2 . . . 35
- 7.2. MySQL . . . 36
- 7.3. phpMyAdmin . . . 36
- 7.4. PhpSysInfo . . . 36

8. Servicio Proftpd **37**

9. Servicio Samba **43**

10. Servicio NFS **47**

11. Servicio Webmin **49**

12. VMware Server 2 **51**

13. Clonezilla: clonando sistemas operativos a través de la red **53**

A. Descargar las imágenes ISO de la distribución y grabarlas en medios ópticos (CD/DVD) a través de línea de comandos **55**

B. Comando: alias **57**

C. Listado de distribuciones y LiveCD **59**

D. Configurar Servidor NAT con iptables **69**

E. Instalación de Openbox: Escritorio rápido y ligero **71**

F. Actualizar de Debian 4.0 Etch a Debian 5.0 Lenny **73**

Capítulo 1

Instalación y configuración de un servidor multifunción

1.1. Requisitos de hardware

Una vez que haya reunido información sobre el hardware de su ordenador debe verificar que su hardware le permita realizar el tipo de instalación que desea efectuar. Dependiendo de sus necesidades, podría arreglarse con menos del hardware recomendado listado más abajo. Sin embargo, la mayoría de usuarios se arriesgan a terminar frustrados si ignoran estas sugerencias.
Se recomienda como mínimo un Pentium 4, a 1 GHz para un sistema de escritorio.

Sin escritorio: 64 Megabytes (RAM mínimo), 256 Megabytes (RAM recomendado), 1 Gigabyte de disco duro.

Con escritorio: 64 Megabytes (RAM mínimo), 512 Megabytes (RAM recomendado), 5 Gigabytes d disco duro.

Los requisitos de memoria mínimos necesarios son en realidad inferiores a los indicados arriba. En función de la arquitectura, es posible instalar Debian en sistemas con tan sólo 20 MB (en el caso de s390) a 48 MB (para i386 y amd64). Lo mismo se puede decir del espacio necesario en disco, especialmente si escoge las aplicaciones que se van a instalar manualmente.
Es posible ejecutar un entorno de escritorio gráfico en sistemas antiguos o de gama baja. En este caso es recomendable instalar un gestor de ventanas que es consuma menos recursos que los utilizados en los entornos de escritorio de GNOME o KDE. Algunas alternativas para estos casos son xfce4, icewm y wmaker, aunque hay más entre los que puede elegir.

Es prácticamente imposible dar requisitos generales de memoria y espacio en disco para instalaciones de servidores ya que éstos dependerán en gran medida de aquello para lo que se utilice el servidor.

Recuerde que estos tamaños no incluyen todos los otros materiales que se encuentran habitualmente, como puedan ser los ficheros de usuarios, el correo y otros datos. Siempre

es mejor ser generoso cuando uno está pensando qué espacio destinar a sus propios ficheros y datos.

Una instalación estándar para i386, incluyendo todos los paquetes estándar y el núcleo 2.6 utilizado por omisión, ocupa 397 MB de espacio en disco. Una instalación mínima base sin seleccionar la tarea Sistema estándar ocupará 250 MB.

Importante:
En ambos casos es importante tener en cuenta que este es el espacio después de haber terminado la instalación y de que se hayan borrado todos los ficheros temporales. Tampoco tiene en cuenta la cantidad utilizada por el propio sistema de ficheros, por ejemplo por los ficheros de journal. Esto significa que hace falta bastante más disco durante la instalación y durante el uso habitual del sistema.
Se listan los tamaños indicados por aptitude para las tareas listadas en tasksel. Tenga en cuenta que algunas tareas tienen componentes comunes, de modo que el tamaño total instalado para dos tareas juntas podría ser inferior al total obtenido al sumar sus tamaños individualmente.

Tenga en cuenta que tendrá que añadir los tamaños que se indican en la tabla al tamaño de la instalación estándar para poder determinar el tamaño de sus particiones. La mayoría del espacio en disco que se indica en **Tamaño instalado** acabará utilizándose de /usr y en /lib. Por otro lado, el tamaño que se indica en **Tamaño de descarga** será necesario (temporalmente) en /var.

Entorno de escritorio: 1830 Tamaño instalado (MB), 703 Tamaño de descarga (MB), 2533 Espacio necesario para instalar (MB)

Portátil: 26 Tamaño instalado (MB), 9 Tamaño de descarga (MB), 35 Espacio necesario para instalar (MB)

Servidor Web: 42 Tamaño instalado (MB), 13 Tamaño de descarga (MB), 55 Espacio necesario para instalar (MB)

Servidor de impresoras: 215 Tamaño instalado (MB), 84 Tamaño de descarga (MB), 299 Espacio necesario para instalar (MB)

Servidor de DNS: 3 Tamaño instalado (MB), 1 Tamaño de descarga (MB), 4 Espacio necesario para instalar (MB)

Servidor de ficheros: 74 Tamaño instalado (MB), 29 Tamaño de descarga (MB), 103 Espacio necesario para instalar (MB)

Servidor de correo: 14 Tamaño instalado (MB), 5 Tamaño de descarga (MB), 19 Espacio necesario para instalar (MB)

Base de datos SQL: 50 Tamaño instalado (MB), 18 Tamaño de descarga (MB), 68 Espacio necesario para instalar (MB)

Enlace: http://www.debian.org

1.2. Instalando Debian

1. Configuramos dentro de la BIOS de nuestro sistema la prioridad del dispositivo de arranque; asignando como principal a la lectora de discos.
2. Una vez que tengamos el disco de instalación introducido en nuestra lectora de discos o tengamos ya asignada la imagen en formato .iso en nuestra máquina virtual procedemos a reinciar el equipo (máquina virtual).
3. Procederá a cargar el disco (imagen) de instalación y nos mostrará el logo de Debian, que nos pedirá la pulsación de ENTER para continuar.
4. Ahora seleccionamos el idioma: Spanish (español).
5. Nuestro país: Perú.
6. La distribución del teclado: Latinoamericano.
7. Aquí se nos pedirá la configuración del interfaz de red del equipo, seleccionamos: No configurar la red en este momento.
8. Introducimos el nombre de la máquina para la identificación en la red: admlinux.
9. En el tipo de particionado seleccionamos la opción: Manual.
10. Seleccionamos el disco (sda, hda).
11. Nos preguntará por la creación de la tabla de particiones del disco, seleccionamos: Si.
12. Una vez aquí, seleccionamos la opción ESPACIO LIBRE dentro del disco seleccionado.
13. Ahora: Crear una partición nueva.
14. Especificamos el tamaño de la partición.
15. Tipo de partición: Primario o Lógico.
16. La ubicación de la partición: Principio o Final del disco.
17. Aquí seleccionamos: el sistema de archivos, punto de montaje, las opciones de montaje y la marca de arranque.
18. Una vez creadas las particiones necesarias (recomendadas /, /boot, /cache (para Squid), /repo (para la instalación de servidor de repositorios), /var, /tmp, swap) para nuestro sistema, seleccionamos: Finalizar el particionado y escribir los cambios en el disco.
19. En la confirmación para la escritura de cambios en el disco, seleccionamos: Si.
20. Escribimos la contraseña para root.
21. Confirmamos la contraseña.
22. Escribimos un nombre de cuenta de usuario para las tareas no administrativas del sistema: admlinux.
23. Ahora especificamos el nombre del dueño de la cuenta: admlinux.
24. La contraseña para admlinux.

25. Confirmamos ahora la contraseña.
26. Nos mostrará ahora el progreso de la instalación del sistema.
27. Para el uso de una réplica de red seleccionamos: No.
28. En la entradas comentadas para security.debian.org, seleccionamos: Continuar.
29. En la selección de programas, quitamos las marcas de selección a todos los programas y luego seleccionamos: Continuar.
30. En la instalación de GRUB en el registro principal seleccionamos: Si.
31. En esta etapa ya se ha terminado con la instalación del sistema, seleccionamos: Continuar.
32. Procederá a reiniciar el sistema y luego nos aparecerá el prompt del sistema esperando el ingreso de un usuario del sistema y su contraseña correspondiente.

1.3. Configuración de red

Abrimos el archivo:

vim /etc/network/interfaces

Podemos configurar nuestro interfaz para la obtención de una dirección IP mediante un servidor DHCP o configurarla de manera estática:

Obtención de IP mediante servidor DHCP:

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

1. auto eth0: Instruye que el interfaz será levantado automáticamente cuando el sistema arranque, equivalente a ifup eth0 una vez iniciado el sistema.
2. iface eth0 inet dhcp: Indica que el primer interfaz de red (eth0) será configurado usando un servidor DHCP.

Configuración IP estática:

```
auto eth0
iface eth0 inet static
address 192.168.50.xxx
netmask 255.255.255.0
network 192.168.50.0
gateway 192.168.50.1
broadcast 192.168.50.255
```

1. auto eth0: Instruye que el interfaz será levantado automáticamente cuando el sistema arranque, equivalente a ifup eth0 una vez iniciado el sistema.

2. iface eth0 inet static: Indica que el primer interfaz de red (eth0) será configurado manualmente con los parámetros definidos.
3. address: cada interfaz de red conectada a una red IP es identificada por una IP única de cuatro bytes (32 bits).
4. netmask: es un número que establece qué parte de la IP de un host corresponde a la red y qué parte corresponde a la máquina.
5. network: IP que define el identificador de red.
6. broadcast : es la IP a la que se mandan los paquetes que deben recibir todas las máquinas de la red
7. gateway: es la IP de la máquina de nuestra LAN a través de la cual salimos hacia el exterior.

1.4. Configuración básica de repositorios

Para la selección, descarga e instalación de paquetes para nuestro sistema, tendremos que hacer uso de los repositorios que tiene Debian publicados. Entonces abrimos nuestro archivo de configuración de repositorios:

vim /etc/apt/sources.list

Y agregamos/descomentamos las siguientes lineas:

deb http://security.debian.org/ etch/updates main contrib
deb-src http://security.debian.org/ etch/updates main contrib
deb ftp://ftp.debian.org/debian/ stable main contrib non-free

Finalmente ejecutamos el comando:

apt-get update

para la actualización de la lista de paquetes.

1.5. Instalando paquetes: Dpkg-dev, Ntp, Dhcp, Samba, NFS, Squid, Squidguard, Sarg, LAMP, Webmin, VMware Server 2, Module Assistant, Proftpd

Para la instalación de la paquetería usamos el comando:

apt-get install nombre.del.paquete nombre.del.paquete2

1. apt: APT son las siglas de Advanced Package Tool. Es un sistema de gestión de paquetes de software desarrollado por el Proyecto Debian
2. apt-get: es la utilidad desde línea de comando para el uso de APT.

3. apt-get install nombre.de.paquete: Con nuestra lista de repositorios correctamente configurada, ahora se procederá a la búsqueda, descarga e instalación del paquete seleccionado (nombre.del.paquete).

apt-get install openssh-server dhcp3-server dpkg-dev samba smbfs squid nfs-kernel-server ntp ntpdate apache2 apache2-doc php5 libapache2-mod-php5 (php4 libapache2-mod-php4) mysql-server mysql-client php5-mysql (php4-mysql) mysql-server mysql-client libmysqlclient15-dev phpsysinfo phpmyadmin module-assistant phpsysinfo proftpd

Ahora instalaremos Webmin; es una herramienta de administración de sistemas (programas/servicios) vía web, haciendo uso de módulos. Primero descargamos el paquete correcto desde su página (con extensión .deb):

www.webmin.com

Luego para la instalación del paquete .deb usaremos el comando dpkg:

dpkg —install webmin.xx.deb

Ahora ejecutaremos el comando:

m-a prepare

m-a hace referencia a module-assistant, el argumento prepare determinará si contamos con todo lo necesario para la compilación del módulos, en caso no sea esto cierto, module-assistant se encargará de descargar e instalar lo que haga falta. Lo más usual es que no contemos con las cabeceras del núcleo (kernel-headers), siendo totalmente necesarias en nuestro caso para la instalación de VMware Server 2.

Descargamos el archivo correspondiente a VMware Server 2 con extensión .tar.gz desde la dirección: http://www.vmware.com/download/server/, para eso debemos haber creado anteriormente una cuenta correspondiente en VMware; la cual nos servirá también para la obtención del código de activación correspondiente. Supongamos que descargamos el paquete dentro de la ruta: /home/vmware

cd /home/vmware
tar xvfz VMware-server-*.tar.gz
cd vmware-server-distrib
./vmware-install.pl

Y procedemos a responder a las preguntas con los valores que corresponda, la mayor parte de ellos serán los valores por defecto.

Capítulo 2

Generación de repositorio local

Si nos encontramos ante el caso de instalar un número elevado de computadoras en nuestra red, las cuales no cuentan con un ancho de banda hacia Internet elevado o no contamos con el mismo, es posible que la instalación de paqueteria y/o la actualización de del sistema se efectúe en periodos elevados de tiempo.
Seria necesario el poder contar con una réplica local en nuestra red local (LAN) para la descarga, instalación y actualización de paquetes sobre los equipos clientes.
Para la creación de un repositorio local necesitaremos los 3 DVD (si no cuenta con los DVD y desea descargarlos utilice como ayuda el Apéndice A) de instalación de la distribución (Debian 4).

Nota:
Todos los comandos son ejecutados como root. También vamos a eliminar todo el contenido del archivo de repositorios con el siguiente comando:

echo ≥ /etc/apt/sources.list

1. Necesitamos descargar y/o adquirir los DVD de la distribución (http://www.debian.org).
2. Adicionalmente necesitamos unos 14 o 15 GB de espacio en disco duro (o preferiblemente una partición con el espacio mencionado).
3. Dpkg-dev y servidor web Apache instalado (ruta por defecto /var/www).
4. En el espacio asignado para la tarea crearemos una carpeta denominada y dentro de la ruta para la publicación de Apache: **/repo**.

   mkdir /repo o mkdir -p /ruta.previa/repo

5. Creamos un enlace simbólico del directorio creado a la ruta donde Apache apunta (/var/www/):

   ln -s /repo /var/www/

6. Ahora copiamos todo el contenido de los 3 DVDs de la siguiente manera (debemos montar cada uno de los discos que utilicemos: **mount /dev/cdrom** y para desmontarlo: **mount /dev/cdrom**).

cp -R /cdrom/dists/ /repo
cp -R /cdrom/pool/ /repo

7. Ahora eliminamos los siguientes archivos:

rm -rf /repo/dists/etch/main/debian-installer/
rm /repo/dists/etch/Release

8. Ahora nos dirigimos al directorio donde copiamos los paquetes:

cd /repo/

9. Procedemos a escanear y comprimir los paquetes (main) y (dists):

1. dpkg-scanpackages pool/main/ /dev/null ≥
dists/etch/main/binary-i386/Packages
gzip dists/etch/main/binary-i386/Packages
2. dpkg-scanpackages pool/contrib/ /dev/null ≥
dists/etch/contrib/binary-i386/Packages
gzip dists/etch/contrib/binary-i386/Packages

10. Si todo culminó correctamente verifiquemos si puede ser accedido via web:

http://127.0.0.1/repo

11. Procedemos a editar en los clientes el listado de repositorios, agregamos el repositorio local editando el archivo: **/etc/apt/sources.list**, insertamos:

deb http://ip.del.servidor/repo/ etch main contrib

12. Y ejecutamos el comando:

apt-get update

Nota 2:
Podemos además agregar a la lista de repositorios los DVD de instalación de Debian para el uso de cada equipo individual con el siguiente comando (una recomendación personal es agregar los 3 DVD de la distribución para evitarnos de dependencias incompletas):

apt-cdrom add

Capítulo 3

Servicio SSH

Una vez ya instalado este servicio (openssh-server), procedemos a editar las opciones que trae por defecto para evitar problemas de seguridad:

1. Abrimos el siguiente archivo:

   vim /etc/ssh/sshd_config

2. El puerto conocido para el servidor SSH es el TCP 22, o puerto 22 mayormente conocido. Es recomendable cambiar el puerto para tratar de ocultar el servicio que corre sobre nuestro servidor:

   Port 22

   Hacemos un cambio al puerto 2222 por ejemplo:

   Port 2222

3. Podemos deshabilitar el logueo como root:

   PermitRootLogin yes

   Cambiamos el yes por no:

   PermitRootLogin no

4. Por defecto el servidor escucha sobre todas la redes, podemos configurarlo por ejemplo para que solo permita los accesos desde nuestra red local (considerando que nuestro servidor tiene configurado en su interfaz para la red local la IP:192.168.50.1):

   ListenAddress 0.0.0.0

   Por:

   ListenAddress 192.168.50.1

5. Podemos también restringir el acceso de usuarios mediante el parámetro AllowUsers (en caso de que no se encuentre en el archivo de configuración lo creamos al final):

   AllowUsers admlinux admlinux2

Adicionalmente restringimos el acceso de los usuarios solo desde sus terminales o ciertos host de la red:

AllowUsers admlinux@192.168.50.10 admlinux2@192.168.50.11

6. Reiniciamos nuestro servicio:

/etc/init.d/ssh restart

Nota :
Un cliente muy cómodo desde entornos Windows es: PuTTY.

Capítulo 4

Servicio NTP

Network Time Protocol (NTP) es un protocolo de red para sincronizar el reloj de un computador con la hora de una fuente de referencia, logrando una precisión de orden de milisegundos con respecto a la Hora Universal Coordinada (UTC). La hora UTC, que ha sido adoptado como la escala de tiempo estándar por la mayoría de las naciones del mundo, es basada en la rotación de la Tierra alrededor de su eje y en el calendario Gregoriano, que a su vez es basado en la rotación de la Tierra alrededor del Sol.

La hora UTC es diseminada a través de receptores especiales, como radios, satélites o módems, manejados por los gobiernos de varias naciones del mundo. Un número limitado de computadores están equipados con estos receptores y actúan como servidores de tiempo primarios (stratum 1), usados para sincronizar un número mucho mayor de servidores secundarios (stratum 2), que a su vez sincronizan a clientes ternarios (stratum 3) a través de protocolos de sincronización, como NTP, cuyos daemons a la vez actúan como servidores para sincronizar aún más clientes. Esto crea una cascada de servidores sincronizados.

¿Por qué sincronizar el reloj? Las ventajas son muchas y las desventajas ninguna. El reloj sincronizado con NTP está siempre a la hora oficial y no es necesario ajustarlo cada cierto tiempo. Los problemas asociados a un reloj desincronizado son múltiples. Por ejemplo, el sello de tiempo cuando se crea o modifica un archivo puede quedar con la hora y fecha equivocada. El correo electrónico que envías desde el computador podría llevar un sello de tiempo equivocado. ¿No te ha sucedido que has recibido correo con fechas totalmente erróneas?

Los computadores poseen en su circuito un reloj bastante inexacto, llamado reloj CMOS o reloj del hardware. Hemos comprobado que el drift típico del reloj del hardware en nuestros computadores es de unos 20 segundos por día. Esa es la inexactitud típica de un reloj de hardware que funciona correctamente. No es raro en computadores viejos que éste reloj esté defectuoso, probablemente debido a una batería descargada. Cuando el computador arranca, el reloj del sistema (el que ves en la barra del escritorio) se coloca según el reloj del hardware. Por eso sucede que al arrancar el computador, el reloj del sistema aparece a una hora y fecha descolocada, a pesar de haber sido puesto a la hora correcta recientemente. Esto se debe a la inexactitud o defecto del reloj del hardware.

Enlace: http://ftp.cl.debian.org/man-es

1. Primero necesitamos tener instalados los paquetes ntp y ntpdate. Luego procedemos a configurar el servicio modificando el siguiente archivo:

   vim /etc/ntp.conf

2. El contenido del archivo es el siguiente:
   #/etc/ntp.conf, configuration for ntpd

   driftfile /var/lib/ntp/ntp.drift
   statsdir /var/log/ntpstats/

   statistics loopstats peerstats clockstats
   filegen loopstats file loopstats type day enable
   filegen peerstats file peerstats type day enable
   filegen clockstats file clockstats type day enable

   # You do need to talk to an NTP server or two (or three).
   #server ntp.your-provider.example

   # pool.ntp.org maps to more than 300 low-stratum NTP servers.
   # Your server will pick a different set every time it starts up.
   # *** Please consider joining the pool! ***
   # *** ***
   server 0.debian.pool.ntp.org iburst
   server 1.debian.pool.ntp.org iburst
   server 2.debian.pool.ntp.org iburst
   server 3.debian.pool.ntp.org iburst

   # By default, exchange time with everybody, but don't allow configuration.
   # See /usr/share/doc/ntp-doc/html/accopt.html for details.
   restrict -4 default kod notrap nomodify nopeer noquery
   restrict -6 default kod notrap nomodify nopeer noquery

   # Local users may interrogate the ntp server more closely.
   restrict 127.0.0.1
   restrict ::1

   # Clients from this (example!) subnet have unlimited access,
   # but only if cryptographically authenticated
   #restrict 192.168.123.0 mask 255.255.255.0 notrust

   # If you want to provide time to your local subnet, change the next line.
   # (Again, the address is an example only.)
   #broadcast 192.168.123.255

   # If you want to listen to time broadcasts on your local subnet,

de-comment the next lines. Please do this only if you trust everybody

on the network!

#disable auth
#broadcastclient

3. En esta configuración vamos a usar la siguiente lista de servidores y eliminar o comentar la por defecto:

#server 0.debian.pool.ntp.org iburst
#server 1.debian.pool.ntp.org iburst
#server 2.debian.pool.ntp.org iburst
#server 3.debian.pool.ntp.org iburst
server ntp0.pipex.net
server ntp1.pipex.net
server time.nist.gov

4. Si nuestro servidor va a proveer sincronización a otros equipos de la red (pcs u otros servidores), debemos definir las redes a las cuales el servidor aceptará sincronizaciones ntp:

restrict 192.168.50.0 mask 255.255.255.0 nomodify notrap

5. Una vez hechos los cambios en el archivo de configuración, reiniciamos el servicio:

/etc/init.d/ntp restart

6. En un cliente Linux podemos ejecutar el siguiente comando para sincronizar la hora en esa estación (como root):

ntpdate ip.del.servidor

7. Si obtiene un error anunciando: **the NTP socket is in use, exiting**; significa que ntp ya se encuentra corriendo, para eso tendremos que eliminar todos los procesos ntpd con el siguiente comando:

killall ntpd

Capítulo 5

Servicio DHCP

El servicio de DHCP requiere de un servidor el cual asignará direcciones IPde manera dinámica a todo equipo (host) que se conecte a esa red o segmento de red, el protocolo entrega información a la redes de área local (LAN) o LAN Virtuales (VLAN); reduciendo el tiempo y trabajo de administración de una manera considerable ya que los adaptadores de red de los equipos clientes no necesitan configurarse de manera manual o estática la dirección IP, máscara, puerta de enlace, etc.

1. Debemos tener instalado el paquete: dhcp3-server
2. Podemos optar por eliminar todo el contenido del archivo de configuración (recordar siempre guardar un backup o respaldo de cada archivo de configuración que edite) o modificar el existente. Para nuestro caso eliminaremos todo el contenido y crearemos el nuestro.

   echo /etc/dhcp3/dhcpd.conf

3. Editamos el archivo de configuración:

   vim /etc/dhcp3/dhcpd.conf

4. Ingresamos el siguiente texto:

   subnet 192.168.50.0 netmask 255.255.255.0 {
   option domain-name "infouni.com"; option domain-name-servers 208.67.222.222;
   option subnet-mask 255.255.255.0;
   default-lease-time 3600;
   max-lease-time 7200;
   option routers 192.168.50.1;
   option broadcast-address 192.168.50.255;
   }

   - subnet 192.168.50.0 netmask 255.255.255.0 { }: define el segmento de red al que asignará direcciones.
   - option domain-name "infouni.com";: El domino por defecto en la red.
   - option domain-name-servers 208.67.222.222;: establece el servidor DNS para navegación web de los clientes.

- option subnet-mask 255.255.255.0;: Especifica la máscara de red asignada a los clientes.
- default-lease-time 3600;: Indica el tiempo de asignación en segundos.
- max-lease-time 7200;: Tiempo máximo de asignación en segundos.
- option routers 192.168.50.1;: La puerta de enlace para los equipos de la red.
- option broadcast-address 192.168.50.255;: Dirección de difusión de la red.

5. Podemos además establecer clientes DHCP con direcciones IP fijas. DHCP también se puede utilizar para asignar una dirección estática predefinida a un cliente específico para cada petición.

   Para identificar a cada cliente de la red se utiliza la dirección MAC (dirección física) de cada host, que es un código numérico fijo y único.

   ```
   host computadora1 {
   hardware ethernet 00:00:45:12:EE:F4;
   fixed-address 192.168.50.21;
   }
   ```

   - host computadora1 { }: definimos el nombre del host de la red.
   - hardware ethernet 00:00:45:12:EE:F4;: dirección MAC del equipo.
   - fixed-address 192.168.50.21;: dirección IP asignada al equipo con la dirección MAC definida anteriormente.

6. Tenemos el caso en que nuestro servidor necesita asignar direcciones IP a 2 o más segmentos de red en conectados en interfaces de red distintas.

   Para ello vamos a definir los interfaces de red (eth0, eth1) en el parámetro INTERFACES del archivo :

   vim /etc/default/dhcp3-server

   Para finalizar podemos decir también que nuestro servidor DHCP nos permite la negación de direcciones IP a ciertos equipos por su dirección MAC:

   ```
   host equipo.dañino {
   hardware ethernet 00:00:00:00:00:0;
   deny booting;
   }
   ```

   - deny booting;: el servidor no entrega una dirección IP al equipo con la MAC especificada arriba.

7. Una vez realizados los cambios sobre el archivo de configuración reiniciamos el servicio:

   /etc/init.d/dhcp3-server restart

Capítulo 6

Servicio Proxy - Cache

El término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

En general la palabra proxy se usa en muchas situaciones en donde tiene sentido un intermediario:

–El uso más común es el de servidor proxy, que es un ordenador que intercepta todas las conexiones de red que un cliente hace a un servidor de destino.
–De ellos, el más famoso es el servidor proxy de web (comúnmente conocido solamente como «proxy»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc.
–También existen proxies para otros protocolos, como el proxy de FTP.
–El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.
Como se ve, proxy tiene un significado muy general, aunque siempre es sinónimo de intermediario. También se puede traducir por delegado o apoderado (el que tiene el poder).

En general, los proxies hacen posibles varias cosas nuevas:

–Control: El intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
–Ahorro: Por tanto, sólo uno de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
–Velocidad. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
–Filtrado: El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
–Modificación: Un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
–Anonimato: Si todos los usuarios se identifican como uno sólo, es difícil que el recurso

accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Desventajas:
El uso de un intermediario puede provocar:

–Abuso. Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.
–Carga. Un proxy ha de hacer el trabajo de muchos usuarios.
–Intromisión. Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.
–Incoherencia. Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en cache sigue siendo la misma que la existente en el servidor remoto.
–Irregularidad. El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

Funcionamiento:
Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (p.ej.: una página web) en una caché que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de proxy se agrupan diversas técnicas.

Proxy de web / Proxy cache de web:
El proxy para el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una caché para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

Funcionamiento:
–El cliente realiza una petición (mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.
–Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto, si la página no ha cambiado desde que se cargo en caché la devuelve inmediatamente, ahorrándose de esta manera mucho tráfico pues solo intercambia un paquete para comprobar la versión, si la versión es antigua o simplemente no se encuentra en la caché, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones. El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el

usado menos recientemente, en inglés Least Recently Used) y el LFU (el usado menos frecuentemente, Least Frequently Used). Los proxies web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como proxies Web. Otros tipos de proxy cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA. Algunos operadores de red también tienen proxies para interceptar virus y otros contenidos hostiles servidos por páginas Web remotas.

Ejemplo:
Un cliente de un ISP manda una petición a Google la cual llega en un inicio al servidor Proxy que tiene este ISP, no va directamente a la dirección IP del dominio de Google. Esta página concreta suele ser muy solicitada por un alto porcentaje de usuarios, por lo tanto el ISP la retiene en su Proxy por un cierto tiempo y crea una respuesta en mucho menor tiempo. Cuando el usuario crea una búsqueda en Google el servidor Proxy ya no es utilizado; el ISP envía su petición y el cliente recibe su respuesta ahora sí desde Google.

Otros Usos:
Como método extra y de ayuda en las descargas mediante aplicaciones P2P; el cual es usado en Lphant y algunos Mods del Emule.

Ventajas:
–Ahorro de Tráfico: Las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.
–Velocidad en Tiempo de respuesta: El servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.
–Demanda a Usuarios: Puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.
–Filtrado de contenidos: El servidor proxy puede hacer un filtrado de páginas o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo de valores y características de lo que no se permite, creando una restricción cuando sea necesario.
–Modificación de contenidos: Basándose en la misma función del filtrado, y llamado Privoxy, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

Desventajas:
–Las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché. Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona habitualmente para un proxy.
–El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos.
–Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas.

Proxy Transparente:
Muchas organizaciones (incluyendo empresas, colegios y familias) usan los proxies para

reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché. Normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Por lo tanto, el usuario puede evadir el proxy cambiando simplemente la configuración. Una ventaja de tal es que se puede usar para redes de empresa.
Un proxy transparente combina un servidor proxy con NAT de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Este es el tipo de proxy que utilizan los proveedores de servicios de internet (ISP). En España, la compañía más expandida en cuanto a ADSL se refiere, ISP Telefónica, dejó de utilizar proxy transparente con sus clientes a partir de Febrero de 2006.

Reverse Proxy:
Un reverse proxy es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy. Hay varias razones para instalar un reverse proxy :

–Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.
–Cifrado / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el reverse proxy , el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).
–Distribución de Carga: el reverse proxy puede distribuir la carga entre varios servidores web. En ese caso, el reverse proxy puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).
–Caché de contenido estático: Un reverse proxy puede descargar los servidores web almacenando contenido estático como imágenes u otro contenido gráfico.

Proxy NAT (Network Address Translation) / Enmascaramiento:
Otro mecanismo para hacer de intermediario en una red es el NAT. La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el enmascaramiento).

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó. Estas direcciones privadas se suelen elegir en rangos prohibidos para su uso en Internet como 192.168.x.x, 10.x.x.x, 172.16.x.x y 172.31.x.x Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya

sido determinada para tal fin en el propio proxy. La función de NAT reside en los Cortafuegos y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un mero encaminador.

Proxy Abierto:
Este tipo de proxy que acepta peticiones desde cualquier ordenador, esté o no conectado a su red. En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de spam. Un proxy se usa, normalmente, para almacenar y redirigir servicios como el DNS o la navegación Web, mediante el cacheo de peticiones en el servidor proxy, lo que mejora la velocidad general de los usuarios. Este uso es muy beneficioso, pero al aplicarle una configuración abierta a todo internet, se convierte en una herramienta para su uso indebido. Debido a lo anterior, muchos servidores, como los de IRC, o correo electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras (BlackList).

Enlace: http://es.wikipedia.org/wiki/Proxy

1. Necesitamos tener instalado el paquete squid.

   apt-get install squid

2. Definamos primero las líneas a editar dentro del archivo:

3. visible_hostname: Define el nombre del servidor.

4. http_port. Este parámetro define en que puerto responderá a las solicitudes Squid. Usaremos el puerto 3128

5. cache_mem. Memoria utilizada por Squid para ciertos procesos.

6. cache_dir. Directorio de ubicación del cache. Este parámetro incluye tres parámetros numéricos adicionales. El primero incluye el número de MB que se utilizarán en este directorio para el cache, por defecto 100MB, el segundo el número de directorios a utilizar en el primer nivel (16 por defecto) y el tercero el número de subdirectorios en el segundo nivel (256 por defecto):

7. acl: (Lista de Control de Acceso) Con ésta línea determinamos quien accederá a Internet a través del proxy y quien no.

8. http_access: Permite el acceso o denegación a las listas de control de acceso (ACL).

visible_hostname Servidor Proxy
http_port 3128
cache_mem 128 MB
cache_dir ufs /squid 1024 16 256
acl redinterna src 192.168.50.0/255.255.255.0
http_access allow redinterna

6.1. ACL: Listas de Control de Acceso

Las listas de control de acceso nos permiten controlar los recursos o los equipos que pueden tener acceso a nuestra red. Vamos a definir ahora algunos tipos de ACL:

1. src: Especifica la dirección origen de la conexión (en formato IP/Máscara).
2. dst: Especifica la dirección destino de la conexión (en formato IP/Máscara)
3. srcdomain, dstdomain: Especifica un nombre de dominio origen. Y dstdomain comprueba el dominio que se haya especificado en la petición de página web.
4. time: Permite especificar el horario en el que se tendrá acceso a Internet.
5. url_regex: Permite especificar expresiones para comprobar en una URL. Denegando la petición si coinciden con la regla.

6.2. Squidguard Squid

1. Necesitamos tener instalado el paquete de squidguard:

   apt-get install squidguard

2. Descargamos la lista negra de direcciones web (http://urlblacklist.com):

   http://urlblacklist.com/cgi–bin/commercialdownload.pl?type=download&file=bigblacklist

3. Descomprimimos el archivo:

   tar xvzf bigblacklist.tar.gz

4. Movemos el contenido a el directorio de base de datos de Squidguard:

   mv blacklists/* /var/lib/squidguard/db/

5. Ahora debemos asociar el Squidguard al Squid, añadiendo o desdocumentando las siguientes líneas:

   vim /etc/squid/squid.conf
   redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf
   redirect_children 20

6. Para mayor facilidad (aunque no lo recomiendo), asignaremos todos los permisos y propietario (root) a los archivos de la base de datos de SquidGuard:

   chmod 777 -R /var/lib/squidguard/db/*
   chown -R root:root /var/lib/squidguard/db/*

7. Editamos el archivo de configuración de SquidGuard:

   vim /etc/squid/squidGuard.conf

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard/db
logdir /var/log/squid

#
# TIME RULES:
# abbrev for weekdays:
# s = sun, m = mon, t =tue, w = wed, h = thu, f = fri, a = sat

time workhours {

weekly mtwhf 08:00 - 16:30
date *-*-01 08:00 - 16:30
}
#
# REWRITE RULES:
#

#rew dmz {
# s@://admin/@://admin.foo.bar.no/@i
# s@://foo.bar.no/@://www.foo.bar.no/@i
#}

#
# SOURCE ADDRESSES:
#

#src admin {
# ip 1.2.3.4 1.2.3.5
# user root foo bar
# within workhours
#}

#src foo-clients {
# ip 172.16.2.32-172.16.2.100 172.16.2.100 172.16.2.200
#}

#src bar-clients {
# ip 172.16.4.0/26
#}

#
# DESTINATION CLASSES:
#

dest good {
```

```
}

dest local {
}

dest ads {
domainlist ads/domains
urllist ads/urls
expressionlist ads/expressions
}
dest adult {
domainlist adult/domains
urllist adult/urls
}
dest aggessive {
domainlist aggressive/domains
urllist aggressive/urls
}
dest antispyware {
domainlist antispyware/domains
urllist antispyware/urls
}
dest artnudes {
domainlist artnudes/domains
urllist artnudes/urls
}
dest astrology {
domainlist astrology/domains
}
dest audio-video {
domainlist audio-video/domains
urllist audio-video/urls
}
dest beerliquorsale {
domainlist beerliquorsale/domains
}
dest beerliquorinfo {
domainlist beerliquorinfo/domains
}
dest blog {
domainlist blog/domains
urllist blog/urls
}
dest chat {
domainlist chat/domains
urllist chat/urls
}
dest childcare {
domainlist childcare/domains
```

```
urllist childcare/urls
}
dest clothing {
domainlist clothing/domains
}
dest culinary {
domainlist culinary/domains
}
dest dating {
domainlist dating/domains
urllist dating/urls
}
dest desktopsillies {
domainlist desktopsillies/domains
urllist desktopsillies/urls
}
dest dialers {
domainlist dialers/domains
urllist dialers/urls
}
dest drugs {
domainlist drugs/domains
urllist drugs/urls
}
dest ecommerce {
domainlist ecommerce/domains
urllist ecommerce/urls
}
dest entertainment {
domainlist entertainment/domains
urllist entertainment/urls
}
dest filehosting {
domainlist filehosting/domains
}
dest games {
domainlist games/domains
urllist games/urls
}
dest gardening {
domainlist gardening/domains
}
dest hacking {
domainlist hacking/domains
urllist hacking/urls
}
dest homerepair {
domainlist homerepair/domains
urllist homerepair/urls
```

```
}
dest hygiene {
domainlist hygiene/domains
}
dest instantmessaging {
domainlist instantmessaging/domains
urllist instantmessaging/urls
}
dest jewelry {
domainlist jewelry/domains
}
dest kidstimewasting {
domainlist kidstimewasting/domains
urllist kidstimewasting/urls
}
dest marketingware {
domainlist marketingware/domains
}
dest medical {
domainlist medical/domains
urllist medical/urls
}
dest mixed_adult {
domainlist mixed_adult/domains
}
dest naturism {
domainlist naturism/domains
urllist naturism/urls
}
dest onlinegames {
domainlist onlinegames/domains
urllist onlinegames/urls
}
dest pets {
domainlist pets/domains
urllist pets/urls
}
dest phishing {
domainlist phishing/domains
urllist phishing/urls
}
dest porn {
domainlist porn/domains
urllist porn/urls
expressionlist porn/expressions
}
dest proxy {
domainlist proxy/domains
urllist proxy/urls
```

```
}
dest radio {
domainlist radio/domains
urllist radio/urls
}
dest ringtones {
domainlist ringtones/domains
}
dest sexuality {
domainlist sexuality/domains
urllist sexuality/urls
}
dest shopping {
domainlist shopping/domains
}
#dest spyware {
#domainlist spyware/domains
#urllist spyware/urls
#}
dest violence {
domainlist violence/domains
urllist violence/urls
}
dest virusinfected {
domainlist virusinfected/domains
urllist virusinfected/urls
}
dest warez {
domainlist warez/domains
urllist warez/urls
}
dest weapons {
domainlist weapons/domains
urllist weapons/urls
}
acl {
default {
pass !ads !adult !aggessive !antispyware !artnudes !astrology !audio-video
!beerliquorsale !beerliquorinfo !blog !chat !childcare !clothing !culinary
!dating !desktopsillies !dialers !drugs !ecommerce !entertainment all
redirect http://www.google.com }
}
```

8. Convertimos las blacklists a un formato de base de datos para su consulta:

squidGuard -C all

9. Para verificar el estado de SquidGuard, utilizaremos el archivo de log. Si ha finalizado correctamente debe mostrarnos algo parecido a:

tail -f /var/log/squid/squidGurad.log

create new dbfile /var/lib/squidguard/db/weapons/urls.db

10. Reiniciamos Squid:

/etc/init.d/squid restart

6.3. Sarg Squid

Sarg es un programa que nos permite ver los informes de Squid en la red, nos permite mostrar: direcciones IP, páginas web visitadas, tráfico generado, etc.

1. Necesitamos tener instalado el paquete Sarg:

apt-get install sarg

2. Para la generación de reportes simplemente ejecutamos:

sarg

3. Los reportes serán generados por defecto en: /var/www/squid-reports.
4. Podemos acceder a los reportes abriendo un navegador web desde cualquier equipo dentro de la red y colocando como dirección: http://IP.del.servidor/squid-reports.
5. Veamos ahora las principales líneas de configuración:

vim /etc/squid/sarg.conf

–language English : El idioma que sarg muestra en las opciones.
–access_log /var/log/squid/access.log : Indicamos el archivo de donde vamos a sacar los registros. Por defecto viene a ser el archivo de log de Squid.
–title Squid User Access Reports : El título que se vizualizará en la barra de título de la ventana de navegación.
–output_dir /var/www/squid-reports : Indicamos el archivo de salida de registros.
–resolve_ip yes o no : Nos permite decidir si deseamos mostrar las direcicones IP de los clientes.

6.4. Bloqueo de Advertising

1. Ingresamos al siguiente enlace, copiamos toda la lista de servidores y las guardamos en el siguiente archivo:

http://pgl.yoyo.org/adservers/serverlist.php?hostformat=squid-dstdom-regex
vim /etc/squid/ads

2. Abrimos el archivo de configuración de Squid y agregamos las siguientes lineas en los ACL:

acl ads dstdom_regex -i "/etc/squid/ads"
http_access deny ads

3.

6.5. Squid Transparente

1. Abrimos el archivo de configuración de Squid y agregamos la palabra: transparent, donde indicamos el puerto del servicio Squid.

http_port 3128 transparent

2. Habilitamos el bit de forward, NAT y el direccionamiento de puerto (de 80 a 3128):

echo 1 >/proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A PREROUTING -i eth0 -p tcp —dport 80 -j REDIRECT —to-port 3128

3. Permitimos el acceso al puerto 80 en el servidor:

iptables -A INPUT -p tcp —dport 80 -j ACCEPT

Capítulo 7

Servicio LAMP

LAMP es escencialmente un servidor corriendo un sistema operativo Linux, Apache, MySQL y Php/Perl. Procederemos ahora a configurar cada uno de los servicios, pero primero definamos cada uno de ellos:

Necesitamos tener instalados los siguientes paquetes:

apache2 apache2-doc php5 libapache2-mod-php5 (php4 libapache2-mod-php4) mysql-server mysql-client php5-mysql (php4-mysql) mysql-server mysql-client libmysqlclient15-dev phpsysinfo phpmyadmin phpsysinfo

1. Apache 2 - Servidor Web Linux
2. MySQL 5 - Servidor de Base de Datos
3. PHP5 - Lenguaje script
4. phpMyAdmin - Software de administración de base de datos via web.
5. PhpSysInfo - Muestra información acerca de nuestro sistema.
6. Awstats - Analizador de estadísticas web.

7.1. Apache 2

El archivo de confuguración de Apache se encuentra en la ruta:

/etc/apache2/apache2.conf

Y la ruta donde se almacena el contenido web:

/var/www

Para verificar la correcta instalación de PHP5, vamos a crear el ya conocido archivo test.php con el comando phpinfo:

vim /var/www/apache2-default/test.php
<?php phpinfo(); ?>

Abrimos un navegador web e ingresamos a la siguiente dirección:

http://IP.del.servidor/apache2-default/test.php

7.2. MySQL

El archivo de configuración se encuentra en:

/etc/mysql/my.cnf

Por defecto MySQL en su instalación crea un usuario root sin clave, lo cual resulta un riesgo de seguridad para los datos almacenados en las bases de datos. Vamos ahora a crear una clave para el usuario root:

mysql -u root
mysql>USE mysql;
mysql>UPDATE user SET Password=PASSWORD('clave.nueva') WHERE user='root';
mysql>FLUSH PRIVILEGES;

7.3. phpMyAdmin

El archivo de configuración se encuentra localizado en:

/etc/phpmyadmin

Para poder acceder a phpMyAdmin desde los sitios web necesitamos añadir la siguiente línea en el archivo de configuración de Apache2 (http://IP.del.servidor/phpmyadmin/):

vim /etc/apache2/apache2.conf
Include /etc/phpmyadmin/apache.conf

Para finalizar reiniciamos el servidor Apache:

/etc/init.d/apache2 restart

7.4. PhpSysInfo

El archivo de configuración se encuentra en:

/etc/phpsysinfo/config.php

Podemos cambiar el lenguaje en que se muestra el contenido (de inglés a español), abrimos el archivo de configuración:

vim /var/phpsysinfo/config.php

Y modificamos la siguiente línea: **$default_lng="en"** por **$default_lng="es"** y guardamos el archivo.

Capítulo 8

Servicio Proftpd

ProFTPd es un servidor FTP. Se promociona desde su página web como estable y seguro, cuando se configura correctamente. El servidor ProFTPd se promociona a sí mismo como un Software servidor FTP altamente configurable con licencia GPL.

Enlace: http://es.wikipedia.org/wiki/ProFTPd

1. Necesitamos tener instalado el paquete proftpd.

2. El archivo de configuración se encuentra en:

   /etc/proftpd/proftpd.conf

3. Vamos a crear dos carpetas. Una llamada upload para la carga de archivos en el servidor y otra llamada download para la descarga; cada una con sus respectivos permisos. En la carpeta upload se permite la escritura de archivos pero no en la carpeta download.

4. Se utilizará como usuario anónimo (anonymous) al usuario ftp (creado por defecto con la instalación del servicio) con su carpeta home por defecto (/home/ftp). Además establecemos una clave al usuario ftp.

   passwd ftp
   Enter new UNIX password: ftp
   Retype new UNIX password: ftp
   mkdir -p /home/ftp/upload
   mkdir -p /home/ftp/download

5. Cambiamos ahora los permisos y propietario sobre las carpetas creadas:

   chown ftp /home/ftp/download
   chown ftp /home/ftp/upload
   chmod 755 -R /home/ftp/download
   chmod a+rw /home/ftp/upload

6. Nuestro archivo de configuración debería quedar así:

```
#
# /etc/proftpd/proftpd.conf —This is a basic ProFTPD
configuration file.
# To really apply changes reload proftpd after modifications.
#

# Includes DSO modules
Include /etc/proftpd/modules.conf


# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6 off
ServerName “Debian”
ServerType standalone
DeferWelcome off


MultilineRFC2228 on
DefaultServer on
ShowSymlinks on


TimeoutNoTransfer 600
TimeoutStalled 600
TimeoutIdle 1200


DisplayLogin welcome.msg
DisplayFirstChdir .message
ListOptions “–l”

DenyFilter .*/


# Port 21 is the standard FTP port.
Port 21


# In some cases you have to specify passive ports range to by-pass
# firewall limitations. Ephemeral ports can be used for that, but
# feel free to use a more narrow range.
# PassivePorts 49152 65534
# To prevent DoS attacks, set the maximum number of child processes
# to 30. If you need to allow more than 30 concurrent connections
# at once, simply increase this value. Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances 30
```

```
# Set the user and group that the server normally runs at.
User proftpd
Group nogroup


# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask 022 022
# Normally, we want files to be overwriteable.
AllowOverwrite on


# Uncomment this if you are using NIS or LDAP to retrieve passwords:
# PersistentPasswd off


# Be warned: use of this directive impacts CPU average load
#
# Uncomment this if you like to see progress and transfer rate with ftpwho
# in downloads. That is not needed for uploads rates.
# UseSendFile off


TransferLog /var/log/proftpd/xferlog
SystemLog /var/log/proftpd/proftpd.log

<IfModule mod_tls.c>
TLSEngine off
</IfModule>
<IfModule mod_quota.c>
QuotaEngine on
</IfModule>
<IfModule mod_ratio.c>
Ratios on
</IfModule>


# Delay engine reduces impact of the so-called Timing Attack described in
# http://security.lss.hr/index.php?page=details&ID=LSS-2004-10-02
# It is on by default.
<IfModule mod_delay.c>
DelayEngine on
</IfModule>

<IfModule mod_ctrls.c>
ControlsEngine on
ControlsMaxClients 2
```

```
ControlsLog /var/log/proftpd/controls.log
ControlsInterval 5
ControlsSocket /var/run/proftpd/proftpd.sock
</IfModule>

<IfModule mod_ctrls_admin.c>
AdminControlsEngine on
</IfModule>

# A basic anonymous configuration, no upload directories.

<Anonymous  ftp>
User ftp
Group ftp
# We want clients to be able to login with .ªnonymous.ªs well as "ftp"
UserAlias anonymous ftp
# Cosmetic changes, all files belongs to ftp user
DirFakeUser on ftp
DirFakeGroup on ftp

RequireValidShell off

# Limit the maximum number of anonymous logins
MaxClients 10

# We want 'welcome.msg' displayed at login, and '.message' displayed
# in each newly chdired directory.
DisplayLogin welcome.msg
DisplayFirstChdir .message

# Limit WRITE everywhere in the anonymous chroot
<Directory /home/ftp>
<Limit WRITE READ>
DenyAll
</Limit>
</Directory>
<Directory /home/ftp/upload>
Umask 744
Allowoverwrite off
<Limit READ>
DenyAll
</Limit>
<Limit WRITE CWD>
AllowAll
</Limit>
</Directory>

<Directory /home/ftp/download>
Umask 444
```

<Limit READ>
AllowAll
</Limit>
</Directory>

    #
Uncomment this if you're brave.
<Directory incoming>
Umask 022 is a good standard umask to prevent new files and dirs
(second parm) from being group and world writable.
Umask 022 022
<Limit READ WRITE>
DenyAll
</Limit>
<Limit STOR>
AllowAll
</Limit>
</Directory>
#
</Anonymous>

Ahora reiniciamos el servicio:

/etc/init.d/proftpd restart

Capítulo 9

Servicio Samba

Samba es un paquete que brinda a los usuarios Linux la posibilidades de interactuar con equipos Windows que estén coexistiendo en redes heterogéneas. Permitiéndonos:

1. Compartir impresoras, instaladas tanto en el servidor como en los clientes.
2. Compartir uno o más sistemas de archivos.
3. Samba permite compartir entre máquinas Windows y Linux recursos.

Enlace: http://www.linuxparatodos.net/

Veremos 3 escenarios:
- Compartiendo un recurso para un usuario en Windows:

1. Creamos la carpeta a compartir:

   mkdir -p /home/conf1

2. Creamos el usuario que será asociado con la carpeta:

   adduser conf1
   Enter new UNIX password: conf1
   Retype the new UNIX password: conf1

3. Con motivos de prueba estableceremos todos los permisos sobre la carpeta:

   chmod 777 /home/conf1

4. Cambiamos el propietario del recurso a conf1:

   chown conf1 /home/conf1

5. Agregamos el usuario a la base de datos de Samba:

   smbpasswd -a conf1
   New SMB password: conf1
   Retype SMB password: conf1

6. Abrimos el archivo de configuración y agregamos las siguientes líneas al final:

vim /etc/samba/smb.conf

[conf1]
comment = Config conf1
writable = yes
path = /home/conf1
public = yes
browseable= yes

7. Ahora en nuestro equipo con sistema operativo Windows XP, presionamos la tecla: Windows+R (Ejecutar) e intentamos conectarnos al recurso compartido:

\\ip.del.servidor

- Compartiendo un recurso para un grupo de usuarios, acceso desde Windows:

1. Creamos la carpeta a compartir:

mkdir -p /home/conf2

2. Creamos 2 usuarios que pertenecerán al grupo çonf2z configuramos como propietario de la carpeta /home/conf2.ªl grupo de usuarios:

addgroup conf2
adduser conf2a —ingroup conf2
Enter new UNIX password: conf2a
Retype the new UNIX password: conf2a
adduser conf2b —ingroup conf2
Enter new UNIX password: conf2b
Retype the new UNIX password: conf2b

3. Agregamos los usuarios a la base de datos de Samba:

smbpasswd -a conf2a
New SMB password: conf2a
Retype SMB password: conf2a
smbpasswd -a conf2b
New SMB password: conf2b
Retype SMB password: conf2b

4. Ahora establecemos como propietario de la carpeta al grupo çonf2":

chown -R root:conf2 /home/conf2

5. Con motivos de prueba estableceremos todos los permisos sobre la carpeta:

chmod 777 /home/conf2

6. Abrimos el archivo de configuración y agregamos las siguientes líneas al final:

vim /etc/samba/smb.conf

[conf2]
comment = Config conf2
path = /home/conf2
valid users = @conf2
writable = yes
browseable= yes

7. Ahora en nuestro equipo con sistema operativo Windows XP, presionamos la tecla: Windows+R (Ejecutar) e intentamos conectarnos al recurso compartido:

\\ip.del.servidor

- Accediendo a un recurso compartido desde un cliente Linux:

1. Para acceder a un servidor SAMBA desde un cliente Linux, necesitamos tener instalado el paquete: samba-client.
2. Primero determinamos los recursos compartidos por el servidor:

smbclient -L //IP.del.servidor -U Usuario
Password: Clave.de.usuario

3. Una vez determinado el recurso a ser accedido (por ejemplo: files), ejecutamos el siguiente comando:

smbclient //IP.del.servidor/files -U Usuario
Password: Clave.de.usuario

4. Una vez ejecutado el comando anterior nos aparecerá un prompt como el siguiente: smb: \>. Para realizar operaciones sobre los archivos debemos ejecutar los mismos comandos que para el cliente FTP:

   –help [comando] : Muestra los comandos a ejecutar o la utilización de un comando si se especifica.

   –ls dir: lista los ficheros del directorio actual.

   –get fichero.remoto fichero.local : Transfiere un fichero desde el servidor al cliente guardándolo opcionalmente con el nombre especificado en el segundo argumento.

   –mget patrón : Transfiere desde el servidor al cliente todos ficheros que satisfagan el patrón especificado.

   –put fichero.local fichero.remoto : Transfiere un fichero desde el cliente al servidor guardándolo opcionalmente con el nombre especificado en el segundo argumento.

   –mput patrón : transfiere desde el cliente al servidor todos los ficheros que satisfagan el patrón especificado.

–recurse : Activa y desactiva la transferencia recursiva de directorios para los comandos mget y mput. También determina que la salida de los comandos ls y dir sea recursiva o no.

–prompt : Activa y desactiva el modo interactivo al hacer las transferencias múltiples con mget y mput.

–rm, rd y rmdir : Permiten borrar ficheros y directorios en el servidor.

–exit y quit : Cierran la conexión con el servidor.

Enlace: http://www.ispcmw.rimed.cu/sitios/digbiblio/cont/EI/SO_Linux/Avanzado-html/node116.html

Capítulo 10

Servicio NFS

NFS proviene de las siglas Network File System (Sistema de Archivos en Red) que es un sistema de archivos distribuido para un entorno de área local (LAN), permitiendo a diversas máquinas acceder a un recurso como si se tratase de uno local.
Podemos utilizar NFS para los siguientes casos por ejemplo:

1. Si contamos con varias máquinas de trabajo y todas ellas conectadas en red; podemos contar en cada una de ellas con el mismo software y configuración exportando desde un servidor los directorios /usr y /etc.
2. Si contamos con equipos clientes en la red con espacio en disco duro reducido y ellos necesitan ejecutar aplicaciones de gran tamaño, permitiéndonos a nosotros compartir dichas aplicaciones en la red y ejecutarlas en los equipos clientes como si fueran locales.

Ahora vamos a proceder con la configuración de NFS:

1. Para el servidor necesitamos tener instalados los siguientes paquetes: nfs-kernel-server nfs-common portmap.
2. Para nuestro cliente necesitamos los siguientes paquetes: nfs-common portmap.
3. En el servidor creamos el recurso a ser exportado:

   mkdir -p /home/export

4. Ahora cambiaremos de usuario a "nobodyz de grupo a "nogroup.ªl directorio /home/export, para el acceso de todos los equipos que deseen hacerlo (personalmente no recomiendo cambiar de propietario a "nobody", debido a que vamos a leer y **escribir** sobre /home/export.)
5. Editamos ahora:

   vim /etc/exports
   /home/export IP.del.equipo.cliente:Máscara.de.subred (rw)

6. Ahora indicamos al sistema que releea el fichero y ejecute los cambios:

   exportfs –ra

7. En el cliente creamos el punto de montaje para los directorios NFS:

   mkdir -p /mnt/nfs

8. Ahora ejecutamos el siguiente comando como root:

   mount IP.del.servidor:Directorio.compartido Punto.de.montaje

9. Pongamos como ejemplo: IP del servidor: 192.168.50.34, directorio NFS: /home/export, IP del equipo cliente: 192.168.50.35, punto de montaje: /mnt/nfs:

   mount 192.168.50.34:/home/export /mnt/nfs

10. Podemos ver en el cliente el directorio NFS montado con el comando:

    df -h

11. Si deseamos que el recurso NFS sea montado a iniciar el equipo, debemos modificar el archivo /etc/fstab y agregamos la siguiente línea:

    vim /etc/fstab
    192.168.50.34:/home/export /mnt/nfs nfs rw 0 0

Capítulo 11

Servicio Webmin

Webmin es una herramienta web que facilita la administración de un servidor con sistema operativo UNIX o Linux.

1. Primero instalamos las dependencias del paquete Webmin:

   apt-get install libnet-ssleay-perl libauthen-pam-perl libio-pty-perl libmd5-perl openssl

2. Descargamos el paquete Webmin:

   wget http://ufpr.dl.sourceforge.net/sourceforge/webadmin/webmin_1.460_all.deb

3. Procedemos ahora a instalar el paquete descargado (como root):

   dpkg -i webmin_1.460_all.deb

4. Finalmente accederemos a la interfaz de administración del servidor por la siguiente URL:

   https://IP.del.servidor:10000/

Capítulo 12

VMware Server 2

VMware Server 2 es un producto que nos permite la virtualización de equipos con sistemas operativos Microsoft Windows y Linux. Presenta ventajas tales como:

1. Acceso basado en web, el cual nos permite conectarnos desde cualquier parte simplemente contando con un navegador web.
2. Soporte mejorado de USB 2.0
3. El tamaño permitido de memoria RAM para las máquinas virtuales ha aumentado de 3.6 GB a 8 GB.
4. La consola remota de VMware nos permite la interacción con el virtualizado desde cualquier lugar con la simple instalación de un plugin en nuestro navegador web.

Procedamos ahora a la instalación de VMware Server 2 en nuestro equipo servidor:

1. En el Capítulo 1 se mencionó sobre la generación de una cuenta de usuario en la página de VMware para descarga del paquete de instalación y la generación de la serie de instalación para el producto.
2. Vamos a considerar la ruta: /home/vm como el lugar donde almacenamos el paquete .tar.gz de VMware Server 2.
3. Ahora nos dirigimos a dicha ruta:

   cd /home/vm

4. Descomprimimos e ingresmaos a la nueva ruta creada:

   tar xvfz VMware-server-*.tar.gz
   cd vmware-server-distrib

5. Ejecutamos:

   ./vmware-install.pl

6. Respondemos a las preguntas que se nos presenten, introducimos la serie en la instalación y nos pedirá el usuario asociado para la administración de las máquinas virtuales, para el cual podemos colocar al usuario: root, o crear uno para dicha labor:

adduser vmware

7. Para ingresar al servidor debemos colocar la siguiente dirección en nuestro navegador web:

https://IP.del.servidor:8333/ui/#

Capítulo 13

Clonezilla: clonando sistemas operativos a través de la red

Nota:
Instalado y configurado sobre Debian 4 Etch.

1. Debemos contar como mínimo con 2 interfaces de red; eth0 (acceso a internet) y eth1 (red local) previamente configurados.
2. Agregamos las llaves a nuestro apt-key como root: wget -q http://drbl.sourceforge.net/GPG-KEY-DRBL -O- |apt-key add -
3. Descargamos la llave desde el servidor: gpg —keyserver subkeys.pgp.net —recv-key D7E8DF3A, entonces ejecutar: gpg -a —export D7E8DF3A |apt-key add -
4. Agregamos a la lista de repositorios lo siguiente:

   deb http://ftp.us.debian.org/debian/ etch main
   deb http://drbl.sourceforge.net/drbl-core drbl stable

5. Ahora ejecutamos:

   apt-get update

   Para actualizar la lista de paquetes de nuestro repositorio.
6. Procedemos a instalar drbl:

   apt-get install drbl

7. Ahora procedemos a ejecutar el script de DRBL, al que tendremos que responder algunas preguntas sobre la configuración:

   /opt/drbl/sbin/drblsrv -i

8. Ahora ejecutamos y respondemos a los pasos de configuración:

   /opt/drbl/sbin/drblpush -i

9. Para la configuración final del servidor:

/opt/drbl/sbin/dcs

10. Si deseamos desinstalar DRBL y sus dependencias:

/opt/drbl/sbin/drblsrv -u

Apéndice A

Descargar las imágenes ISO de la distribución y grabarlas en medios ópticos (CD/DVD) a través de línea de comandos

Si hemos realizado la instalación de nuestro sistema operativo a través de una imagen NET-INST y necesitamos paquetes adicionales para su instalación, o deseamos instalar una gran variedad de equipos descargando los paquetes correspondientes a los múltiples programas que utilicen los usuarios y no contamos con el ancho de banda adecuado para dicha tarea, deberiamos contar con la primera imagen de DVD. Ya que dicha imagen contiene todos los archivos necesarios para la instalación de un sistema estándar. Y si deseamos crear un repositorio local necesitaremos todas las imágenes DVD.

1. Necesitamos tener instalado cdrecord, y una contar con una grabadora de CD/DVD en nuestro equipo.
2. Instalamos cdrecord (herramienta para la grabación de discos de datos o de audio):

   apt-get install cdrecord

3. Procedemos a la descarga de los archivos ISO usando el comando wget:

   wget http://ruta.completa/imagen.iso

4. Una vez descargada la imagen ISO, la grabamos en el medio óptico (CD/DVD), vamos a considerar la ruta donde se almacenó la imagen al directorio /isos:

   cdrecord -v /isos/imagen.iso

5. Si estamos descargando la imagen ISO de un DVD; dicho proceso tardará una buena cantidad de horas (dependiendo de nuestra conexión a Internet) y tendríamos que estar pendientes de la descarga de dicha imagen para proceder a su quemado. Para librarnos de ese proceso automatizaremos dichas tareas haciendo uso de &&, que nos permitirá la ejecución de los dos comandos (uno después del otros):

wget http://ruta.completa/imagen.iso && cdrecord -v /isos/imagen.iso

6. Es obvio que deberemos dejar el CD/DVD introducido en nuestra grabadora de discos. Una vez terminada la tarea extraemos el disco.

Nota:

El comando **-eject**, permite expulsar el CD/DVD una vez grabado pero no es soportado por todos los dispositivos.

Referencia: http://www.forat.info

Apéndice B

Comando: alias

Nos permite agregar un **alias** a los comandos que usamos más a menudo abreviando su escritura. Veamos:

1. Tenemos por ejemplo el siguiente comando: ls –la, que nos permite listar archivos y directorios incluyendo los ocultos de una manera no abreviada (muestra permisos, grupo, propietario, tamaño, etc).
2. Ahora usemos un alias para dicho comando:

   alias la='ls –la'

3. A partir de ahora el comando la realizará el trabajo de ls –la, siendo ahora más abreviado y reduciendonos los tiempos de escritura en el teclado.
4. Para el curso podriamos crear los siguientes alias que nos ayudarán en el desarrollo del curso:

   alias resq='/etc/init.d/squid restart'
   alias resa='/etc/init.d/samba restart'
   alias redh='/etc/init.d/dhcp3-server restart'
   alias clone='/opt/drbl/sbin/dcs'
   alias int='vim /etc/network/interfaces'

5.

Apéndice C

Listado de distribuciones y LiveCD

Un Live CD o Live DVD, más genéricamente Live Distro, (traducido en ocasiones como CD vivo o CD autónomo), es un sistema operativo (normalmente acompañado de un conjunto de aplicaciones) almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de ficheros. Algunos Live CD incluyen una herramienta que permite instalarlos en el disco duro. Otra característica es que por lo general no se efectúan cambios en la computadora utilizada, aunque algunos pueden almacenar preferencias si así se desea.

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

Características de las distribuciones GNU/Linux Live CD

Son distribuciones fáciles de encontrar, ya que algunas revistas informáticas se deciden por este tipo de distribuciones para llegar al usuario de Windows. No hay instalación, por lo que no hay que tocar el disco duro, ni seguir procedimientos complicados. Además, los datos, particiones o sistemas operativos del disco duro no se pierden. Aun así algunas poseen un instalador para poder ser instaladas, pudiendo conocer el rendimiento real de la distro, pues la velocidad de transferencia de las unidades lectoras (CD/DVD) es muy inferior a la de los discos duros.

Suelen tener un reconocimiento de hardware avanzado, fruto también de las últimas versiones del kernel que suelen poseer. En definitiva, las distribuciones Live CD intentan hacer llegar Linux a los usuarios de otros sistemas operativos.

Enlace: http://es.wikipedia.org/wiki/CD_autónomo

.

.

.

.

.

.

.

.

Apéndice D

Configurar Servidor NAT con iptables

1. Instalamos iptables (Netfilter):

   apt-get install iptables

2. Activamos el bit de forward: Permite que transfieran paquetes de un interfaz de red hacia otro, permitiendo que nuestro equipo se comporte como un dispositivo de NAT

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

   Si queremos que esto sea permanente debemos retirar el comentario de:

   vim /etc/sysctl.conf
   net.ipv4.conf.default.forwarding=1

3. Limpiamos todas las reglas:

   iptables -t nat -F
   iptables -F

4. Habilitamos el NAT (suponiendo que el interfaz que tiene salida a Internet es eth0):

   iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

Apéndice E

Instalación de Openbox: Escritorio rápido y ligero

Lo primero que debemos de hacer después de haber instalado el sistema base es hacer una actualización de todos los paquetes instalados hasta el momento con un simple:

 # aptitude update

Con esto ponemos al día nuestro el listado de paquetes.
Bueno una vez realizado esto debemos instalar el servidor de las X, poniendo lo siguiente:

 # aptitude install x-window-system-core

Display Manager:
Mientras el aptitude hace su trabajo debemos tomar una decision, la cual es con que Display Manager voy a usar este es cada vez que prendamos nuestra computadora nos pregunte en forma gráfica el login y el password asi que voy a poner los 3 más usados:

Xdm: el más pequeño y trabaja muy bien, altamente configurable.

gdm: fácilmente configurable, ademas contiene muchas más funciones extra de xdm.

kdm: el más grande y pesado, para los que le gusta KDE.

Asi que puedes escoger cualquiera, los 3 funciona en cualquier entorno de escritorio que elijas. Pero si te gusta gnome elige gdm, o si te gusta KDE elige kdm, o sino puedes elegir xdm si no tienes preferencia.
asi que tipeamos lo siguiente escogiendo el login manager a usar:

 # aptitude install display_manager

Openbox Openbox es otro windows Manager para las X, en sus inicios estaba basado en blackbox, pero a partir de la version 3.0 fue reescrito totalmente, está diseñado para ser rápido y consumir una mínima cantidad de recursos, para instalrlo debemos poner:

 # aptitude install openbox obconf

Enlace: http://www.esdebian.org

Si deseamos que no cargue por defecto el entorno gráfico en nuestro sistema, debemos de documentar una línea en el archivo: default-display-mananger (en el ejemplo tenemos instalado gdm)

vim /etc/X11/default-display-manager
#/usr/bin/gdm

Y cuando necesitemos cargar el escritorio de nuestro sistema ejecutamos:

startx

Apéndice F

Actualizar de Debian 4.0 Etch a Debian 5.0 Lenny

El proyecto Debian ha anunciado la publicación oficial de la versión 5.0 de Debian GNU/Linux, nombre en clave "Lenny"(14 de febrero del 2009), tras 22 meses de desarrollo constante.
Debian GNU/Linux es un sistema operativo libre que soporta un total de doce arquitecturas de procesador e incluye los entornos de escritorio KDE, GNOME, Xfce y LXDE.

Esta versión incluye una gran cantidad de paquetes de programas actualizados como: el entorno de escritorio K Desktop Environment 3.5.10 (KDE), una versión actualizada del entorno de escritorio GNOME 2.22.2, el entorno de escritorio Xfce 4.4.2, LXDE 0.3.2.1, el escritorio GNUstep 7.3, X.Org 7.3, OpenOffice.org 2.4.1, GIMP 2.4.7, Iceweasel 3.0.6 (una versión de Mozilla Firefox que no utiliza la marca registrada), Icedove 2.0.0.19 (una versión de Mozilla Thunderbird que no utiliza la marca registrada), PostgreSQL 8.3.6, MySQL 5.0.51a, la colección de compiladores del GNU (GCC) 4.3.2, el núcleo de Linux versión 2.6.26, Apache 2.2.9, Samba 3.2.5, Python 2.5.2 y 2.4.6, Perl 5.10.0, PHP 5.2.6, Asterisk 1.4.21.2, Emacs 22, Inkscape 0.46, Nagios 3.06, Xen Hypervisor 3.2.1 (con soporte tanto para dom0 como para domU), OpenJDK 6b11 y más de otros 23.000 paquetes de programas listos para usarse (contruídos a partir de 12.000 paquetes fuente).

Precisamente con la integración de X.Org 7.3 el servidor X se configura de forma automática con la mayor parte de hardware existente. La introducción de nuevos paquetes permiten dar soporte completo al sistema de ficheros NTFS, así como utilizar la mayor parte de las teclas multimedia sin configuración adicional. Se dispone de soporte para el formato de archivos Flash® de Adobe® a través de los complementos swfdec o Gnash. Se han introducido una serie de mejoras generales para ordenadores portátiles, como es el soporte integrado del escalado de frecuencia de la CPU. Se han añadido distintos juegos entre ellos rompecabezas y juegos de acción en primera persona. Un cambio notable es la introducción de goplay, un navegador gráfico de juegos que incluye filtros, capacidad de búsqueda, descripciones e instantáneas de los juegos en Debian.
La disponibilidad de OpenJDK, el compilador Java de GNU, el intérprete de bytecodes Java de GNU, Classpath, y otras versiones libre de la tecnología Java de Sun, en Debian GNU/Linux 5.0 hace posible la distribución de las aplicaciones basadas en Java dentro del

repositorio principal ("main") de Debian.

Puedes instalar Debian GNU/Linux utilizando distintos mecanismos de instalación, como DVDs, CDs, memorias USB y diskettes y hasta discos Blu-ray, e incluso directamente desde la red. El entorno de escritorio predeterminado es el de GNOME, y se encuentra en el primer CD. Se pueden instalar otros entornos de escritorio, como KDE, Xfce y LXDE, utilizando las dos nuevas imágenes de CD alternativas. De nuevo se encuentran disponible CDs y DVDs multi-arquitectura para Debian GNU/Linux 5.0, que permiten la instalación de varias arquitecturas desde un solo disco.

Se puede actualizar desde la versión anterior automáticamente.

Enlace: http://www.ubuntips.com.ar

Bueno ahora toca a nosotros actualizar nuestro sistema Debian Etch 4 a la versión estable actual (Lenny), para lo cual realizaremos los siguientes pasos:

1. Actualizar las fuentes de los paquetes sustituyendo ."Etch"por "Lenny", ingresamos a nuestro archivo de configuración de repositorios y hacemos los siguientes cambios:

   vim /etc/apt/sources.list

   Antes:

   deb http://security.debian.org/ etch/updates main contrib
   deb-src http://security.debian.org/ etch/updates main contrib
   deb ftp://ftp.debian.org/debian/ stable main contrib non-free

   Después:

   deb http://security.debian.org/ lenny/updates main contrib
   deb-src http://security.debian.org/ lenny/updates main contrib
   deb ftp://ftp.debian.org/debian/ stable main contrib non-free

2. Realizar una copia del software instalado (recomendado):

   dpkg –get-selections ≥ /respaldo/softwareinstalado.log

3. Restauración de lista de software:

   dpkg –set-selections < /respaldo/softwareinstalado.log

4. Ahora renovamos la lista de paquetes e instalamos la actualización:

   aptitude update
   aptitude install apt dpkg aptitude
   aptitude full-upgrade

Verificamos la versión actual

cat /etc/debian_version

Obtendremos: 5.0.

Bibliografía

[1] Curso Preparatorio Parte I y II LPI 101/102 - LOGIC Linux - LOGIC Linux

[2] Administración de Sistemas Linux - Tom Adelstein, Bill Lubanovic - O'Reilly

[3] LINUX SERVER, Los Mejores Trucos - Bill von Hagen, Brian K. Jones - O'Reilly

[4] La Biblia de Linux - Hector Facundo Arena - USERS

[5] Curso de Administración de Servidores Linux - Universidad Mayor Facultad de Ingeniería

[6] Linux Máxima Seguridad - Anónimo - Prentice Hall

[7] SUSE Linux 9.2 Manual de Administración - Novell - Novell

[8] Debian GNU/Linux Bible - Steve Hunger - Hungry Minds

[9] Squid: The Definitive Guide - Duane Wessels - O'Reilly