Implementación De Servidores Con GNU/Linux

Edición Mayo 2008

Joel Barrios Dueñas

A mi difunto padre, a quien debo reconocer jamás supe comprender y a quien jamás le dí la oportunidad de entenderme.

A mi madre, quien siempre tuvo una increíble paciencia con mi desorden.

A Blanca, Ana Elena, Gabriela M. (q.e.p.d.), Alejandra, Anahí, Gabriela C., Nely, Julieta, Nancy y Rebeca, las personas que de alguna forma y en algún momento han tenido significado en mi vida y fueron fuente de inspiración durante diversas etapas de mi existencia.

Blanca, gracias a ti inicié mi gusto por escribir. Te agradezco el haberme permitido escribirte todas esas cosas hace tantos años. Siempre tendrás un lugar muy especial en mi corazón y mis pensamientos.

Ai

Conformación.

Me encuentro de regreso en mis raíces,
reviso mis trabajos pasados,
entre risas y otros cursis versos
(sueños entonces de adolescente),
desde existenciales a lo absurdo,
ligerezas tan sentimentales
construyendo un carácter (mi mundo).

Acerca de Joel Barrios Dueñas.

Hay poco que decir respecto a mi. Solía ser médico veterinario zootecnista, dedicado principalmente la atención médica de pequeñas especies y otras mascotas (perros, gatos peces y tortugas) y a la venta de alimentos y accesorios para mascotas. Trabajo activamente con computadoras personales desde 1990, con las cuales siempre he tenido gran facilidad. Mi primera computadora, fue una Apple IIe que me prestó un amigo, y que eventualmente me vendió. Curiosamente, salvo por una clase que tomé en tercero de secundaria, durante la cual nos impartieron una introducción a la programación en BASIC y el uso general de computadoras Comodore 16, jamás he tomado un curso o capacitación relacionada con la informática o computación. Siempre he sido auto-didáctica.

Utilizo GNU/Linux desde Febrero de 1998, y desde Junio de 1999 como única plataforma en mi trabajo diario. Creo que es más que evidente que equivoque de carrera.

Gran parte de las razones de mi incursión en el mundo de la informática fueron verdaderamente incidentales. En 1997, nunca hubiera imaginado que me estaría ganado al vida en un ámbito completamente distinto al que me dedicaba durante ese tiempo. Yo ya tenía un consultorio y negocio pequeño de distribución de alimentos para mascotas, los cuales me aseguraban un ingreso regular. Lamentablemente las condiciones del mercado durante el siguiente año repercutieron de forma importante en mis ingresos, y fue entonces que empecé a buscar alternativas. Durante 1999 me estuve dedicando a la venta de equipo de computo y algo de diseño de sitios de red. Fueron algunos meses durante los cuales pude sobrevivir gracias a mis ahorros y a la suerte de contar un con talento poco común con las computadoras.

A mediados de 1999, mientras visitaba a un buen amigo mío, tuve un encuentro amistoso de unos 10 minutos con quien fue, en algún momento, la persona más importante que ha habido en mi vida, Blanca. Yo subía por un elevador, divagando en mis pensamientos con sutilezas y otros menesteres relacionados con mi profesión de veterinario. Salí del ascensor y me dirigí hacia la puerta de mi amigo. Me detuve unos instantes antes de pulsar el botón del timbre. Había una extraña sensación que circundaba mi mente, como un aroma familiar que no era posible recordar. Mi amigo tenía una reunión con varias personas, algunas de las cuales yo conocía desde hacía algunos años pero que por diversas circunstancias no frecuentaba, así que supuse que era solo la sensación de volver a ver a personas después de mucho tiempo. Toque el timbre y nos instantes después mi amigo abrió la puerta. Le saludé con un apretón de manos y tras saludarle de la acostumbrada forma cortes, quedé mudo al ver que la chica de la que me había enamorado durante mis de años de preparatoria, estaba presente. Frente a mi, sonriendo y mirándome. Habían pasado varios años desde la última vez que nos habíamos visto. Conversamos un poco mientras ella cargaba al perro de mi amigo, a cual me disponía a aplicar una vacuna. Fue difícil dejar de mirarle y lo fue también el gusto de volver a verle de nuevo. Me despedí, pues tenía otro compromiso, pero en mi mente quedó un sentimiento de alegría de ver que aquella persona que había tenido un gran impacto en mi vida, estaba bien, muy hermosa y, en apariencia, feliz.

Fue ese breve encuentro el que me inspiró algunos meses después a crear algo que me proporcionara los medios para lograr hacer algo importante en vida. Fue ese deseo de ser alguien y tener algo que ofrecer si algún día, y si las circunstancias lo permitían, buscar una segunda oportunidad con la persona de la que me había enamorado muchos años atrás y que de alguna forma jamás olvidé. Fue así que tras pasar muchas semanas planeando y tratando de dar forma a las ideas, el proyecto Linux Para Todos nació un 27 de agosto de 1999. Surgió como un sueño, se materializó, se desarrollo y creció más allá de lo que hubiera imaginado. Es irónico que años después, mi relativamente breve reencuentro con Blanca coincidiera con el fin del ciclo de Linux Para Todos, aunque también coincide con el inicio de otros proyectos y una nueva etapa con **Alcance Libre**.

Esta obra, que ahora comparto con los lectores, constituye la culminación del trabajo de más de 7 años de investigación y experiencias. Mucho del material que le compone fue escrito durante

diferentes etapas de mi ciclo con Linux Para Todos. El fin de dicho ciclo me da la oportunidad de explorar otras áreas de la informática desde un diferente enfoque, mismo que se verá reflejado en el material actualizado que compone esta obra. Nunca me ha interesado ser famoso o un millonario. Tengo una percepción distinta acerca de trascender más allá de los recuerdos familiares y trascender en la historia. Tal vez algún día, tal vez cien años después de haya muerto, se que de alguna forma mi legado en la historia será a través de todo lo que escribí y las cosas que pensaba y aquellas en las que creía.

Currículo.

Datos personales

- Nombre: Joel Barrios Dueñas.
- Año y lugar de nacimiento: 1970, México, Distrito Federal.
- Sexo: masculino.
- Estado civil: Unión Libre.

Escolaridad

- Secundaria: Colegio México (Acoxpa). 1982-1985
- Preparatoria: Instituto Centro Unión. 1985-1988
- Facultad de Medicina Veterinaria y Zootecnia, U.N.A.M. 1989-1993

Empleos en los que me he desempeñado.

- 1993-1999
    - Mi propia sub-distribuidora de alimentos y accesorios para mascotas. Dirección general.
    - Visitador Médico y asesor en informática. Distribuidora de Alimentos para Pequeñas Especies (Dialpe). Junio 1997 - Noviembre 1997.
    - Consultor externo de Dialpe 1998 – 1999.
- 1999 a 2006:
    - Fui el creador, director y administrador www.linuxparatodos.net.
    - Asesoría y consultoría en GNU/Linux.
    - Capacitación en GNU/Linux.
- 2002 - 2003:
    - Director Operativo Grupo MPR S.A. de C.V. (Actualmente Buytek Network Solutions)
- 2002 a 2006:
    - Director del proyecto LPT Desktop.
- 2004 a 2006:
    - Director Operativo de la unidad Linux de Factor Evolución S.A. de C.V.
- 2007 a la fecha:
        - Director de proyecto AL Desktop.
        - Fundador y director de proyecto de AlcanceLibre.org
        - Director General Alcance Empresarial, S.A. De C.V.

Capacidades

- Inglés 97.5%
- Ensamble, configuración y mantenimiento de computadoras personales.
- Programación HTML 4.0
- Programación CSS 1.0

- Instalación, configuración y administración de Linux y servicios que trabajan sobre éste (Samba, Apache, Sendmail, MailScanner, ClamAV, OpenLDAP, NFS, OpenSSH, VSFTPD, Shorewall, SNMP, MRTG, Squid)

Índice de contenido

1.¿Que es GNU/Linux?....29
1.1.Requerimientos del sistema....30

2.Estándar de Jerarquía de Sistema de Ficheros....31
2.1.Introducción....31
2.2.Estructura de directorios....31
2.3.Particiones recomendadas para instalar GNU/Linux....33

3.Instalación en modo texto de CentOS 4....34
3.1.Procedimientos....34

4.Instalación en modo gráfico de CentOS 4....53
4.1.Procedimientos....53

5.Instalación en modo texto de CentOS 5....72
5.1.Procedimientos....72

6.Instalación en modo gráfico de CentOS 5....90
6.1.Procedimientos....90

7.Cómo iniciar el modo de rescate en CentOS 4....109
7.1.Procedimientos....109

8.Iniciando el sistema en nivel de corrida 1 (nivel mono-usuario)....114
8.1.Introducción....114
8.2.Procedimientos....114

9.Procedimientos de emergencia....118
9.1.Introducción....118
9.2.Disco de rescate....118
9.3.Verificación de la integridad del disco....119
9.4.Asignación de formato de las particiones....119

10.Cómo configurar y utilizar Sudo....120
10.1.Introducción....120
10.1.1.Historia....120
10.2.Fichero /etc/sudoers....120
10.2.1.Cmnd_Alias....121
10.2.2.User_Alias....121
10.2.3.Host_Alias....121
10.2.4.Runas_Alias....122
10.3.Candados de seguridad....122
10.4.Lo que no se recomienda....123
10.5.Facilitando la vida a través de ~/.bash_profile....123

11.Cómo crear cuentas de usuario....125
11.1.Introducción....125
11.2.Procedimientos....125
11.2.1.Creando una cuenta en el modo de texto: useradd y passwd....125

11.2.1.1.Lo primero: el mandato useradd....125
11.2.1.2.Lo segundo: el mandato passwd....126
11.2.1.3.Opciones avanzadas....126
11.2.2.Eliminar una cuenta de usuario....127
11.3.Manejo de grupos....128
11.3.1.Alta de grupos....128
11.3.2.Alta de grupos de sistema....128
11.3.3.Baja de grupos....128
11.3.4.Asignación de usuarios existentes a grupos existentes....128
11.4.Comentarios finales acerca de la seguridad....128
11.5.Apéndice: Configurando valores predefinidos para el alta de cuentas de usuario....130
11.5.1.Fichero /etc/default/useradd para definir variables utilizadas por el mandato useradd....130
11.5.1.1.Variable HOME....130
11.5.1.2.Variable SHELL....130
11.5.2.Directorio /etc/skel como molde para crear los directorios de inicio de los usuarios....131
11.6.Apéndice: Ejercicio: Creando cuentas de usuario....132
11.6.1.Introducción....132
11.6.2.Procedimientos....132

12.Breve lección de mandatos básicos....134
12.1.Introducción....134
12.2.Procedimientos....134
12.2.1.Visualizando contenido de ficheros....137
12.2.2.Generación de texto por bucles....139
12.2.3.Bucles....140
12.2.4.Aliases....140
12.2.5.Apagado y reinicio de sistema....141
12.3.Resumen de mandatos básicos....142

13.Cómo utilizar lsof....143
13.1.Introducción....143
13.1.1.Acerca de lsof....143
13.2.Procedimientos....143

14.Funciones básicas de vi....146
14.1.Introducción....146
14.2.Procedimientos....146
14.2.1.Instalación y paquetes adicionales....146
14.3.Conociendo vi....146
14.4.Otras combinaciones de teclas....159
14.5.Más allá de las funciones básicas....160

15.Introducción a sed....161
15.1.Introducción....161
15.1.1.Acerca de sed....161
15.2.Procedimientos....161
15.3.Bibliografía....166

16.Introducción a AWK....167
16.1.Introducción....167
16.1.1.Acerca de AWK....167
16.1.2.Estructura de los programas escritos en AWK....167
16.2.Procedimientos....168

17.Permisos del Sistema de Ficheros....173
17.1.Introducción....173
17.2.Notación simbólica....173
17.3.Notación octal....174

17.3.1.Permisos adicionales....174
17.4.Ejemplos....175
17.4.1.Ejemplos de permisos regulares....175
17.4.2.Ejemplos de permisos especiales....176
17.5.Uso de chmod....176
17.5.1.Opciones de chmod....177
17.5.2.El mandato chmod y los enlaces simbólicos....177

18.Cómo utilizar el mandato chattr....178
18.1.Introducción....178
18.1.1.Acerca del mandato chattr....178
18.2.Opciones....178
18.3.Operadores....179
18.4.Atributos....179
18.5.Utilización....180
18.5.1.Ejemplos....180

19.Creando depósitos yum....181
19.1.Introducción....181
19.2.Procedimientos....181

20.Uso de yum para instalar y desinstalar paquetería y actualizar sistema....183
20.1.Introducción....183
20.2.Procedimientos....183
20.2.1.Actualizar sistema....183
20.2.2.Búsquedas....183
20.2.3.Consulta de información....183
20.2.4.Instalación de paquetes....184
20.2.5.Desinstalación de paquetes....184
20.2.5.1.Algunos paquetes que se pueden desinstalar del sistema....184
20.2.6.Listado de paquetes....184
20.2.7.Limpieza del sistema....185

21.Cómo utilizar RPM....186
21.1.Introducción....186
21.1.1.Acerca de RPM....186
21.2.Procedimientos....186
21.2.1.Reconstrucción de la base de datos de RPM....186
21.2.2.Consulta de paquetería instalada en el sistema....187
21.2.3.Instalación de paquetes....189
21.2.3.1.Recuperación de permisos originales a partir de rpm....194
21.2.4.Desinstalación de paquetes....195

22.Cómo crear paquetería con rpmbuild....197
22.1.Introducción....197
22.2.Instalación del sustento lógico necesario....197
22.3.Procedimientos....198
22.3.1.Creación de la clave GnuPG....198
22.3.2.Configuración y creación de una jaula para rpmbuild....198
22.3.2.1.Componentes del fichero ~/.rpmmacros....199
22.3.2.2.Creación de la estructura de la jaula para rpmbuild....199
22.3.3.Creación de los ficheros*.spec....200
22.3.3.1.Ejemplo de fichero *.spec....202
22.3.4.Uso del mandato rpmbuild....203
22.3.4.1.Ejemplos de uso del mandato rpmbuild....204
22.4.Ejercicios....205
22.4.1.Paquete RPM binario y el paquete *.src.rpm correspondiente creando el fichero *.spec necesario....205
22.4.2.Paquete RPM binario y el paquete *.src.rpm correspondiente realizando limpieza de directorio, firma

digital....206

23.Cómo asignar cuotas de disco....207
23.1.Introducción....207
23.2.Procedimientos....207
23.2.1.Edquota....208
23.2.1.1.Cuota absoluta....209
23.2.1.2.Cuota de gracia....209
23.2.1.3.Aplicando cuotas masivamente....209
23.3.Comprobaciones....209

24.Introducción a TCP/IP....211
24.1.Introducción....211
24.2.Niveles de pila....211
24.2.1.Modelo TCP/IP....212
24.2.1.1.Nivel de aplicación....214
24.2.1.2.Nivel de Transporte....214
24.2.1.3.Nivel de Red....216
24.2.1.4.Nivel de Enlace....217
24.2.1.5.Nivel Físico....217
24.2.2.Modelo OSI....217

25.Introducción a IP versión 4....219
25.1.Introducción....219
25.2.Direcciones....219
25.2.1.Representación de las direcciones....219
25.3.Asignación....220
25.3.1.Bloques reservados....220
25.3.1.1.Redes privadas....221
25.3.1.2.Anfitrión local (Localhost)....221
25.4.Referencia de sub-redes de IP versión 4....222
25.5.Referencias....223

26.Cómo configurar correctamente los parámetros de red....224
26.1.Introducción....224
26.2.Procedimientos....224
26.2.1.Detección y configuración del sustento físico (hardware)....224
26.2.2.Asignación de parámetros de red....225
26.2.2.1.Nombre del anfitrión (HOSTNAME)....225
26.2.2.2.Dirección IP, máscara de subred y puerta de enlace....225
26.2.2.3.Servidores de nombres....225
26.2.3.Agregar encaminamientos (rutas) adicionales....226
26.2.4.Función de reenvío de paquetes para IP versión 4....226
26.2.5.Comprobaciones....226
26.2.6.Alta de direcciones IP virtuales....227
26.2.7.La función Zeroconf....227
26.2.8.Deshabilitar IPv6....229
26.3.Ejercicios....229
26.3.1.Encaminamientos estáticos....229
26.3.2.Direcciones IP virtuales....232

27.Cómo utilizar Netcat (nc)....237
27.1.Introducción....237
27.1.1.Acerca de Netcat....237
27.2.Procedimientos....237
27.2.1.Conexiones simples....237
27.2.2.Revisión de puertos....237
27.2.3.Creando un modelo cliente servidor....238
27.2.4.Transferencia de datos....239

28.Como utilizar Netstat....240
28.1.Introducción....240
28.1.1.Acerca de Netstat....240
28.2.Procedimientos....240

29.Cómo utilizar ARP....245
29.1.Introducción....245
29.1.1.Acerca de ARP....245
29.2.Procedimientos....245

30.Introducción a IPTABLES....248
30.1.Introducción....248
30.1.1.Acerca de Iptables y Netfilter....248
30.2.Equipamiento lógico necesario....248
30.2.1.Instalación a través de yum....248
30.2.2.Instalación a través de up2date....248
30.3.Procedimientos....249
30.3.1.Cadenas....249
30.3.2.Reglas de destino....249
30.3.3.Políticas por defecto....249
30.3.4.Limpieza de reglas específicas....249
30.3.5.Reglas específicas....249
Ejemplos de reglas....250
30.3.5.1.Cerrar accesos....251
30.3.6.Eliminar reglas....251
30.3.7.Mostrar la lista de cadenas y reglas....251
30.3.8.Iniciar, detener y reiniciar el servicio iptables....253
30.3.9.Agregar el servicio iptables al arranque del sistema....253
30.4.Bibliografía....253

31.Cómo configurar un servidor DHCP en una LAN....254
31.1.Introducción....254
31.1.1.Acerca del protoclo DHCP....254
31.1.2.Acerca de dhcp por Internet Software Consortium, Inc....255
31.2.Equipamiento lógico necesario....255
31.2.1.Instalación a través de yum....255
31.2.2.Instalación a través de up2date....255
31.3.Procedimientos....255
31.3.1.Fichero de configuración /etc/dhcpd.conf....255
31.3.2.Fichero de configuración /etc/sysconfig/dhcpd....256
31.3.3.Iniciar, detener y reiniciar el servicio dhcpd....256
31.3.4.Agregar el servicio dhcpd al arranque del sistema....257
31.4.Comprobaciones desde cliente DHCP....257
31.5.Modificaciones necesarias en el muro cortafuegos....257

32.Cómo configurar vsftpd (Very Secure FTP Daemon)....259
32.1.Introducción....259
32.1.1.Acerca del protocolo FTP....259
32.1.2.Acerca de vsftpd....259
32.2.Equipamiento lógico necesario....259
32.2.1.Instalación a través de yum....259
32.2.2.Instalación a través de up2date....259
32.3.Ficheros de configuración....260
32.4.Procedimientos....260
32.4.1.Parámetro anonymous_enable....260
32.4.2.Parámetro local_enable....260
32.4.3.Parámetro write_enable....260
32.4.4.Parámetro anon_upload_enable....260
32.4.5.Parámetro anon_mkdir_write_enable....260

32.4.6.Parámetro ftpd_banner....261
32.4.7.Estableciendo jaulas para los usuarios: parámetros chroot_local_user y chroot_list_file....261
32.4.8.Control del ancho de banda....261
32.4.8.1.Parámetro anon_max_rate....261
32.4.8.2.Parámetro local_max_rate....261
32.4.8.3.Parámetro max_clients....261
32.4.8.4.Parámetro max_per_ip....262
32.4.9.Iniciar, detener y reiniciar el servicio vsftpd....262
32.4.10.Agregar el servicio al arranque del sistema....262
32.5.Modificaciones necesarias en el muro cortafuegos....262
32.6.Ejercicio VSFTPD....263

33.Cómo configurar pure-ftpd....265
33.1.Introducción....265
33.1.1.Acerca del protocolo FTP....265
33.1.2.Acerca de pure-ftpd....265
33.2.Equipamiento lógico necesario....265
33.2.1.Instalación a través de yum....265
33.3.Procedimientos....266
33.3.1.Fichero de configuración /etc/pure-ftpd/pure-ftpd.conf....266
33.3.1.1.Parámetro MaxClientsNumber....266
33.3.1.2.Parámetro MaxClientsPerIP....266
33.3.1.3.Parámetro DisplayDotFiles....266
33.3.1.4.Parámetro NoAnonymous....267
33.3.1.5.Parámetro AnonymousCanCreateDirs....267
33.3.1.6.Parámetro MaxLoad....267
33.3.1.7.Parámetro AntiWarez....267
33.3.1.8.Parámetro AnonymousBandwidth....267
33.3.1.9.Parámetro UserBandwidth....267
33.3.1.10.Parámetro umask....267
33.3.1.11.Parámetro ProhibitDotFilesWrite....268
33.3.1.12.Parámetro AnonymousCantUpload....268
33.3.1.13.Parámetro CreateHomeDir....268
33.3.1.14.Parámetro Quota....268
33.3.1.15.Parámetro MaxDiskUsage....268
33.3.1.16.Parámetro CustomerProof....268
33.3.2.Agregar el servicio al arranque del sistema....269
33.3.3.Iniciar, detener y reiniciar servicio....269
33.4.Modificaciones necesarias en el muro cortafuegos....269

34.Cómo configurar OpenSSH....270
34.1.Introducción....270
34.1.1.Acerca de SSH....270
34.1.2.Acerca de SFTP....270
34.1.3.Acerca de SCP....270
34.1.4.Acerca de OpenSSH....270
34.2.Equipamiento lógico necesario....271
34.3.Ficheros de configuración....271
34.4.Procedimientos....271
34.4.1.Parámetro Port....271
34.4.2.Parámetro ListenAddress....271
34.4.3.Parámetro PermitRootLogin....271
34.4.4.Parámetro X11Forwarding....272
34.4.5.Parámetro AllowUsers....272
34.5.Aplicando los cambios....272
34.6.Probando OpenSSH....273
34.6.1.Acceso a través de intérprete de mandatos....273
34.6.2.Transferencia de ficheros a través de SFTP....273
34.6.3.Transferencia de ficheros a través de SCP....274
34.7.Modificaciones necesarias en el muro cortafuegos....275

35.Cómo utilizar OpenSSH con autenticación a través de clave pública....276
35.1.Introducción....276

35.2.Procedimientos....276
35.2.1.Modificaciones en el Servidor....276
35.2.2.Modificaciones en el Cliente....276
35.2.2.1.Generar clave pública....276
35.2.3.Comprobaciones....277

36.Cómo configurar OpenSSH con Chroot....278
36.1.Introducción....278
36.2.Equipamiento lógico necesario....278
36.3.Procedimientos....280
36.3.1.Componentes mínimos para la jaula....280
36.3.2.Ficheros /etc/passwd y /etc/group....281
36.3.2.1.Ejemplo del contenido de /etc/passwd dentro de la jaula....281
36.3.2.2.Ejemplo del contenido de /etc/group dentro de la jaula....281
36.3.3.Dispositivos de bloque....281
36.4.Ejemplo práctico....281
36.4.1.Crear las cuentas de los usuarios....281
36.4.2.Ejemplo aplicado a sitio de red virtual con Apache....282
36.4.2.1.Comprobaciones del ejemplo....283

37.Cómo configurar NTP....284
37.1.Introducción....284
37.1.1.Acerca de NTP....284
37.1.1.1.Estratos....284
37.1.2.Acerca de UTC....285
37.2.Equipamiento lógico necesario....285
37.2.1.Instalación a través de yum....285
37.2.2.Instalación a través de up2date....285
37.3.Procedimientos....285
37.3.1.Herramienta ntpdate....285
37.3.2.Fichero de configuración /etc/ntp.conf....285
37.3.3.Iniciar, detener y reiniciar el servicio ntpd....286
37.3.4.Agregar el servicio ntpd al arranque del sistema....287
37.4.Modificaciones necesarias en el muro cortafuegos....287

38.Cómo configurar el sistema para sesiones gráficas remotas....288
38.1.Introducción....288
38.2.Sesión gráfica remota con GDM....288
38.2.1.Procedimiento....288

39.Cómo configurar un servidor NFS....291
39.1.Introducción....291
39.2.Procedimientos....291
39.2.1.Instalación del sustento lógico necesario....291
39.3.Configurando la seguridad....291
39.3.1.Compartir un volumen NFS....292
39.3.2.Configurando las máquinas clientes....293
39.4.Instalación de GNU/Linux a través de un servidor NFS....294

40.Cómo configurar SAMBA....296
40.1.Introducción....296
40.1.1.Acerca del protocolo SMB....296
40.1.2.Acerca de Samba....296
40.2.Equipamiento lógico necesario....296
40.3.Configuración básica de Samba....297
40.3.1.Alta de cuentas de usuario....297
40.3.2.El fichero lmhosts....297
40.3.3.Parámetros principales del fichero smb.conf....298
40.3.4.Parámetros útiles para la seguridad....298

40.3.5.Impresoras en Samba....299
40.3.6.Compartiendo directorios a través de Samba....300
40.4.Configuración avanzada de Samba....301
40.4.1.Reasignación de grupos de Windows en Samba....301
40.4.2.Alta de cuentas de usuario en Controlador Primario de Dominio....303
40.4.3.Parámetros de configuración avanzada en el fichero smb.conf....304
40.4.3.1.Anunciando el servidor Samba en los grupos de trabajo....304
40.4.3.2.Ocultando y denegando acceso a ficheros....304
40.4.3.3.Opciones para cliente o servidor Wins....305
40.4.3.4.Opciones específicas para Controlador Primario de Dominio (PDC)....305
Directorio para Netlogon y perfiles en Controlador Primario de Dominio (PDC)....306
40.5.Iniciar el servicio y añadirlo al arranque del sistema....307
40.6.Accediendo hacia Samba....307
40.6.1.Modo texto....307
40.6.1.1.Smbclient....307
40.6.1.2.Por montaje de unidades de red....308
40.6.2.Modo gráfico....310
40.6.2.1.Desde el entorno de GNOME....310
40.6.2.2.Desde Windows....310
40.7.Uniendo máquinas al dominio del Controlador Primario de Dominio....310
40.7.1.Creando manualmente cuentas de máquinas....311
40.7.2.Windows 95/98/ME y Windows XP Home....311
40.7.3.Windows NT....311
40.7.4.Windows 2000/2003 y Windows XP Profesional....311

41.La ingeniería social y los [incorrectos] hábitos del usuario....313
41.1.Recomendaciones para evitar ser víctimas de la ingeniería social a través del correo electrónico....314

42.Configuración básica de Sendmail....315
42.1.Introducción....315
42.1.1.Acerca de Sendmail....315
42.1.2.Acerca de Dovecot....315
42.1.3.Acerca de SASL y Cyrus SASL....315
42.1.4.Protocolos utilizados....316
42.1.4.1.SMTP (Simple Mail Transfer Protocol)....316
42.1.4.2.POP3 (Post Office Protocol, version 3)....316
42.1.4.3.IMAP (Internet Message Access Protocol)....317
42.2.Equipamiento lógico necesario....319
42.2.1.Instalación a través de yum....319
42.2.2.Instalación a través de Up2date....319
42.3.Procedimientos....320
42.3.1.Alta de cuentas de usuario y asignación de claves de acceso....320
42.3.2.Dominios a administrar....320
42.3.3.Control de acceso....321
42.3.4.Alias de la cuenta de root....322
42.3.5.Configuración de funciones de Sendmail....322
42.3.5.1.confSMTP_LOGIN_MSG....322
42.3.5.2.confAUTH_OPTIONS....323
42.3.5.3.TRUST_AUTH_MECH y confAUTH_MECHANISMS....323
42.3.5.4.DAEMON_OPTIONS....323
42.3.5.5.FEATURE(`accept_unresolvable_domains')....323
42.3.5.6.Enmascaramiento....324
42.3.5.7.Parámetro Cw....324
42.3.6.Usuarios Virtuales....324
42.3.7.Control del correo chatarra (Spam) a través de DNSBLs....325
42.3.8.Protocolos para acceder hacia el correo....326
42.3.9.Reiniciando servicio....326
42.4.Encaminamiento de dominios....326
42.4.1.Redundancia del servidor de correo....326
42.4.2.Servidor de correo intermediario....327
42.5.Verificando el servicio....328
42.6.Pruebas para el envío de correo....329

42.6.1.Utilizando telnet....329
42.6.2.Utilizando mutt....331
42.7.Referencias....332

43.Opciones avanzadas de seguridad para Sendmail....333
43.1.Introducción....333
43.2.Funciones....333
43.2.1.confMAX_RCPTS_PER_MESSAGE....333
43.2.2.confBAD_RCPT_THROTTLE....333
43.2.3.confPRIVACY_FLAGS....333
43.2.4.confMAX_HEADERS_LENGTH....334
43.2.5.confMAX_MESSAGE_SIZE....334
43.2.6.confMAX_DAEMON_CHILDREN....334
43.2.7.confCONNECTION_RATE_THROTTLE....334

44.Cómo configurar Sendmail y Dovecot con soporte SSL/TLS....335
44.1.Introducción....335
44.1.1.Acerca de DSA....335
44.1.2.Acerca de RSA....335
44.1.3.Acerca de X.509....335
44.1.4.Acerca de OpenSSL....336
44.2.Procedimientos....336
44.2.1.Sendmail. 336
44.2.1.1.Generando clave y certificado....336
44.2.1.2.Parámetros de /etc/mail/sendmail.mc....337
44.2.1.3.Comprobación....338
44.2.2.Dovecot. 338
44.2.2.1.Generando clave y certificado....338
44.2.2.2.Parámetros de /etc/dovecot.conf....339
44.2.2.3.Comprobación....340
44.2.3.Configuración de GNOME Evolution....340
44.2.3.1.Configuración GNOME Evolution....340
44.2.3.2.Configuración Mozilla Thunderbird....342
44.2.4.Modificaciones necesarias en el muro cortafuegos....343

45.Cómo configurar Cyrus IMAP....344
45.1.Introducción....344
45.2.Equipamiento lógico necesario....344
45.2.1.Instalación a través de yum....344
45.2.2.Instalación a través de up2date....344
45.3.Procedimientos....344
45.3.1.Alta de cuentas de usuario y asignación de claves de acceso....345
45.3.2.Iniciar, detener y reiniciar el servicio cyrus-imapd....346
45.3.3.Agregar el servicio cyrus-imapd al arranque del sistema....346
45.3.4.Integración con Sendmail....346
45.4.Comprobaciones....346

46.Instalación y configuración de SquirrelmMail (correo a través de interfaz HTTP)... 349
46.1.Introducción....349
46.2.Procedimientos....349
46.2.1.Instalación del sustento lógico necesario....349
46.2.2.Configuración de SquirrelMail....349
46.3.Finalizando configuración....352
46.4.Ajustes en php.ini para optimizar el uso de Squirrelmail....353

47.Apéndice: Enviar correo a todos los usuarios del sistema....355
47.1.Procedimientos....355
47.2.Acerca de la seguridad....355

48.Configuración de MailScanner y ClamAV con Sendmail....356
48.1.Introducción....356
48.1.1.Acerca de MailScanner....356
48.1.2.Acerca de ClamAV....357
48.1.3.Acerca de SpamAssassin....357
48.2.Procedimientos....357
48.2.1.Equipamiento lógico necesario....357
48.2.2.Configuración de MailScanner....358
48.2.2.1.Lenguaje de los mensajes de sistema....358
48.2.2.2.Identificación de la organización....358
48.2.2.3.Adjuntos en formato de texto enriquecido....359
48.2.2.4.Definir anti-virus a utilizar....359
48.2.2.5.¿Poner en cuarentena los mensajes infectados o no?....360
48.2.2.6.Permitir mensajes con etiqueta Iframe, Form y Script....360
48.2.3.Control de Spam....361
48.2.3.1.A través de DNSBL o listas negras....361
48.2.3.2.A través de SpamAssassin....361
48.2.3.3.Listas Blancas....363
48.2.4.Configuración de servicios....363
48.3.Comprobaciones....364
48.4.Modificaciones necesarias en el muro cortafuegos....365

49.Cómo configurar clamav-milter....366
49.1.Introducción....366
49.1.1.Acerca de clamav-milter....366
49.1.2.Acerca de ClamAV....366
49.2.Equipamiento lógico necesario....367
49.2.1.Instalación a través de yum....367
49.3.Procedimientos....367
49.3.1.Requisitos previos....367
49.3.2.Fichero /etc/mail/sendmail.mc....367
49.3.3.Configuración....368
49.3.4.Iniciar, detener y reiniciar el servicio clamav-milter....368

50.Cómo configurar spamass-milter....369
50.1.Introducción....369
50.1.1.Acerca de spamass-milter....369
50.1.2.Acerca de SpamAssassin....369
50.2.Equipamiento lógico necesario....369
50.2.1.Instalación a través de yum....369
50.3.Procedimientos....370
50.3.1.Requisitos previos....370
50.3.2.Fichero /etc/mail/sendmail.mc....370
50.3.3.Configuración....370
50.3.4.Fichero /etc/sysconfig/spamass-milter....371
50.3.5.Fichero /etc/sysconfig/spamassassin....372
50.3.6.Iniciar, detener y reiniciar el servicio spamass-milter....372

51.Cómo configurar un servidor NIS....374
51.1.Introducción....374
51.2.Procedimientos....374
Instalación del equipamiento lógico necesario en el servidor NIS....374
51.2.1.1.Instalación a través de yum....374
51.2.1.2.Instalación a través de up2date....375
51.2.2.Configuración del servidor NIS....375
51.2.2.1.Configuración del fichero /etc/yp.conf....375
51.2.2.2.Configuración del fichero /etc/ypserv.conf....375
51.2.2.3.Configuración del fichero /etc/sysconfig/network....375
51.2.2.4.Creación y contenido del fichero /var/yp/securenets....376
51.2.2.5.Inicio y reinicio de servicios portmap y ypserv....376
51.2.2.6.Creación de mapas NIS....376
51.2.2.7.Arranque de servicios ypbind, yppasswdd y ypxffrd....377

51.2.3.Instalación del equipamiento lógico necesario en el cliente NIS....377
51.2.3.1.Instalación a través de yum....377
51.2.3.2.Instalación a través de up2date....377
51.2.4.Configuración del cliente NIS....377
51.2.4.1.Configuración de ficheros /etc/sysconfig/network, /etc/yp.conf y /etc/hosts....377
51.2.4.2.Establecer el domino NIS....378
51.2.4.3.Ajustes en los ficheros /etc/nsswitch.conf, /etc/hosts.allow y /etc/hosts.deny....378
51.2.4.4.Iniciar servicio ypbind....379
51.2.4.5.Comprobaciones....379

52.Cómo configurar OpenLDAP como servidor de autenticación....380
52.1.Introducción....380
52.2.Equipamiento lógico requerido....380
52.2.1.Instalación a través de yum....380
52.2.2.Instalación a través de up2date....380
52.3.Procedimientos....380
52.4.Comprobaciones....382
52.5.Configuración de clientes....384
52.5.1.authconfig (modo texto)....384
52.5.2.authconfig-gtk (modo gráfico)....385
52.6.Administración....386
52.7.Respaldo de datos....387
52.8.Restauración de datos....387
52.9.Modificaciones necesarias en el muro cortafuegos....388

53.Cómo configurar OpenLDAP como libreta de direcciones....389
53.1.Introducción....389
53.2.Equipamiento lógico requerido....389
53.2.1.Instalación a través de yum....389
53.2.2.Instalación a través de up2date....389
53.3.Procedimientos....389
53.4.Configuración de clientes....392
53.4.1.Novell Evolution....392
53.4.2.Mozilla Thunderbird....394
53.4.3.Squirrelmail....395
53.5.Administración....395
53.6.Respaldo de datos....396
53.7.Restauración de datos....396
53.8.Modificaciones necesarias en el muro cortafuegos....397

54.Cómo configurar OpenLDAP con soporte SSL/TLS....398
54.1.Introducción....398
54.1.1.Acerca de LDAP en modo SSL/TLS....398
54.1.2.Acerca de RSA....398
54.1.3.Acerca de X.509....398
54.1.4.Acerca de OpenSSL....399
54.2.Procedimientos....399
54.2.1.Generando clave y certificado....399
54.2.2.Parámetros de /etc/openldap/slapd.conf....400
54.2.3.Comprobación....400
54.2.4.Configuración de GNOME Evolution....400
54.2.5.Configuración de Mozilla Thunderbird....401
54.2.6.Configuración LDAP Browser....402
54.2.7.Configuración LDAP Administration Tool....402
54.3.Modificaciones necesarias en el muro cortafuegos....403

55.Configuración básica de Freeradius con soporte de LDAP....404
55.1.Introducción....404
55.1.1.Acerca de RADIUS....404
55.1.2.Acerca de Freeradius....404

55.2.Equipamiento lógico necesario.....405
55.2.1.Instalación a través de yum.....405
55.2.2.Instalación a través de Up2date.....405
55.3.Procedimientos.....405
55.3.1.Agregar el servicio al arranque del sistema.....406
55.3.2.Iniciar, detener y reiniciar el servicio.....406
55.4.Modificaciones necesarias en el muro cortafuegos.....406
55.5.Comprobaciones.....406

56.Cómo instalar y configurar MySQL™.....408
56.1.Introducción.....408
56.1.1.Acerca de MySQL™.....408
56.2.Equipamiento lógico necesario.....408
56.2.1.Instalación a través de yum.....408
56.2.2.Instalación a través de up2date.....408
56.3.Procedimientos.....409
56.3.1.SELinux y el servicio mysqld.....409
56.3.2.Iniciar, detener y reiniciar el servicio mysqld.....409
56.3.3.Agregar el servicio mysqld al arranque del sistema.....410
56.3.4.Asignación de clave de acceso al usuario root.....410
56.3.4.1.Método corto.....410
56.3.4.2.Método largo.....410
56.4.Creando y destruyendo bases de datos.....412
56.5.Otorgando permisos a los usuarios.....412
56.6.Modificaciones necesarias en el muro cortafuegos.....413

57.Configuración básica de Apache.....414
57.1.Introducción.....414
57.1.1.Acerca del protocolo HTTP.....414
57.1.2.Acerca de Apache.....414
57.2.Equipamiento lógico necesario.....414
57.2.1.Instalación a través de yum.....414
57.2.2.Instalación a través de Up2date.....415
57.3.Iniciar servicio y añadir el servicio al arranque del sistema.....415
57.4.Procedimientos.....415
57.4.1.SELinux y Apache.....415
57.4.2.UTF-8 y codificación de documentos.....416
57.4.3.Ficheros de configuración.....417
57.4.4.Directorios virtuales.....417
57.4.5.Redirección de directorios.....418
57.4.6.Tipos de MIME.....418
57.4.7.Soporte para CGI con extensión *.cgi.....418
57.4.7.1.Probando la configuración.....418
57.4.7.2.Problemas posteriores.....419
57.4.7.3.Error más común número 1.....419
57.4.7.4.Error más común número 2.....419
57.4.8.Robo de imágenes.....419
57.5.Modificaciones necesarias en el muro cortafuegos.....420
57.6.Apéndice: Configuración de Sitios de Red virtuales en Apache.....421

58.Cómo habilitar los ficheros .htaccess y SSI)Server Side Includes) en Apache 2.x..423
58.1.Introducción.....423
58.2.Procedimientos.....423
58.2.1.Autenticación de directorios.....423
58.2.1.1.Ejemplo.....423
58.2.2.Asignación de directivas para PHP.....424
58.2.2.1.Ejemplo.....425

59.Cómo configurar Apache con soporte SSL/TLS. 427

59.1.Introducción..... .427
59.1.1.Acerca de HTTPS.....427
59.1.2.Acerca de RSA.....427
59.1.3.Acerca de Triple DES.....427
59.1.4.Acerca de X.509.....428
59.1.5.Acerca de OpenSSL.....428
59.1.6.Acerca de mod_ssl.....428
59.2.Requisitos..... 428
59.3.Equipamiento lógico necesario..... 428
59.3.1.Instalación a través de yum.....428
59.3.2.Instalación a través de Up2date.....428
59.4.Procedimientos..... 429
59.4.1.Generando clave y certificado.....429
59.4.2.Configuración de Apache.....431
59.4.3.Comprobación.....431
59.4.4.Modificaciones necesarias en el muro cortafuegos.....432

60.Cómo instalar y configurar Geeklog 1.4.x.....433
60.1.Introducción..... .433
60.1.1.Acerca de Geeklog.....433
60.1.2.¿Por qué Geeklog?.....433
60.2.Aspectos de seguridad a considerar..... ..433
60.2.1.Prefijo de las tablas de Geeklog.....434
60.2.2.Rutas de los directorios de Geeklog.....434
60.2.3.Desactivar el despliegue de errores de PHP.....434
60.3.Equipamiento lógico necesario..... 434
60.3.1.Instalación a través de yum.....434
60.3.2.Instalación a través de Up2date.....435
60.4.Procedimientos..... 435
Arranque de servicios.....435
60.4.1.Instalación de Geeklog.....436
60.5.Procedimientos..... 436
60.5.1.Respaldo de la base de datos existente.....436
60.5.2.Creación de la base de datos para Geeklog en MySQL.....436
60.5.3.Configuración de directorios para Geeklog.....437
60.5.4.Fichero lib-common.php.....438
60.5.5.Fichero config.php.....438
60.5.6.Instalador de Geeklog.....439
60.5.7.Procedimientos posteriores.....439
60.6.Problemas posteriores..... 439

61.Cómo configurar un servidor de nombres de dominio (DNS).....440
61.1.Introducción..... .440
61.1.1.Bind (Berkeley Internet Name Domain).....440
61.1.2.DNS (Domain Name System).....440
61.1.3.NIC (Network Information Center).....440
61.1.4.FQDN (Fully Qualified Domain Name).....441
61.1.5.Componentes de un DNS.....441
61.1.5.1.Clientes DNS.....441
61.1.5.2.Servidores DNS.....441
61.1.5.3.Zonas de Autoridad.....442
61.1.6.Herramientas de búsqueda y consulta.....444
61.1.6.1.Mandato host.....444
61.1.6.2.Mandato dig.....444
61.1.6.3.Mandato jwhois (whois).....445
61.2.Equipamiento lógico necesario..... 445
61.2.1.Instalación a través de yum.....445
61.2.2.Instalación a través de Up2date.....445
61.3.Procedimientos..... 446
61.3.1.Preparativos.....446
61.3.2.Creación de los ficheros de zona.....446
61.3.2.1.Zona de reenvío red local /var/named/chroot/var/named/red-local.zone.....446

61.3.2.2.Zona de resolución inversa red local /var/named/chroot/var/named/1.168.192.in-addr.arpa.zone....447
61.3.2.3.Zona de reenvío del dominio /var/named/chroot/var/named/dominio.com.zone....447
61.3.2.4.Zona de resolución inversa del dominio /var/named/chroot/var/named/1.243.148.in-addr.arpa.zone....448
61.3.2.5.Configuración de parámetros en el fichero /etc/named.conf....448
61.3.3.Seguridad adicional en DNS para uso público....449
61.3.3.1.Fichero /etc/named.conf....449
61.3.4.Seguridad adicional en DNS para uso exclusivo en red local....450
61.3.4.1.Fichero /etc/named.conf....450
61.3.5.Las zonas esclavas....451
61.3.5.1.Fichero /etc/named.conf Servidor DNS secundario....451
61.3.5.2.Fichero /etc/named.conf Servidor DNS primario....451
61.3.6.Reiniciar servicio y depuración de configuración....452

62.Cómo configurar Squid: Parámetros básicos para Servidor Intermediario (Proxy).. 454
62.1.Introducción.... 454
62.1.1.¿Qué es Servidor Intermediario (Proxy)?....454
62.1.2.Acerca de Squid....455
62.1.2.1.Algoritmos de caché utilizados por Squid....455
62.2.Equipamiento lógico necesario....456
62.2.1.Instalación a través de yum....456
62.2.2.Instalación a través de up2date....456
62.2.3.Otros componentes necesarios....456
62.3.Antes de continuar....457
62.4.Configuración básica....457
62.4.1.Parámetro http_port: ¿Qué puerto utilizar para Squid?....457
62.4.2.Parámetro cache_mem....458
62.4.3.Parámetro cache_dir: ¿Cuánto desea almacenar de Internet en el disco duro?....459
62.4.4.Parámetro ftp_user....459
62.4.5.Controles de acceso....459
62.4.5.1.Listas de control de acceso....460
62.4.5.2.Reglas de Control de Acceso....460
62.4.6.Aplicando Listas y Reglas de control de acceso....461
62.4.6.1.Caso 1....461
62.4.6.2.Caso 2....462
62.4.7.Parámetro chache_mgr....463
62.4.8.Parámetro cache_peer: caches padres y hermanos....463
62.5.Estableciendo el idioma de los mensajes mostrados por de Squid hacia el usuario....463
62.6.Iniciar, reiniciar y añadir el servicio al arranque del sistema....464
62.7.Depuración de errores....464
62.8.Ajustes para el muro corta-fuegos....465
62.8.1.Re-direccionamiento de peticiones a través de iptables y Firestarter....465
62.8.2.Re-direccionamiento de peticiones a través de la opción REDIRECT en Shorewall....465

63.Cómo configurar Squid: Acceso por autenticación....467
63.1.Introducción.... 467
63.2.Equipamiento lógico necesario....467
63.3.Eligiendo el módulo de autenticación....467
63.3.1.Autenticación a través del módulo LDAP....467
63.3.1.1.Parámetros en /etc/squid/squid.conf....468
63.3.2.Autenticación a través del módulo NCSA....468
63.3.2.1.Creación del fichero de claves de acceso....468
63.3.2.2.Parámetros en /etc/squid/squid.conf....468
63.4.Listas y reglas de control de acceso....469
63.4.1.Finalizando procedimiento....470

64.Cómo configurar Squid: Restricción de acceso a Sitios de Red....471
64.1.Introducción.... 471
64.2.Equipamiento lógico necesario....471
64.3.Definiendo patrones comunes....471
64.4.Parámetros en /etc/squid/squid.conf....472
64.4.1.Permitiendo acceso a sitios inocentes incidentalmente bloqueados....472

64.4.2.Finalizando procedimiento....473

65.Cómo configurar Squid: Restricción de acceso a contenido por extensión....474
65.1.Introducción.... 474
65.2.Equipamiento lógico necesario....474
65.3.Definiendo elementos de la Lista de Control de Acceso....474
65.4.Parámetros en /etc/squid/squid.conf....475
65.4.1.Finalizando procedimiento....476

66.Cómo configurar Squid: Restricción de acceso por horarios....477
66.1.Introducción.... 477
66.2.Equipamiento lógico necesario....477
66.3.Procedimientos....477
66.3.1.Más ejemplos....478
66.3.1.1.Restringiendo el tipo de contenido....478
66.3.1.2.Combinando reglas de tiempo y contenido....478
66.3.2.Finalizando procedimiento....479

67.Apéndice: Listas y reglas de control de acceso para Squid....480
67.0.1.Reglas aplicadas....480

68.Cómo configurar un muro cortafuegos con Shorewall y tres interfaces de red. 482
68.1.Introducción.... 482
68.1.1.Acerca de Shorewall....482
68.1.2.Acerca de Iptables y Netfilter....482
68.1.3.Acerca de Iproute....482
68.1.4.Requisitos....483
68.2.Conceptos requeridos....483
68.2.1.¿Qué es una zona desmilitarizada?....483
68.2.2.¿Que es una Red Privada?....483
68.2.3.¿Qué es un NAT?....484
68.2.4.¿Qué es un DNAT?....484
68.3.Procedimientos....484
68.3.1.Equipamiento lógico necesario....484
68.3.2.Fichero de configuración /etc/shorewall/shorewall.conf....484
68.3.3.Fichero de configuración /etc/shorewall/zones....485
68.3.4.Fichero de configuración /etc/shorewall/interfaces....485
68.3.5.Fichero de configuración /etc/shorewall/policy....486
68.3.6.Fichero de configuración /etc/shorewall/masq....487
68.3.7.Fichero de configuración /etc/shorewall/rules....487
68.3.7.1.ACCEPT....487
68.3.7.2.REDIRECT....488
68.3.7.3.DNAT....488
68.3.7.4.Ejemplos diversos de reglas....488
68.4.Iniciar el cortafuegos y añadirlo a los servicios de arranque del sistema....490

69.Cómo configurar SNMP....491
69.1.Introducción.... 491
69.1.1.Acerca de SNMP....491
69.1.2.Acerca de Net-SNMP....491
69.2.Equipamiento lógico necesario....491
69.2.1.Instalación a través de yum....491
69.2.2.Instalación a través de up2date....491
69.3.Procedimientos....492
Fichero de configuración /etc/snmp/snmpd.conf....492
69.3.1.1.Listas de control de acceso....492
69.3.1.2.Definición de grupos....492
69.3.1.3.Ramas permitidas....493
69.3.1.4.Asignación de permisos a los grupos....493
69.3.1.5.Parámetros de carácter informativo....493

69.3.2.Un ejemplo funcional de configuración....493
69.3.3.Iniciar, detener y reiniciar el servicio snmpd....494
69.3.4.Agregar el servicio snmpd al arranque del sistema....495
69.4.Comprobaciones....495
69.5.Modificaciones necesarias en el muro cortafuegos....495

70.Cómo configurar MRTG....496
70.1.Introducción....496
70.1.1.Acerca de MRTG....496
70.2.Equipamiento lógico necesario....496
70.2.1.Instalación a través de yum....496
70.2.2.Instalación a través de up2date....496
70.3.Procedimientos....496
70.4.Comprobaciones....497

71.Cómo configurar Asterisk 1.4 para utilizar Ekiga y Linphone como clientes SIP....499
71.1.Introducción....499
71.1.1.Acerca de Ekiga....499
71.1.2.Acerca de Asterisk....499
71.1.3.Acerca de Linphone....499
71.1.4.Acerca del protocolo SIP....500
71.2.Equipamiento lógico necesario....500
71.2.1.Instalación de servidor Asterisk....500
71.2.1.1.Instalación a través de yum....501
71.2.2.Instalación de cliente Ekiga....501
71.2.2.1.Instalación a través de yum....501
71.2.3.Instalación de clientes Linphone y Linphonec....501
71.2.3.1.Instalación a través de yum....501
71.3.Procedimientos....502
71.3.1.Configuración de servidor Asterisk....502
71.3.1.1.Fichero /etc/asterisk/manager.conf....502
71.3.1.2.Fichero /etc/asterisk/sip.conf....502
71.3.1.3.Fichero /etc/asterisk/voicemail.conf....503
71.3.1.4.Fichero /etc/asterisk/extensions.conf....504
71.3.2.Configuración de cliente Ekiga....505
71.3.3.Configuración de cliente Linphone y Linphonec....506
71.4.Comprobaciones....508
71.5.Modificaciones necesarias en el muro cortafuegos en el servidor Asterisk....508
71.6.Bibliografía....509

72.Cómo instalar correctamente Java™ a partir de paquete RPM....510
72.1.Procedimiento....510
72.2.Comprobaciones....511

73.Cómo instalar la extensión (plug-in) Flash para Mozilla....513
73.1.Introducción....513
73.2.Procedimientos....513
73.2.1.Instalación del sustento lógico necesario en CentOS, White Box y Red Hat™ Enterprise Linux 3...513
73.2.2.Instalación del sustento lógico necesario en CentOS, White Box y Red Hat™ Enterprise Linux 4...513
73.2.3.Comprobaciones....514

74.Cómo configurar escáner en red....515
74.1.Introducción....515
74.1.1.Acerca de SANE....515
74.1.2.Acerca de Xsane....515
74.2.Equipamiento lógico necesario....516
74.2.1.Instalación del servicio saned....516
74.2.1.1.Instalación a través de yum....516

74.2.1.2.Instalación a través de up2date....516
74.2.2.Instalación del cliente Xsane....516
74.2.2.1.Instalación a través de yum....516
74.2.2.2.Instalación a través de up2date....516
74.3.Procedimientos....516
74.3.1.Configuración del servicio saned....516
74.3.2.Configuración del cliente Xsane....518

75.Usando Smartd para anticipar los desastres de disco duro....519
75.1.Introducción....519
75.2.Procedimientos....519

76.Glosario de mandatos básicos....521
76.1.Mandatos generales....521
76.2.Tratamiento de archivos....522
76.3.Manejo de paquetería....522
76.4.Sistema....523

77.AL Desktop....525
77.1.¿Que es AL Desktop?....525
77.2.Sistemas operativos soportados por AL Desktop....525
77.3.¿Cómo puedo instalarlo?....525
77.3.1.AL Desktop 1.0....526
77.3.1.1.CentOS 4, Red Hat Enterprise Linux 4, Whitebox Enterprise Linux 4....526
77.3.1.2.CentOS 5, Red Hat Enterprise Linux 5, Whitebox Enterprise Linux 5....526
77.3.2.Procedimientos....526
77.3.2.1.AL Desktop 1.0....526
77.4.Errores conocidos....526
77.4.1.AL Desktop 1.0....526
77.5.¿Cómo puedo cooperar con el proyecto?....527
77.6.¿Más preguntas?....527

78.Ejercicios....528
78.1.Ejercicio NFS....528
78.1.1.Introducción....528
78.1.2.Procedimientos....528
78.1.2.1.Servidor....528
78.1.2.2.Cliente....528
78.2.Ejercicio SAMBA....530
78.2.1.Procedimientos....530
78.3.Ejercicio Apache® y VSFTPD....533
78.3.1.Procedimientos....533
78.3.2.Comprobaciones....534
78.4.Ejercicio: Cuotas de disco, Apache, VSFTPD y DNS....536
78.4.1.Procedimientos....536
78.4.2.Comprobaciones....540
78.5.Ejercicio: Servidor Intermediario (Proxy)....542
78.5.1.Introducción....542
Procedimientos....542
78.6.Ejercicio de configuración del sistema para Linux, Apache, PHP y MySQL....548
78.7.Configuración del sistema como estación de trabajo....551

Información de Derechos reservados de esta publicación.

Reconocimiento-NoComercial-CompartirIgual 2.1

Usted es libre de:

- copiar, distribuir y comunicar públicamente la obra
- hacer obras derivadas

Bajo las condiciones siguientes:

Reconocimiento. Debe reconocer y citar al autor original.

No comercial. No puede utilizar esta obra para fines comerciales.

Compartir bajo la misma licencia. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

- Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.
- Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior.

Reconocimiento-NoComercial-CompartirIgual 2.1

CREATIVE COMMONS CORPORATION NO ES UN DESPACHO DE ABOGADOS Y NO PROPORCIONA SERVICIOS JURÍDICOS. LA DISTRIBUCIÓN DE ESTA LICENCIA NO CREA UNA RELACIÓN ABOGADO-CLIENTE. CREATIVE COMMONS PROPORCIONA ESTA INFORMACIÓN TAL CUAL (ON AN "AS-IS" BASIS). CREATIVE COMMONS NO OFRECE GARANTÍA ALGUNA RESPECTO DE LA INFORMACIÓN PROPORCIONADA, NI ASUME RESPONSABILIDAD ALGUNA POR DAÑOS PRODUCIDOS A CONSECUENCIA DE SU USO.

Licencia

LA OBRA (SEGÚN SE DEFINE MÁS ADELANTE) SE PROPORCIONA BAJO TÉRMINOS DE ESTA LICENCIA PÚBLICA DE CREATIVE COMMONS ("CCPL" O "LICENCIA"). LA OBRA SE ENCUENTRA PROTEGIDA POR LA LEY ESPAÑOLA DE PROPIEDAD INTELECTUAL Y/O CUALESQUIERA OTRAS NORMAS RESULTEN DE APLICACIÓN. QUEDA PROHIBIDO CUALQUIER USO DE LA OBRA DIFERENTE A LO AUTORIZADO BAJO ESTA LICENCIA O LO DISPUESTO EN LAS LEYES DE PROPIEDAD INTELECTUAL.

MEDIANTE EL EJERCICIO DE CUALQUIER DERECHO SOBRE LA OBRA, USTED ACEPTA Y CONSIENTE LAS LIMITACIONES Y OBLIGACIONES DE ESTA LICENCIA. EL LICENCIADOR LE CEDE LOS DERECHOS CONTENIDOS EN ESTA LICENCIA, SIEMPRE QUE USTED ACEPTE LOS PRESENTES TÉRMINOS Y CONDICIONES.

1. Definiciones

a. La **"obra"** es la creación literaria, artística o científica ofrecida bajo los términos de esta licencia.

b. El **"autor"** es la persona o la entidad que creó la obra.

c. Se considerará **"obra conjunta"** aquella susceptible de ser incluida en alguna de las siguientes categorías:

   i. **"Obra en colaboración"**, entendiendo por tal aquella que sea resultado unitario de la colaboración de varios autores.

d. **"Obra colectiva"**, entendiendo por tal la creada por la iniciativa y bajo la coordinación de una persona natural o jurídica que la modifique y divulgue bajo su nombre y que esté constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en una creación única y autónoma, para la cual haya sido concebida sin que sea posible atribuir separadamente a cualquiera de ellos un derecho sobre el conjunto de la obra realizada.

e. **"Obra compuesta e independiente"**, entendiendo por tal la obra nueva que incorpore una obra preexistente sin la colaboración del autor de esta última.

f. Se considerarán **"obras derivadas"** aquellas que se encuentren basadas en una obra o en una obra y otras preexistentes, tales como: las traducciones y adaptaciones; las revisiones, actualizaciones y anotaciones; los compendios, resúmenes y extractos; los arreglos musicales y, en general, cualesquiera transformaciones de una obra literaria, artística o científica, salvo que la obra resultante tenga el carácter de obra conjunta en cuyo caso no será considerada como una obra derivada a los efectos de esta licencia. Para evitar la duda, si la obra consiste en una composición musical o grabación de sonidos, la sincronización temporal de la obra con una imagen en movimiento ("synching") será considerada como una obra derivada a los efectos de esta licencia.

g. Tendrán la consideración de **"obras audiovisuales"** las creaciones expresadas mediante una serie de imágenes asociadas, con o sin sonorización incorporada, así como las composiciones musicales, que estén destinadas esencialmente a ser mostradas a través de aparatos de proyección o por cualquier otro medio de comunicación pública de la imagen y del sonido, con independencia de la naturaleza de los soportes materiales de dichas obras.

h. El **"licenciador"** es la persona o la entidad que ofrece la obra bajo los términos de esta licencia y le cede los derechos de explotación de la misma conforme a lo dispuesto en ella.

i. **"Usted"** es la persona o la entidad que ejercita los derechos cedidos mediante esta licencia y que no ha violado previamente los términos de la misma con respecto a la obra, o que ha recibido el permiso expreso del licenciador de ejercitar los derechos cedidos mediante esta licencia a pesar de una violación anterior.

j. La **"transformación"** de una obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente. Cuando se trate de una base de datos según se define más adelante, se considerará también transformación la reordenación de la misma. La creación resultante de la transformación de una obra tendrá la consideración de obra derivada.

k. Se entiende por **"reproducción"** la fijación de la obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella.

l. Se entiende por **"distribución"** la puesta a disposición del público del original o copias de la obra mediante su venta, alquiler, préstamo o de cualquier otra forma.

m. Se entenderá por **"comunicación pública"** todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas. No se considerará pública la comunicación cuando se celebre dentro de un ámbito estrictamente doméstico que no esté integrado o conectado a una red de difusión de cualquier tipo. A efectos de esta licencia se considerará comunicación pública la puesta a disposición del público de la obra por procedimientos alámbricos o inalámbricos, incluida la puesta a disposición del público de la obra de tal forma que cualquier persona pueda acceder a ella desde el lugar y en el momento que elija.

n. La **"explotación"** de la obra comprende su reproducción, distribución, comunicación pública y transformación.

o. Tendrán la consideración de **"bases de datos"** las colecciones de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos propiamente dichas que por la selección o disposición de sus contenidos constituyan creaciones intelectuales, sin perjuicio, en su caso, de los derechos que pudieran subsistir sobre dichos contenidos.

p. Los **"elementos de la licencia"** son las características principales de la licencia según la selección efectuada por el licenciador e indicadas en el título de esta licencia: Reconocimiento de autoría (Reconocimiento), Sin uso comercial (NoComercial), Compartir de manera igual (CompartirIgual).

2. Límites y uso legítimo de los derechos. Nada en esta licencia pretende reducir o restringir cualesquiera límites legales de los derechos exclusivos del titular de los derechos de propiedad intelectual de acuerdo con la Ley de Propiedad Intelectual o cualesquiera otras leyes aplicables, ya sean derivados de usos legítimos, tales como el derecho de copia privada o el derecho a cita, u otras limitaciones como la derivada de la primera venta de ejemplares.

3. Concesión de licencia. Conforme a los términos y a las condiciones de esta licencia, el licenciador concede (durante toda la vigencia de los derechos de propiedad intelectual) una licencia de ámbito mundial, sin derecho de remuneración, no exclusiva e indefinida que incluye la cesión de los siguientes derechos:

a. Derecho de reproducción, distribución y comunicación pública sobre la obra;

b. Derecho a incorporarla en una o más obras conjuntas o bases de datos y para su reproducción en tanto que incorporada a dichas obras conjuntas o bases de datos;

c. Derecho para efectuar cualquier transformación sobre la obra y crear y reproducir obras derivadas;

d. Derecho de distribución y comunicación pública de copias o grabaciones de la obra, como incorporada a obras conjuntas o bases de datos;

e. Derecho de distribución y comunicación pública de copias o grabaciones de la obra, por medio de una obra derivada.

Los anteriores derechos se pueden ejercitar en todos los medios y formatos, tangibles o intangibles, conocidos o por conocer. Los derechos mencionados incluyen el derecho a efectuar las modificaciones que sean precisas técnicamente para el ejercicio de los derechos en otros medios y formatos. Todos los derechos no cedidos expresamente por el licenciador quedan reservados, incluyendo, a título enunciativo pero no limitativo, los establecidos en la sección 4(e).

4. Restricciones. La cesión de derechos que supone esta licencia se encuentra sujeta y limitada a las restricciones siguientes:

a. Usted puede reproducir, distribuir o comunicar públicamente la obra solamente bajo términos de esta licencia y debe incluir una copia de la misma, o su Identificador Uniforme de Recurso (URI), con cada copia o grabación de la obra que usted reproduzca, distribuya o comunique públicamente. Usted no puede ofrecer o imponer ningún término sobre la obra que altere o restrinja los términos de esta licencia o el ejercicio de sus derechos por parte de los cesionarios de la misma. Usted no puede sublicenciar la obra. Usted debe mantener intactos todos los avisos que se refieran a esta licencia y a la ausencia de garantías. Usted no puede reproducir, distribuir o comunicar públicamente la obra con medidas tecnológicas que controlen el acceso o uso de la obra de una manera contraria a los términos de esta licencia. Lo anterior se aplica a una obra en tanto que incorporada a una obra conjunta o base de datos, pero no implica que éstas, al margen de la obra objeto de esta licencia, tengan que estar sujetas a los términos de la misma. Si usted crea una obra conjunta o base de datos, previa comunicación del licenciador, usted deberá quitar de la obra conjunta o base de datos cualquier referencia a dicho licenciador o al autor original, según lo que se le requiera y en la medida de lo posible. Si usted crea una obra derivada, previa comunicación del licenciador, usted deberá quitar de la obra derivada cualquier referencia a dicho licenciador o al autor original, lo que se le requiera y en la medida de lo posible.

b. Usted puede reproducir, distribuir o comunicar públicamente una obra derivada solamente bajo los términos de esta licencia, o de una versión posterior de esta licencia con sus mismos elementos principales, o de una licencia iCommons de Creative Commons que contenga los mismos elementos principales que esta licencia (ejemplo: Reconocimiento-NoComercial-Compartir 2.0 Japón). Usted debe incluir una copia de la esta licencia o de la mencionada anteriormente, o bien su Identificador Uniforme de Recurso (URI), con cada copia o grabación de la obra que usted reproduzca, distribuya o comunique públicamente. Usted no puede ofrecer o imponer ningún término respecto de las obras derivadas o sus transformaciones que alteren o restrinjan los términos de esta licencia o el ejercicio de sus derechos por parte de los cesionarios de la misma, Usted debe mantener intactos todos los avisos que se refieran a esta licencia y a la ausencia de garantías. Usted no puede reproducir, distribuir o comunicar públicamente la obra derivada con medidas tecnológicas que controlen el acceso o uso de la obra de una manera contraria a los términos de esta licencia. Lo anterior se aplica a una obra derivada en tanto que incorporada a una obra conjunta o base de datos, pero no implica que éstas, al margen de la obra objeto de esta licencia, tengan que estar sujetas a los términos de esta licencia.

c. Usted no puede ejercitar ninguno de los derechos cedidos en la sección 3 anterior de manera que pretenda principalmente o se encuentre dirigida hacia la obtención de un beneficio mercantil o la remuneración monetaria privada. El intercambio de la obra por otras obras protegidas por la propiedad intelectual mediante sistemas de compartir archivos no se considerará como una manera que pretenda principalmente o se encuentre dirigida hacia la obtención de un beneficio mercantil o la remuneración monetaria privada, siempre que no haya ningún pago de cualquier remuneración monetaria en relación con el intercambio de las obras protegidas.

d. Si usted reproduce, distribuye o comunica públicamente la obra o cualquier obra derivada, conjunta o base datos que la incorpore, usted debe mantener intactos todos los avisos sobre la propiedad intelectual de la obra y reconocer al autor original, de manera razonable conforme al medio o a los medios que usted esté utilizando, indicando el nombre (o el seudónimo, en su caso) del autor original si es facilitado; el título de la obra si es facilitado; de manera razonable, el Identificador Uniforme de Recurso (URI), si existe, que el licenciador especifica para ser vinculado a la obra, a menos que tal URI no se refiera al aviso sobre propiedad intelectual o a la información sobre la licencia de la obra; y en el caso de una obra derivada, un aviso que identifique el uso de la obra en la obra derivada (e.g., "traducción francesa de la obra de Autor Original," o "guión basado en obra original de Autor Original"). Tal aviso se puede desarrollar de cualquier manera razonable; con tal de que, sin embargo, en el caso de una obra derivada, conjunta o base datos, aparezca como mínimo este aviso allá donde aparezcan los avisos correspondientes a otros autores y de forma comparable a los mismos.

e. Para evitar la duda, sin perjuicio de la preceptiva autorización del licenciador, y especialmente cuando la obra se trate de una obra audiovisual, el licenciador se reserva el derecho exclusivo a percibir, tanto individualmente como mediante una entidad de gestión de derechos, o varias, (por ejemplo: SGAE, Dama, VEGAP), los derechos de explotación de la obra, así como los derivados de obras derivadas, conjuntas o bases de datos, si dicha explotación pretende principalmente o se encuentra dirigida hacia la obtención de un beneficio mercantil o la remuneración monetaria privada.

f. En el caso de la inclusión de la obra en alguna base de datos o recopilación, el propietario o el gestor de la base de datos deberá renunciar a cualquier derecho relacionado con esta inclusión y concerniente a los usos de la obra una vez extraída de las bases de datos, ya sea de manera individual o conjuntamente con otros materiales.

5. Exoneración de responsabilidad

A MENOS QUE SE ACUERDE MUTUAMENTE ENTRE LAS PARTES, EL LICENCIADOR OFRECE LA OBRA TAL CUAL (ON AN "AS-IS" BASIS) Y NO CONFIERE NINGUNA GARANTÍA DE CUALQUIER TIPO RESPECTO DE LA OBRA O DE LA PRESENCIA O AUSENCIA DE ERRORES QUE PUEDAN O NO SER DESCUBIERTOS. ALGUNAS JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE TALES GARANTÍAS, POR LO QUE TAL EXCLUSIÓN PUEDE NO SER DE APLICACIÓN A USTED.

6. Limitación de responsabilidad.

SALVO QUE LO DISPONGA EXPRESA E IMPERATIVAMENTE LA LEY APLICABLE, EN NINGÚN CASO EL LICENCIADOR SERÁ RESPONSABLE ANTE USTED POR CUALQUIER TEORÍA LEGAL DE CUALESQUIERA DAÑOS RESULTANTES, GENERALES O ESPECIALES (INCLUIDO EL DAÑO EMERGENTE Y EL LUCRO CESANTE), FORTUITOS O CAUSALES, DIRECTOS O INDIRECTOS, PRODUCIDOS EN CONEXIÓN CON ESTA LICENCIA O EL USO DE LA OBRA, INCLUSO SI EL LICENCIADOR HUBIERA SIDO INFORMADO DE LA POSIBILIDAD DE TALES DAÑOS.

7. Finalización de la licencia

a. Esta licencia y la cesión de los derechos que contiene terminarán automáticamente en caso de cualquier incumplimiento de los términos de la misma. Las personas o entidades que hayan recibido obras derivadas, conjuntas o bases de datos de usted bajo esta licencia, sin embargo, no verán sus licencias finalizadas, siempre que tales personas o entidades se mantengan en el cumplimiento íntegro de esta licencia. Las secciones 1, 2, 5, 6, 7 y 8 permanecerán vigentes pese a cualquier finalización de esta licencia.

b. Conforme a las condiciones y términos anteriores, la cesión de derechos de esta licencia es perpetua (durante toda la vigencia de los derechos de propiedad intelectual aplicables a la obra). A pesar de lo anterior, el licenciador se reserva el derecho a divulgar o publicar la obra en condiciones distintas a las presentes, o de retirar la obra en cualquier momento. No obstante, ello no supondrá dar por concluida esta licencia (o cualquier otra licencia que haya sido concedida, o sea necesario ser concedida, bajo los términos de esta licencia), que continuará vigente y con efectos completos a no ser que haya finalizado conforme a lo establecido anteriormente.

8. Miscelánea

a. Cada vez que usted explote de alguna forma la obra, o una obra conjunta o una base datos que la incorpore, el licenciador original ofrece a los terceros y sucesivos licenciatarios la cesión de derechos sobre la obra en las mismas condiciones y términos que la licencia concedida a usted.

b. Cada vez que usted explote de alguna forma una obra derivada, el licenciador original ofrece a los terceros y sucesivos licenciatarios la cesión de derechos sobre la obra original en las mismas condiciones y términos que la licencia concedida a usted.

c. Si alguna disposición de esta licencia resulta inválida o inaplicable según la Ley vigente, ello no afectará la validez o aplicabilidad del resto de los términos de esta licencia y, sin ninguna acción adicional por cualquiera las partes de este acuerdo, tal disposición se entenderá reformada en lo estrictamente necesario para hacer que tal disposición sea válida y ejecutiva.

d. No se entenderá que existe renuncia respecto de algún término o disposición de esta licencia, ni que se consiente violación alguna de la misma, a menos que tal renuncia o consentimiento figure por escrito y lleve la firma de la parte que renuncie o consienta.

e. Esta licencia constituye el acuerdo pleno entre las partes con respecto a la obra objeto de la licencia. No caben interpretaciones, acuerdos o términos con respecto a la obra que no se encuentren expresamente especificados en la presente licencia. El licenciador no estará obligado por ninguna disposición complementaria que pueda aparecer en cualquier comunicación de usted. Esta licencia no se puede modificar sin el mutuo acuerdo por escrito entre el licenciador y usted.

Creative Commons no es parte de esta licencia, y no ofrece ninguna garantía en relación con la obra. Creative Commons no será responsable frente a usted o a cualquier parte, por cualquier teoría legal de cualesquiera daños resultantes, incluyendo, pero no limitado, daños generales o especiales (incluido el daño emergente y el lucro cesante), fortuitos o causales, en conexión con esta licencia. A pesar de las dos (2) oraciones anteriores, si Creative Commons se ha identificado expresamente como el licenciador, tendrá todos los derechos y obligaciones del licenciador.

Salvo para el propósito limitado de indicar al público que la obra está licenciada bajo la CCPL, ninguna parte utilizará la marca registrada "Creative Commons" o cualquier marca registrada o insignia relacionada con "Creative Commons" sin su consentimiento por escrito. Cualquier uso permitido se hará de conformidad con las pautas vigentes en cada momento sobre el uso de la marca registrada por "Creative Commons", en tanto que sean publicadas su página web (website) o sean proporcionadas a petición previa.

Puede contactar con Creative Commons en: http://creativecommons.org/.

Otras notas acerca de esta publicación.

1. ¿Que es GNU/Linux?

Joel Barrios Dueñas
darkshram@gmail.com
http://www.linuxparatodos.net/

GNU/Linux® es un poderoso y sumamente versátil sistema operativo con licencia libre y que implementa el estándar **POSIX** (acrónimo de **P**ortable **O**perating **S**ystem **I**nterface, que se traduce como Interfaz de Sistema Operativo Portable). Fue creado en 1991 por Linus Torvalds, siendo entonces un estudiante de la Universidad de Helsinski, Finlandia.

GNU/Linux es **Programática Libre**. Esto significa que el usuario es libre de redistribuir y modificar de acuerdo a necesidades específicas, siempre que se incluya el código fuente, como lo indica la Licencia Pública General GNU (acrónimo de **G**NU is **N**ot **U**nix), que es el modo que ha dispuesto la Free Software Foundation (Fundación de Programática Libre). Esto también incluye el derecho a poder instalar el núcleo de **GNU/Linux®** en cualquier número de ordenadores o equipos de cómputo que el usuario desee.

GNU/Linux® **no es un sustento lógico gratuito** (comúnmente denominada como Freeware); se trata de **Programática Libre**. Cuando nos referirnos a **Programática Libre**, lo hacemos en relación a la libertad y no al precio. La **GPL** (acrónimo de **G**eneral **P**ublic **L**icence, que se traduce como Licencia Pública General), a la cual Linus Torvalds incorporó a Linux, está diseñada para asegurar que el usuario tenga siempre la libertad de distribuir copias del sustento lógico libre (y cobrar por el servicio si así lo desea). La **GPL** tiene como objetivo garantizar al usuario la libertad de compartir y cambiar **Programática Libre**; es decir, asegurarse de que el sustento lógico siempre permanezca siendo libre para todos los usuarios. La **GPL** es aplicable a la mayoría del sustento lógico de la Free Software Foundation así como a cualquier otro programa cuyos autores se comprometan a usarlo.

GNU/Linux® es también la mejor alternativa de siglo XXI para los usuarios que no solo desean libertad, sino que también requieren un sistema operativo estable, robusto y confiable. Es un sistema operativo idóneo para utilizar en Redes, como es el caso de servidores, estaciones de trabajo y **también** para computadoras personales.

Las características de GNU/Linux® le permiten desempeñar múltiples tareas en forma simultánea de forma segura y confiable. Los distintos servicios se pueden detener, iniciar o reiniciar independientemente sin afectar al resto del sistema, permitiendo operar las 24 horas del día los 365 días del año.

Tal ha sido el impacto alcanzado por GNU/Linux® en los últimos años, que muchas de las empresas de Software más importantes del mundo, entre las cuales están IBM, Oracle y Sun Microsystems, han encontrado en GNU/Linux una plataforma con un muy amplio mercado, y se han volcado al desarrollo de versiones para Linux de sus más importantes aplicaciones. Grandes corporaciones, como Compaq, Dell, Hewlett Packard, IBM y muchos más, llevan varios años distribuyendo equipos con GNU/Linux® como sistema operativo.

Gracias a sus características, la constante evolución de los ambientes gráficos para X Window®, que cada vez son de más fácil uso, como es el caso de GNOME y KDE, al trabajo de cientos de programadores y usuarios fieles alrededor del mundo, Linux ha dejado de ser un sistema operativo

poco atractivo y complicado de utilizar, para convertirse en una alternativa real para quienes buscan un sistema operativo confiable y poderoso; ya sea para una servidor, estación de trabajo o la computadora personal de un usuario intrépido.

1.1. Requerimientos del sistema

Se debe contar con la suficiente cantidad de memoria y un microprocesador en buen estado. Con casi cualquier distribución comercial de Linux, el ambiente gráfico necesitará al menos 192 MB RAM, y 650-800 MB de espacio en disco duro para la instalación mínima. Para contar con la menor cantidad de aplicaciones prácticas, se requieren al menos 800 MB adicionales de espacio en disco duro, repartido en al menos 2 particiones. Se recomienda un microprocesador 80586 (pentium o equivalente) a 200 MHz. Sin ambiente gráfico, como es el caso de un servidor, o bien solamente aplicaciones para modo de texto, 64MB RAM y un microprocesador 80586 a 100 MHz serán suficientes.

El servidor de vídeo puede funcionar con sólo 64 MB RAM; pero su desempeño será **mucho muy lento**. Algunas aplicaciones para modo gráfico pueden necesitar escalar 64 MB, 128 MB o 256 MB de RAM adicional. El mínimo recomendado para utilizar GNOME 2.x es de 192 MB RAM; se recomiendan 256 MB. El óptimo es de 512 MB RAM.

Si desea instalar Linux en una computadora personal con las suficientes aplicaciones para ser totalmente funcional y productivo y contar con el espacio necesario para instalar herramientas de oficina (OpenOffice.org), se **recomienda** contar con al menos 2 GB de espacio, al menos 256 MB RAM y un microprocesador AMD K6, K6-II, K6-III, Athlon, Duron, Pentium, Pentium MMX, Pentium II, Pentium III, Pentium 4, o Cyrix MII a cuando menos 300 Mhz o más.

2. Estándar de Jerarquía de Sistema de Ficheros

Joel Barrios Dueñas
darkshram@gmail.com
http://www.linuxparatodos.net/

Artículo basado sobre el publicado en inglés por Wikipedia, Enciclopedia Libre, en http://en.wikipedia.org/wiki/FHS.

2.1. Introducción

El estándar de jerarquía de ficheros (FSH o **F**ilesystem **H**ierarchy **S**tandard) define los principales directorios y sus contenidos en GNU/Linux y otros sistemas operativos similares a Unix.

El proceso de desarrollar un estándar de sistema de ficheros jerárquico inició en agosto de 1993, como un esfuerzo para reformar las estructuras de ficheros y directorios de GNU/Linux. El 14 de febrero de 1994 se publicó el FSSTND (**F**ile**s**ystem **St**a**nd**ard); un estándar de jerarquía de ficheros específico para GNU/Linux. Revisiones de éste se publicaron el 9 de octubre de 1994 y el 28 de marzo de 1995.

A principios de 1996, con la ayuda de miembros de la comunidad de desarrolladores de BSD, se fijó como objetivo desarrollar una versión de **FSSTND** más detallada, dirigida no sólo hacia Linux sino también hacia otros sistemas operativos similares a Unix. Como uno de los resultados, el estándar cambió de nombre a FSH o Filesystem Hierarchy Standard.

El FSH es mantenido por Free Standards Group; organización sin fines de lucro constituida por compañías que manufacturan sustento físico (Hardware) y sustento físico (Software) como Hewlett Packard, Dell, IBM y Red Hat. La mayoría de las distribuciones de Linux, inclusive las que forman parte de Free Software Standards, no aplican de forma estricta el estándar. La versión actual del FSH es la 2.3, anunciada en 29 de enero de 2004.

2.2. Estructura de directorios

Todos los ficheros y directorios aparecen debajo del directorio raíz «/», aún si están almacenados en dispositivos físicamente diferentes.

Directorio	Descripción
`/bin/`	Mandatos binarios esenciales (cp, mv, ls, rm, etc.).
`/boot/`	Ficheros utilizados durante el arranque del sistema (núcleo y discos RAM).
`/dev/`	Dispositivos esenciales.
`/etc/`	Ficheros de configuración utilizados en todo el sistema y que son específicos del anfitrión.
`/etc/opt/`	Ficheros de configuración utilizados por programas alojados dentro de /opt/

Directorio	Descripción
/etc/X11/ (opcional)	Ficheros de configuración para el sistema X Window.
/etc/sgml/ (opcional)	Ficheros de configuración para SGML.
/etc/xml/ (opcional)	Ficheros de configuración para XML.
/home/ (opcional)	Directorios de inicio de los usuarios.
/lib/	Bibliotecas compartidas esenciales para los binarios de /bin/, /sbin/ y el núcleo del sistema.
/mnt/	Sistemas de ficheros montados temporalmente.
/media/	Puntos de montaje para dispositivos de medios como unidades lectoras de discos compactos.
/opt/	Paquetes de aplicaciones estáticas.
/proc/	Sistema de ficheros virtual que documenta sucesos y estados del núcleo. Contiene principalmente ficheros de texto.
/root/ (opcional)	Directorio de inicio del usuario root (súper-usuario).
/sbin/	Binarios de administración de sistema.
/tmp/	Ficheros temporales
/srv/	Datos específicos de sitio servidos por el sistema.
/usr/	Jerarquía secundaria para datos compartidos de sólo lectura (**U**nix **s**ystem **r**esources). Este directorio debe poder ser compartido para múltiples anfitriones y no debe contener datos específicos del anfitrión que los comparte.
/usr/bin/	Mandatos binarios.
/usr/include/	Ficheros de inclusión estándar (cabeceras de cabecera utilizados para desarrollo).
/usr/lib/	Bibliotecas compartidas.
/usr/share/	Datos compartidos independientes de la arquitectura del sistema. Imágenes, ficheros de texto, etc.
/usr/src/ (opcional)	Códigos fuente.
/usr/X11R6/ (opcional)	Sistema X Window, versión 11, lanzamiento 6.
/usr/local/	Jerarquía terciaria para datos compartidos de sólo lectura específicos del anfitrión.
/var/	Ficheros variables como son: bitácoras, bases de datos, directorio raíz de servidores HTTP y FTP, colas de correo, ficheros temporales, etc.
/var/account/ (opcional)	Procesa bitácoras de cuentas de usuarios.
/var/cache/	Cache da datos de aplicaciones.
/var/crash/ (opcional)	Depósito de información referente a estrellamientos del sistema.
/var/games/ (opional)	Datos variables de aplicaciones para juegos.
/var/lib/	Información de estado variable. Algunos servidores como MySQL y PostgreSQL almacenan sus bases de datos en directorios

Directorio	Descripción
	subordinados de éste.
/var/lock/	Ficheros de bloqueo.
/var/log/	Ficheros y directorios de bitácoras.
/var/mail/ (opcional)	Buzones de correo de usuarios.
/var/opt/	Datos variables de /opt/.
/var/spool/	Colas y carretes de datos de aplicaciones.
/var/tmp/	Ficheros temporales preservados entre reinicios.

Más detalles acerca del FSH en http://www.pathname.com/fhs/.

2.3. Particiones recomendadas para instalar GNU/Linux

Como mínimo se requieren tres particiones:

/boot	Por lo menos 75 MB. Asignar más espacio puede considerarse desperdicio.
/	350 a 512 MB.
Swap	Debe asignarse el **doble del tamaño del RAM físico**; esta será siempre la última partición del disco duro y no se le asigna punto de montaje.

Otras particiones que se recomienda asignar son:

/usr	Por lo menos 1.5 GB en instalaciones básicas. Debe considerarse todo el sustento lógico a utilizar a futuro. Para uso general, se recomiendan no menos de 5 GB. De ser posible, considere un tamaño óptimo de hasta 8 GB en instalaciones promedio.
/tmp	350 MB y se puede asignar hasta 2 GB o más dependiendo de la carga de trabajo y tipo de aplicaciones. Si por ejemplo el sistema cuenta con un grabador de DVD, será necesario asignar a /tmp el espacio suficiente para almacenar una imagen de disco DVD, es decir, al menos 4.2 GB.
/var	**Un mínimo** de 512 MB en estaciones de trabajo **sin servicios**. En servidores, regularmente se le asigna **cuando menos la mitad del disco duro**.
/home	En estaciones de trabajo se asigna cuando menos la mitad del disco duro a esta partición.

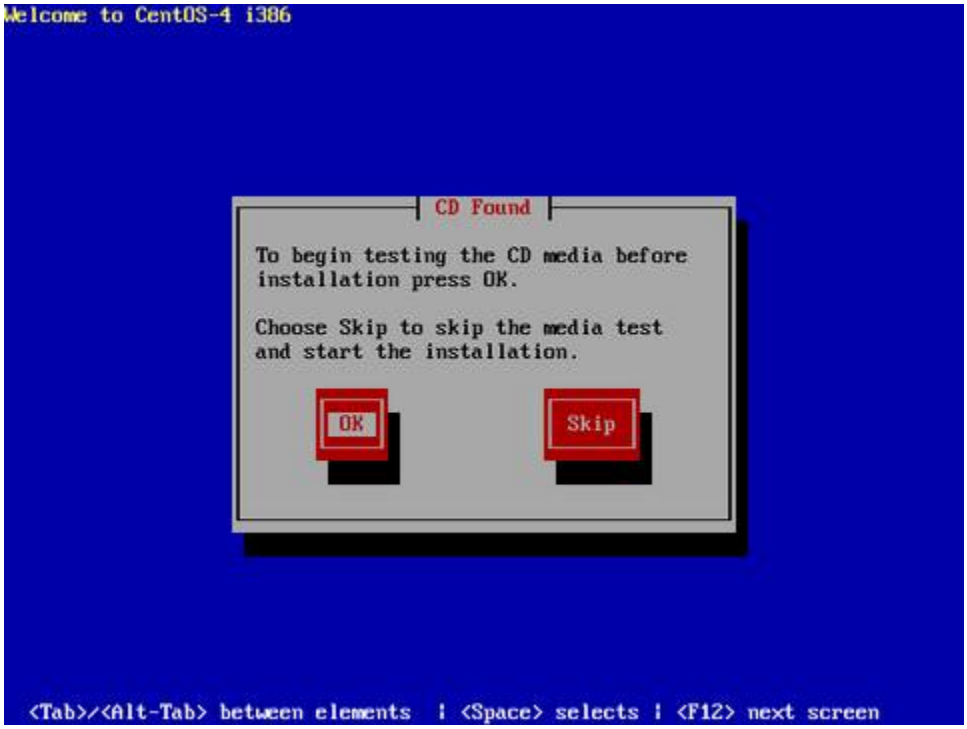
3. Instalación en modo texto de CentOS 4

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

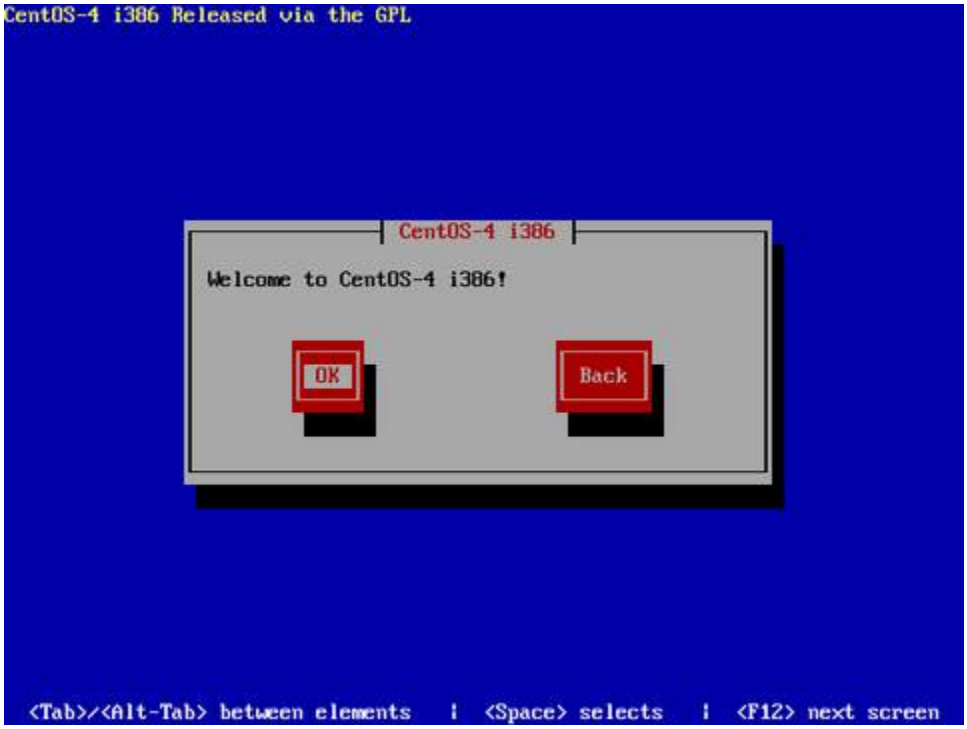
3.1. Procedimientos.

Inserte el disco de instalación de CentOS y en cuanto aparezca el diálogo de inicio (boot:), pulse la tecla **ENTER** o bien ingrese las opciones de instalación deseadas. Para fines prácticos, ingrese **«linux text»** para iniciar la instalación en modo texto.

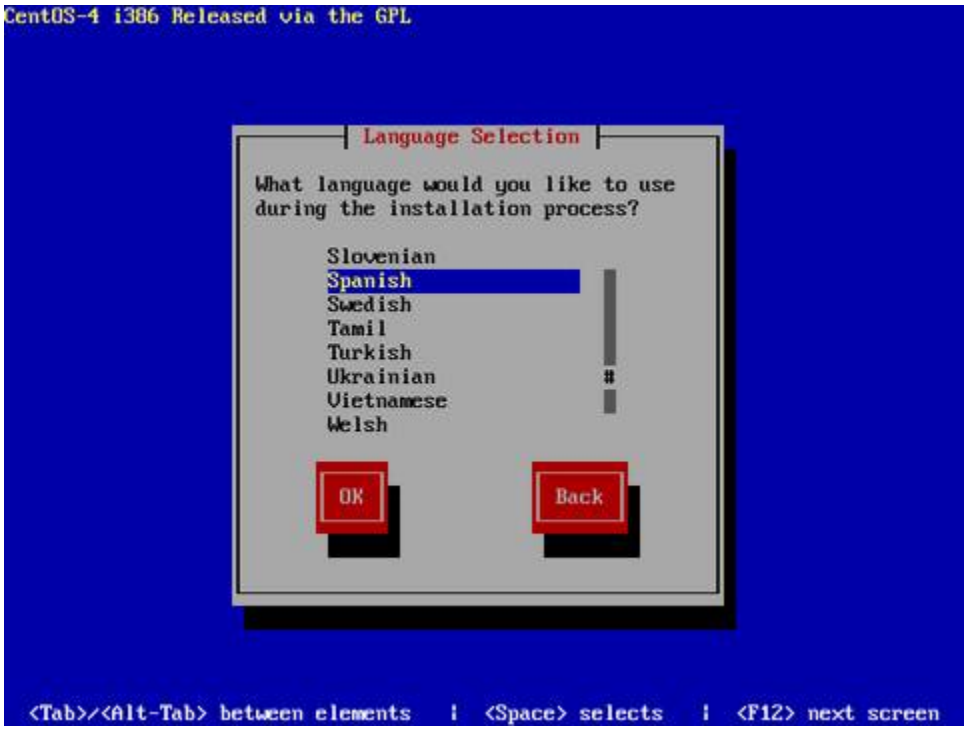
Si desea verificar la integridad del disco a partir del cual se realizará la instalación, seleccione **«OK»** y pulse la tecla **ENTER**, considere que esto puede demorar varios minutos. Si está seguro de que el disco o discos a partir de los cuales se realizará la instalación están en buen estado, seleccione **«Skip»** y pulse la tecla **ENTER**.



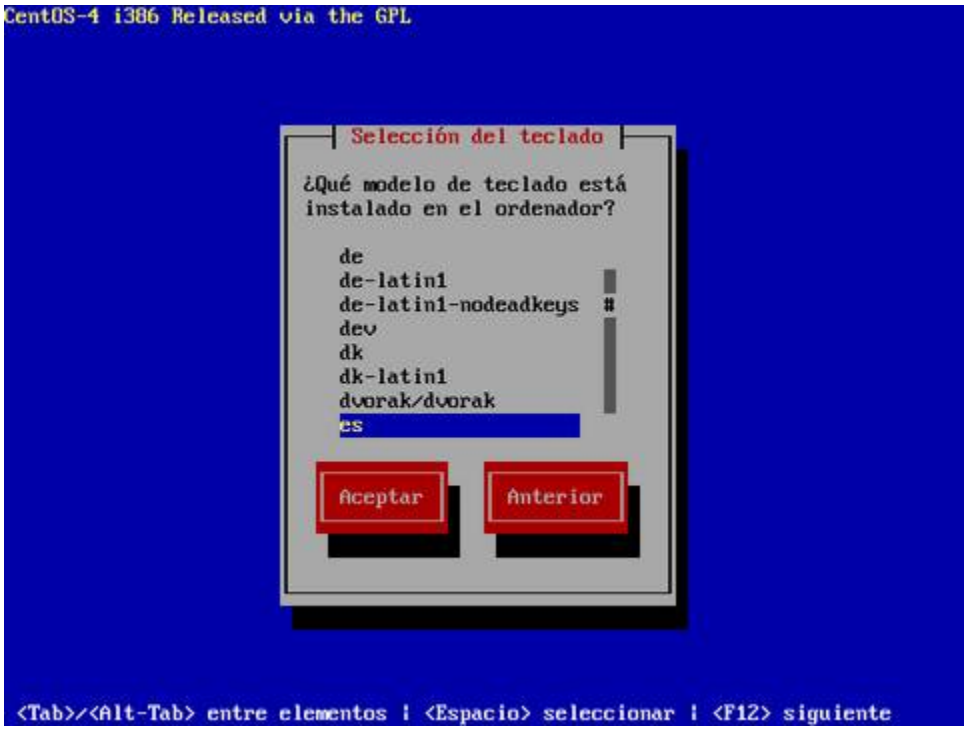
Pulse la tecla **ENTER** en la pantalla de bienvenida al programa de instalación de CentOS.



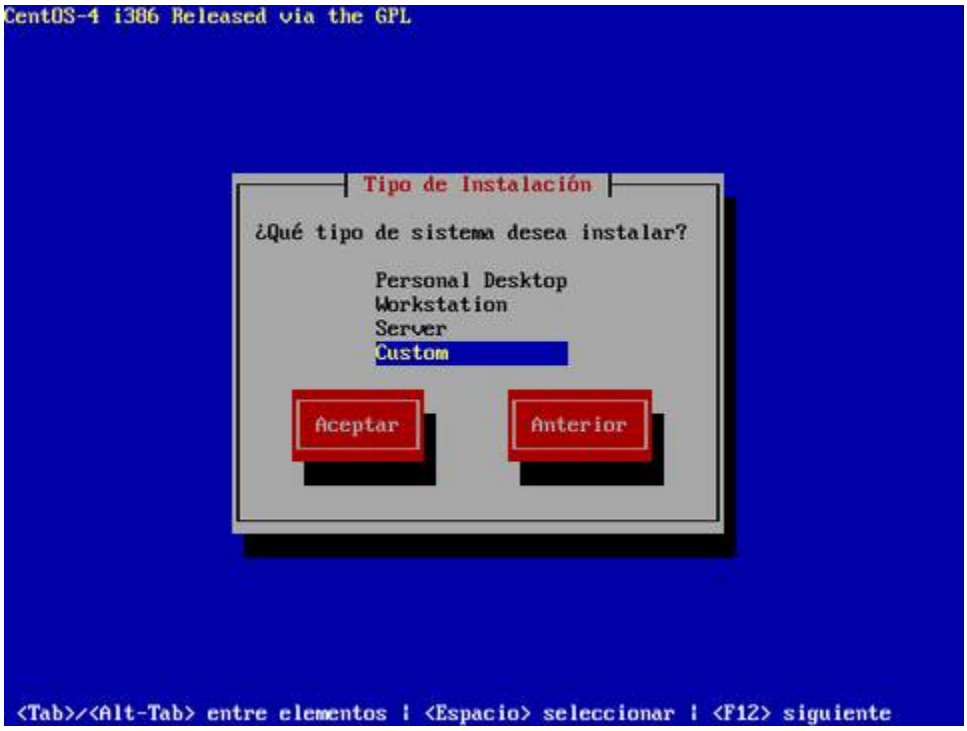
Seleccione **«Spanish»** como idioma para ser utilizado durante la instalación.



Seleccione el mapa de teclado que corresponda al dispositivo utilizado. El mapa **«es»** corresponde a la disposición del teclado Español España. El mapa **«latin-1»** corresponde a la disposición del teclado Español Latino Americano.

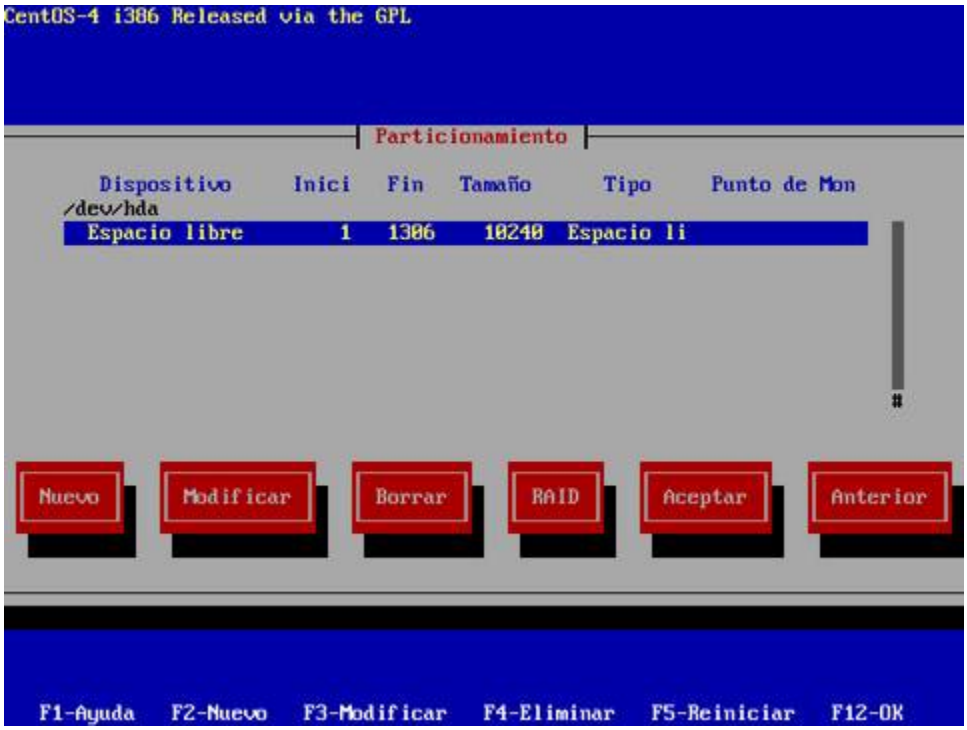


Seleccione **«Custom»** y luego pulse la tecla **ENTER** para realizar una instalación personalizada.

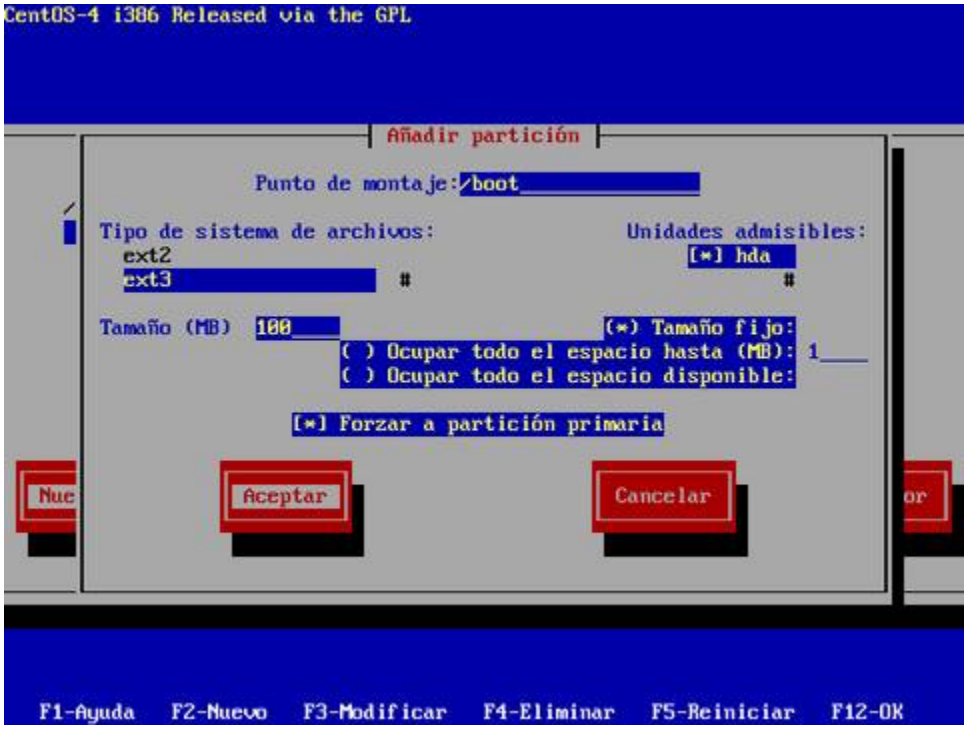


No utilice **«Partición automática»**, a menos de que disponga de muy poco espacio en disco duro. Seleccione **«Disk Druid»** y pulse la tecla **ENTER** para ingresar a la herramienta para particiones del disco duro.

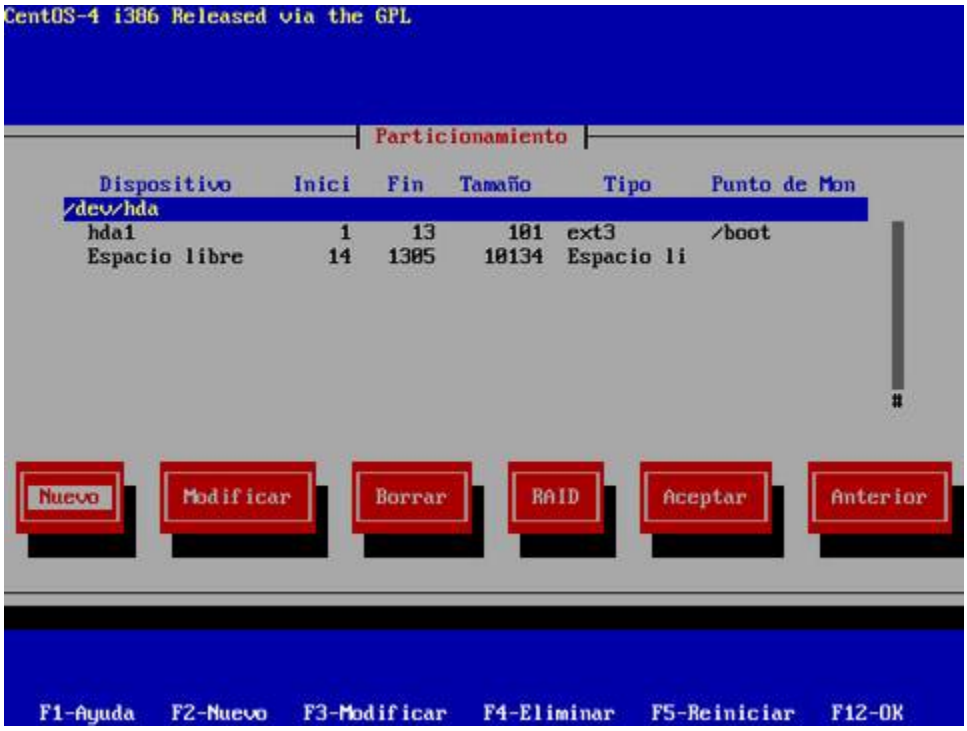
Proceda a crea una nueva partición seleccionado **«Nuevo»** y pulsando la tecla **ENTER**.



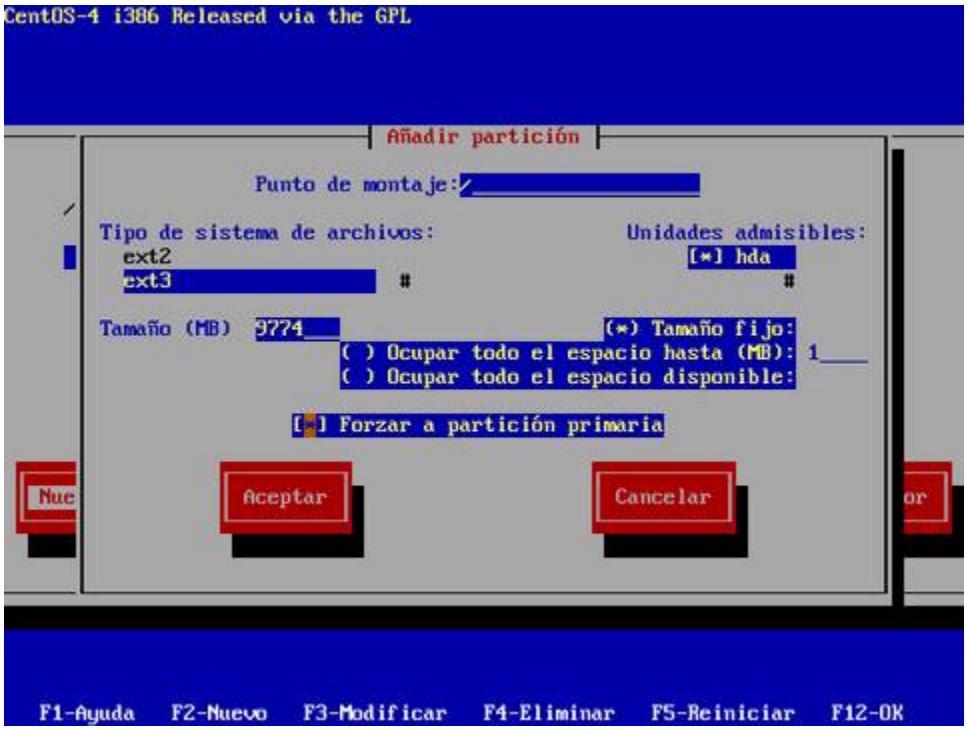
Asigne 100 MB a la partición /boot y defina ésta como partición primaria, siempre que la tabla de particiones lo permita.



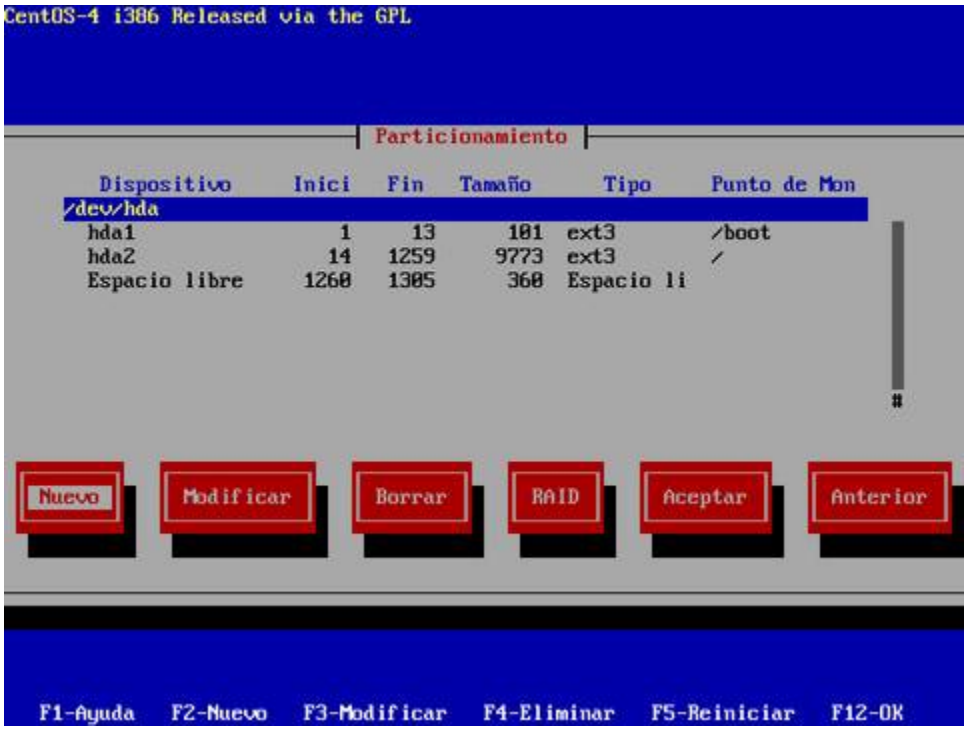
Si está conforme, seleccione otra vez **«Nuevo»** y proceda a crear la siguiente partición.



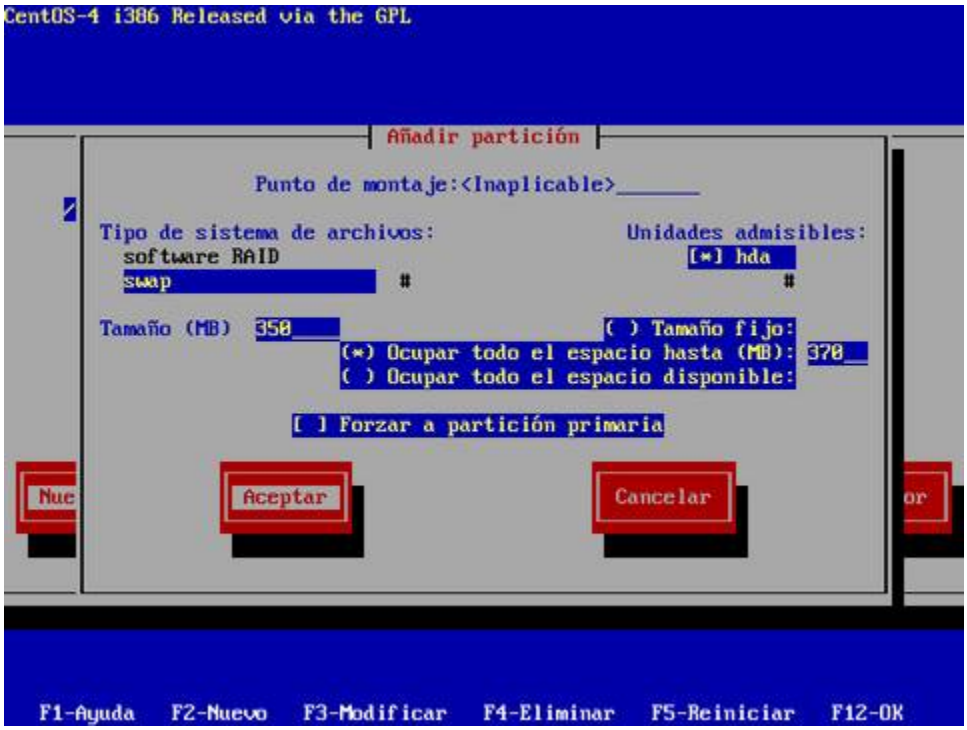
Asigne a la partición / el resto del espacio disponible menos lo que tenga calculado asignar para la partición de intercambio (200% de la memoria física, o cuanto baste para 2 GB). Se recomienda asignar / como partición primaria, siempre que la tabla de particiones lo permita.



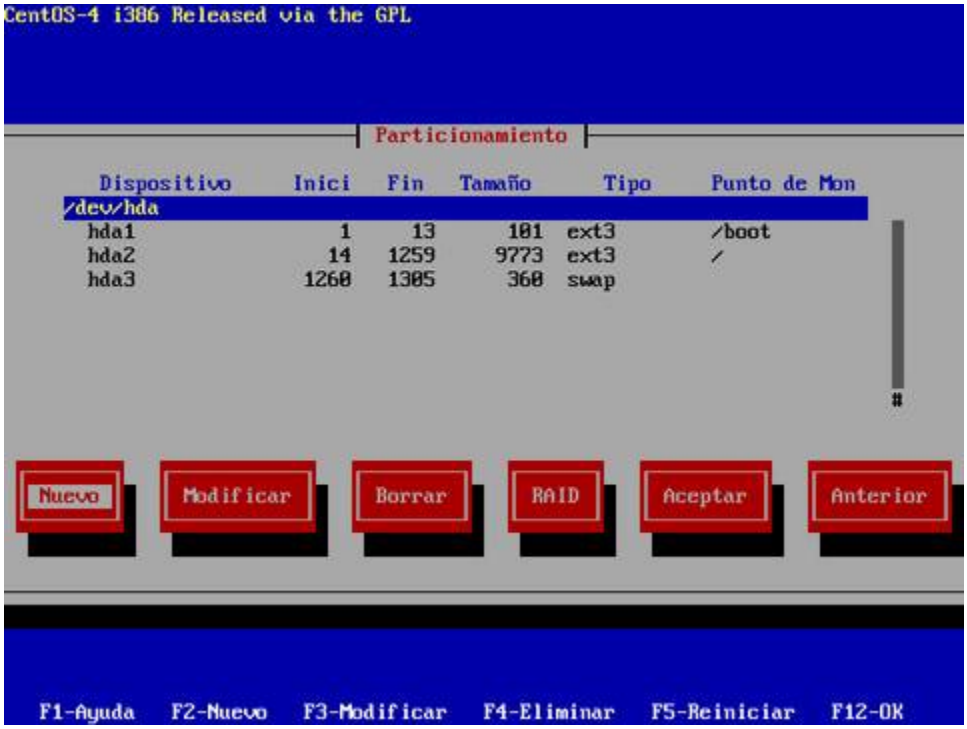
Si está conforme, seleccione otra vez **«Nuevo»** y proceda a crear la siguiente partición.



La partición para la memoria de intercambio no requiere punto de montaje. Seleccione en el campo de **«Tipo de sistema de archivos»** la opción **«swap»**, asigne el 200% de la memoria física (o cuanto basta para 2 GB). Por tratarse de la última partición de la tabla, es buena idea asignarle el espacio por rango.



Si está conforme con la tabla de particiones creada, seleccione **«ACEPTAR»** y pulse la tecla **ENTER** para saltar a la siguiente pantalla.



Seleccione que se utilizará el gestor de arranque GRUB y pulse la tecla **ENTER** para saltar a la siguiente pantalla.

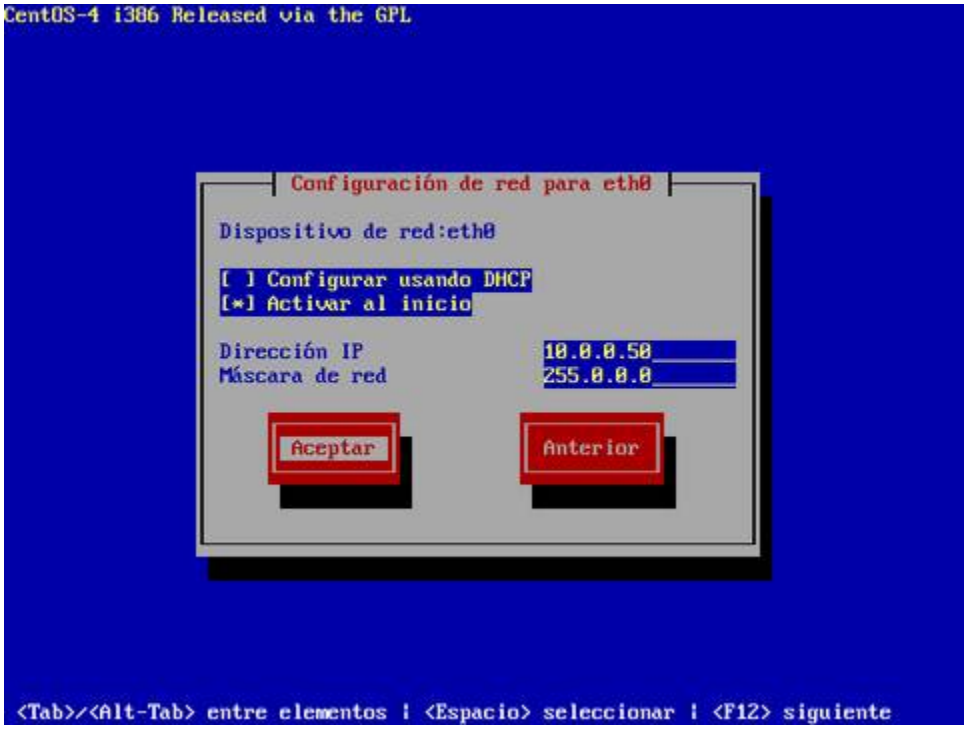
Si necesita pasar algún parámetro en particular al núcleo (kernel), como por ejemplo, la resolución de pantalla para el modo texto, ingrese en el campo correspondiente aquello que sea necesario. En la mayoría de los casos no necesitará ingresar parámetro alguno.

Por motivos de seguridad, y principalmente con la finalidad de impedir que alguien sin autorización y con acceso físico al sistema pueda iniciar el sistema en nivel de corrida 1, o cualquiera otro, asigne, con confirmación, una clave de acceso exclusiva para el gestor de arranque. Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.

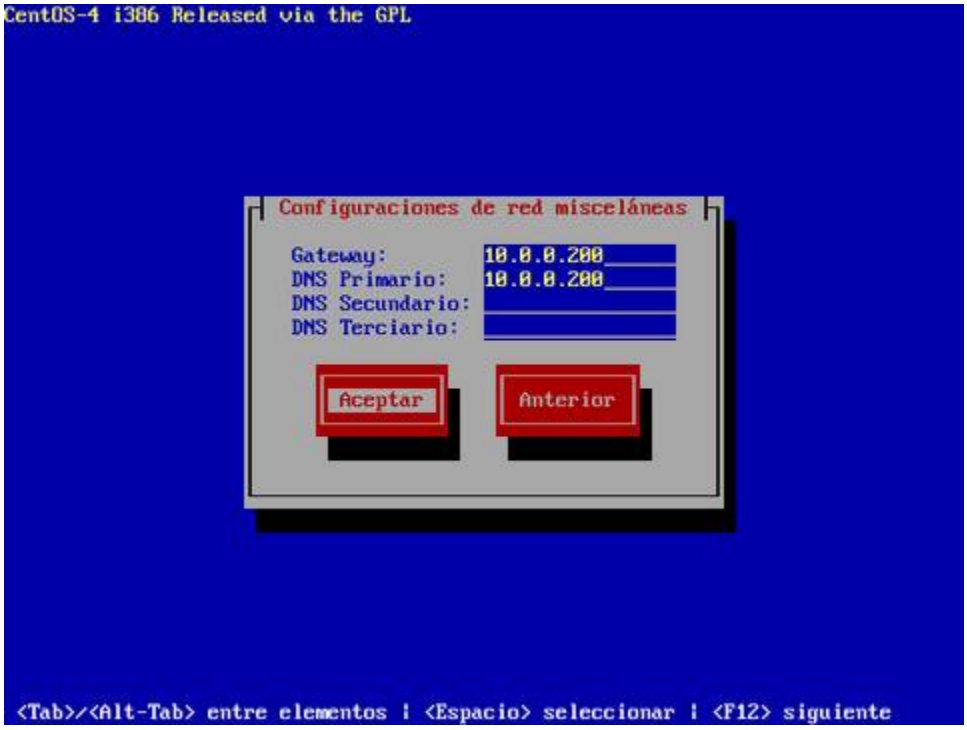
De haber otro sistema operativo instalado en el sistema, seleccione el que utilizará para iniciar de forma predeterminada. Si solo está instalando Linux, solo pulse la tecla **ENTER** para saltar a la siguiente pantalla.

Seleccione que el gestor de arranque se instale en el sector maestro del disco duro (**MBR** o **M**aster **B**oot **R**ecord). Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.

Defina la dirección IP y máscara de subred que utilizará en adelante el sistema. Confirme con el administrador de la red donde se localice que estos datos sean correctos antes de continuar. Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.



Defina la dirección IP de la puerta de enlace y las direcciones IP de los servidores DNS de los que disponga. Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.



Asigne un nombre de anfitrión (HOSTNAME) para el sistema. Se recomienda que dicho nombre sea un **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) resuelto al menos en un DNS local. Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.

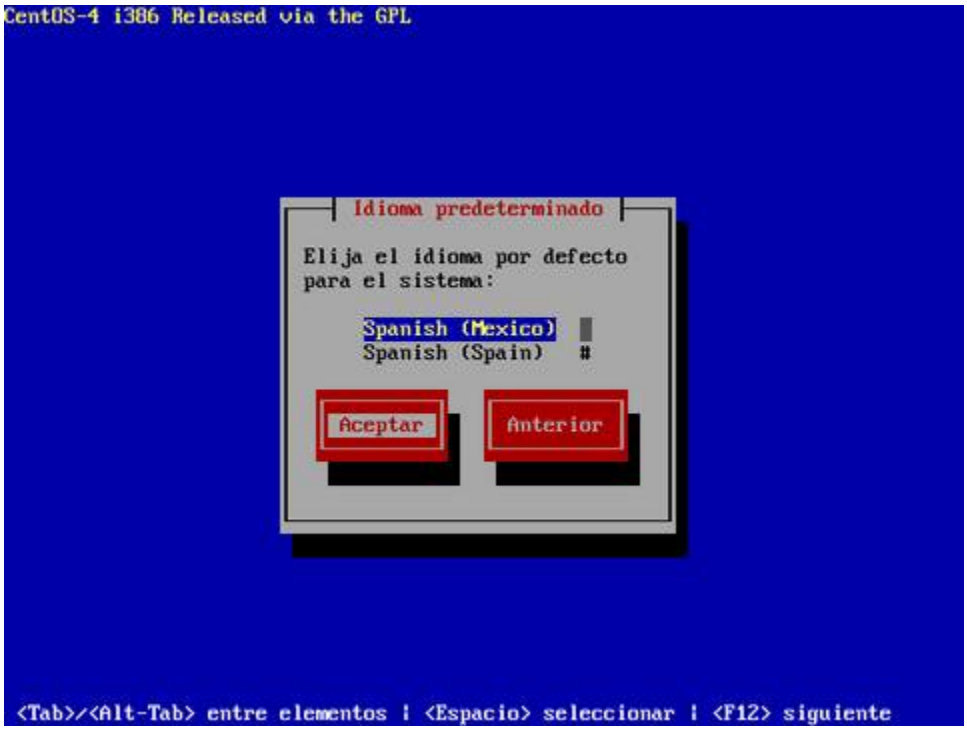
No configure cortafuegos en este momento. La herramienta utilizada para tal fin, **system-config-securitylevel**, crea un cortafuegos simple y con muchas limitaciones. Se recomienda considerar otras alternativas como Firestarter o Shorewall.

Seleccione proceder y pulse la tecla **ENTER** a fin de saltar la configuración del cortafuegos.

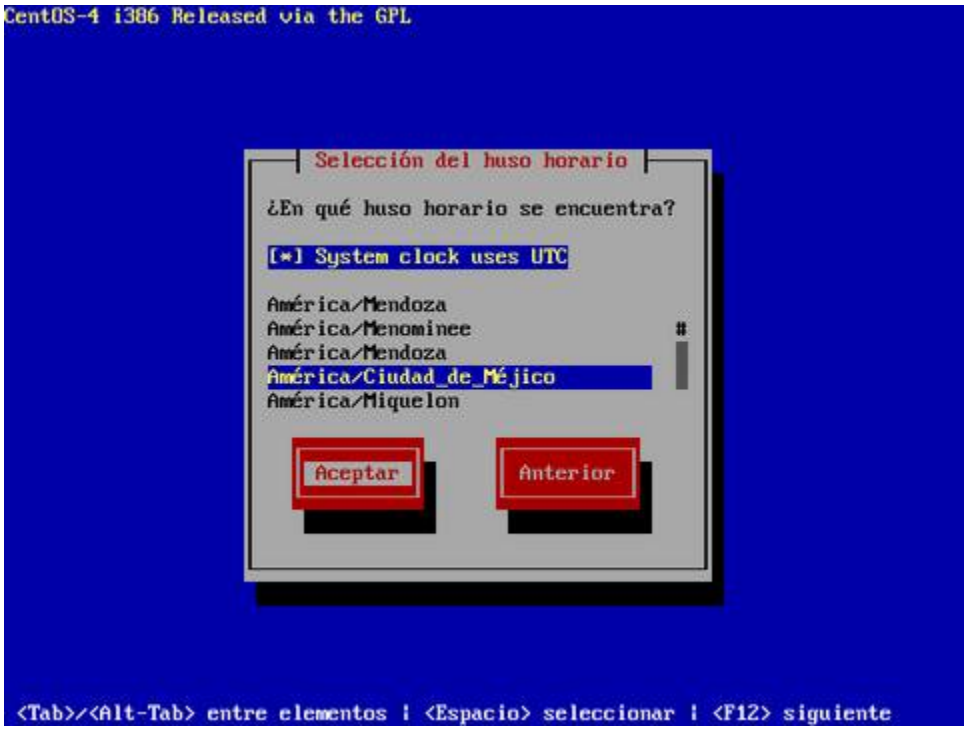
Deje activo SELinux, ya que éste proveerá al sistema de seguridad adicional.

Agregue el soporte para idiomas adicionales de acuerdo al país donde se hospedará el sistema. Si elimina «**Spanish (Spain)**», se eliminará la documentación y soporte para español genérico, por lo que lo es conveniente dejar dicha casilla habilitada.

Seleccione el idioma predeterminado a utilizar en el sistema



Seleccione la casilla **«System clock uses UTC»**, que significa que el reloj del sistema utilizará **UTC** (**T**iempo **U**niversal **C**oordinado), que es el sucesor de **GMT** (b>Greenwich **M**ean **T**ime, que significa Tiempo Promedio de Greenwich), y es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Pulse la tecla de tabulación una vez y seleccione la zona horaria que corresponda a la región donde se hospedará físicamente el sistema.

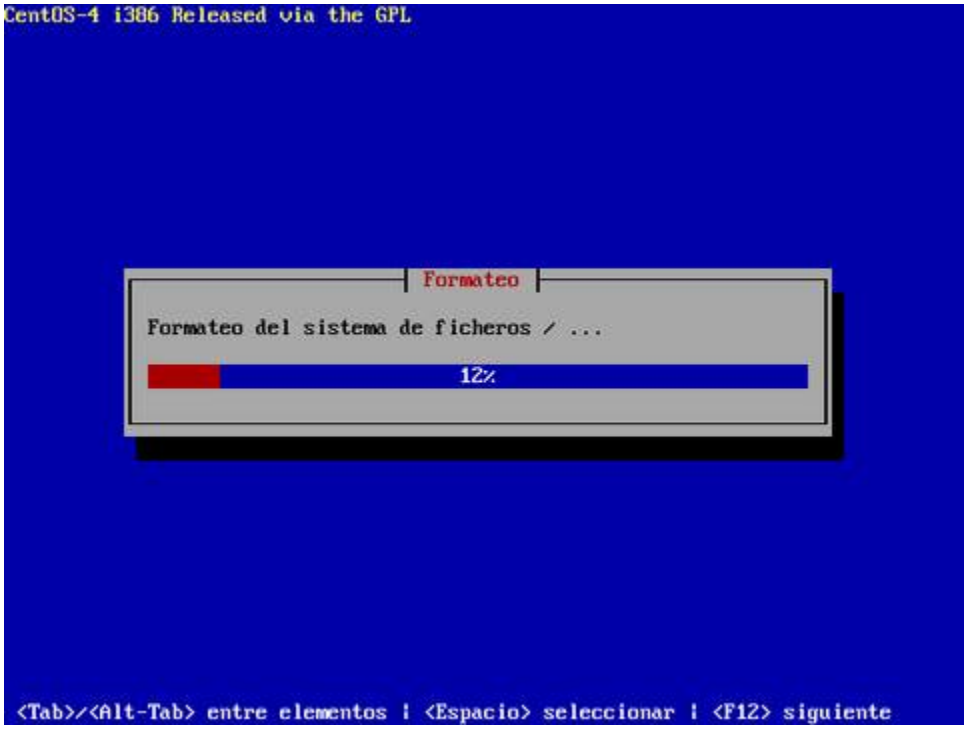


Asigne una clave de acceso al usuario root. Debe escribirla dos veces a fin de verificar que está coincide con lo que realmente se espera. Por razones de seguridad, se recomienda asignar una clave de acceso que evite utilizar palabras provenientes de cualquier diccionario, en cualquier idioma, así como cualquier combinación que tenga relación con datos personales.

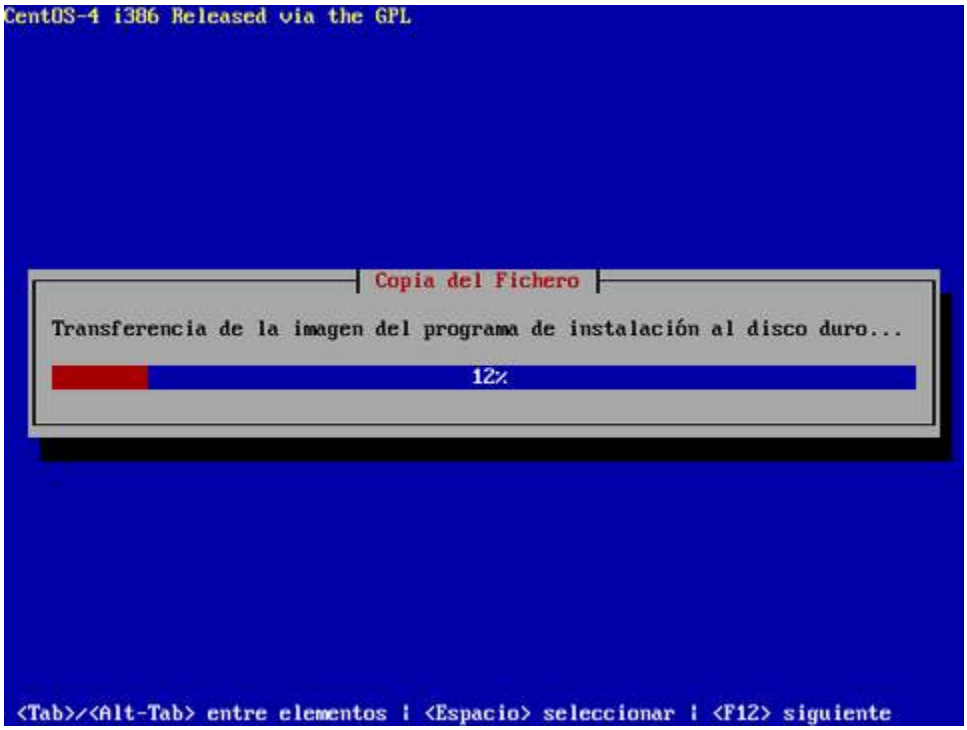
Realice una instalación con el mínimo de paquetes, desactivando todas las casillas de cada grupo de paquetes. El objeto de esto es solo instalar lo mínimo necesario para el funcionamiento del sistema operativo, y permitir instalar, posteriormente, solo aquello que realmente se requiera de acuerdo a la finalidad productiva que tendrá el sistema.

Antes de iniciar la instalación sobre el disco duro, el sistema le informará respecto a que se guardará un registro del proceso en si en el fichero **/root/install.log**. Solo pulse la tecla **ENTER** mientras esté seleccionado **«ACEPTAR»**.

Si iniciará de forma automática el proceso de formato de las particiones que haya creado para instalar el sistema operativo.



Se realizará de forma automática la transferencia de de una imagen del programa de instalación hacia el disco duro, con la finalidad de agilizar el procedimiento.



Iniciará la instalación de los paquetes necesarios para el funcionamiento del sistema operativo. Espere algunos minutos hasta que concluya el proceso.

Una vez concluida la instalación de los paquetes, proceda a pulsar la tecla **ENTER** para reiniciar el sistema.

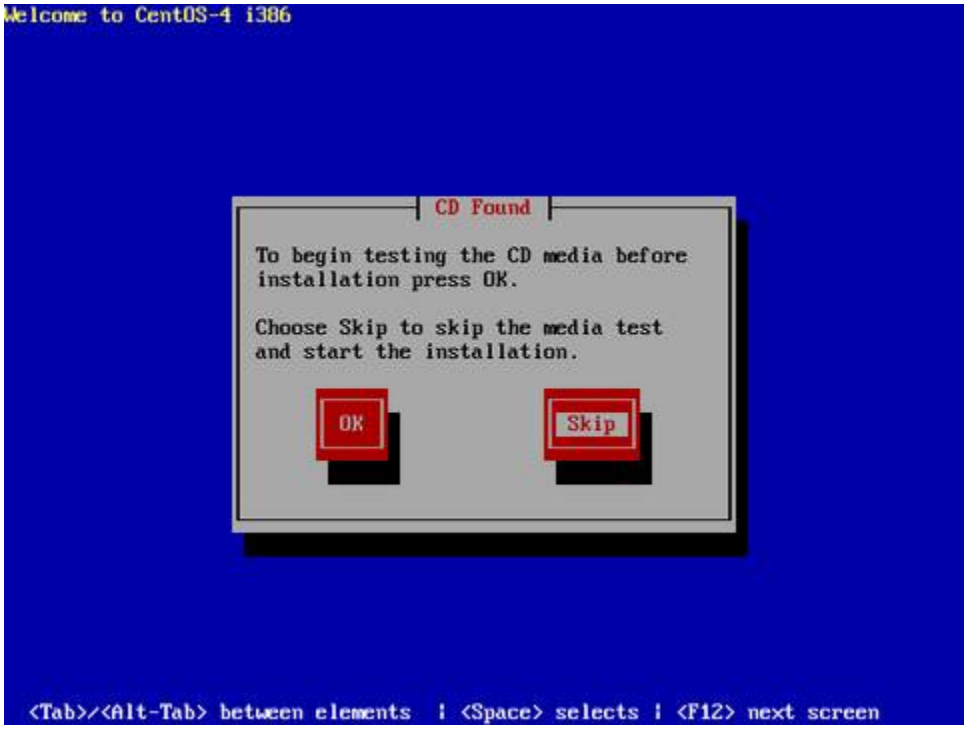
4. Instalación en modo gráfico de CentOS 4

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

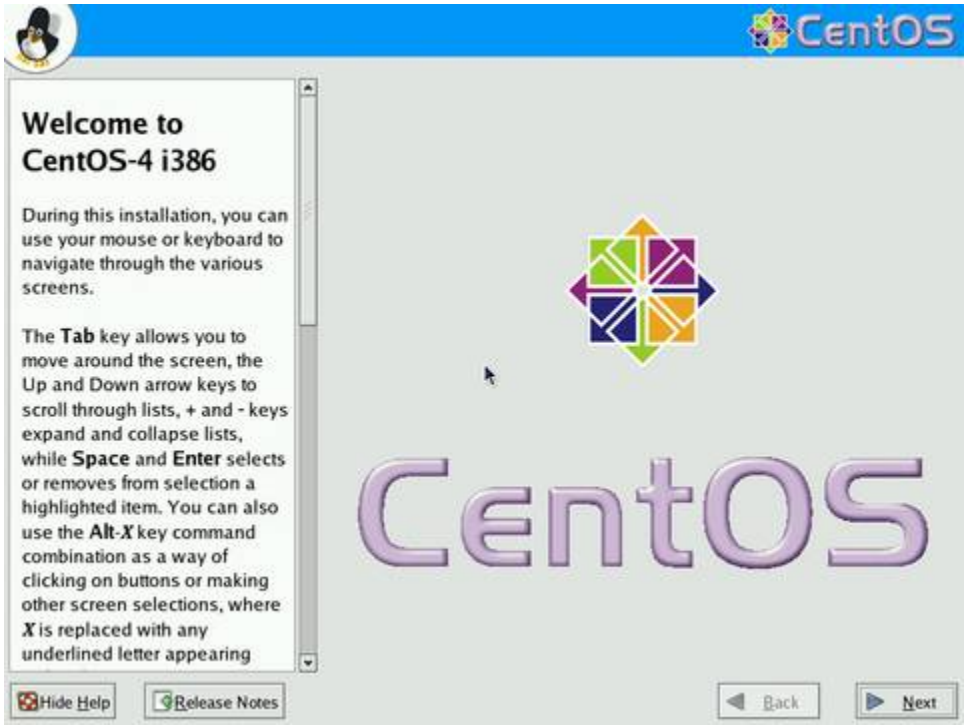
4.1. Procedimientos.

Inserte el disco de instalación de CentOS y en cuanto aparezca el diálogo de inicio (boot:), pulse la tecla **ENTER** o bien ingrese las opciones de instalación deseadas.

Si desea verificar la integridad del disco a partir del cual se realizará la instalación, seleccione **«OK»** y pulse la tecla **ENTER**, considere que esto puede demorar varios minutos. Si está seguro de que el disco o discos a partir de los cuales se realizará la instalación están en buen estado, seleccione **«Skip»** y pulse la tecla **ENTER**.

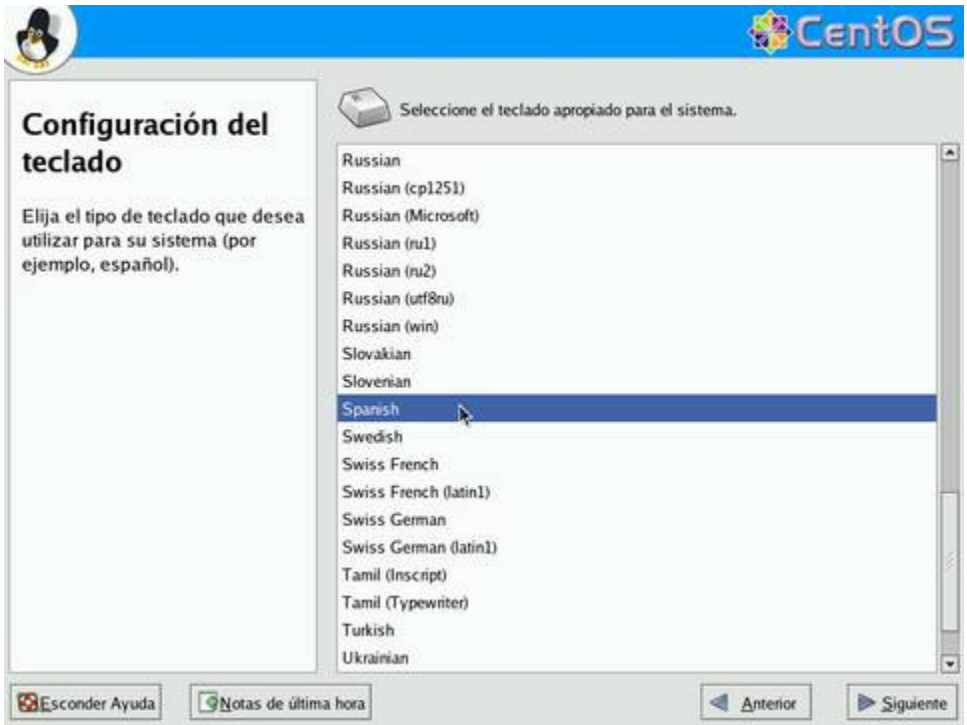


Haga clic sobre el botón **«Next»** en cuanto aparezca la pantalla de bienvenida de CentOS.



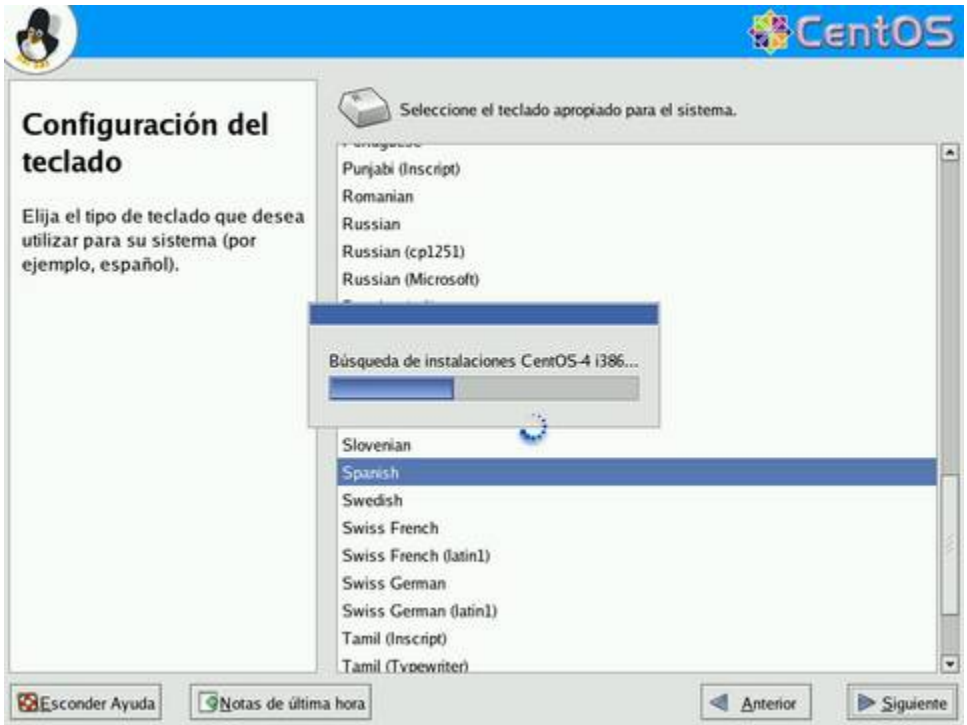
Seleccione **«Spanish»** como idioma para ser utilizado durante la instalación.

Seleccione el mapa de teclado que corresponda al dispositivo utilizado. El mapa **«Spanish»** corresponde a la disposición del teclado Español España. Al terminar, haga clic sobre el botón **«Siguiente»**.



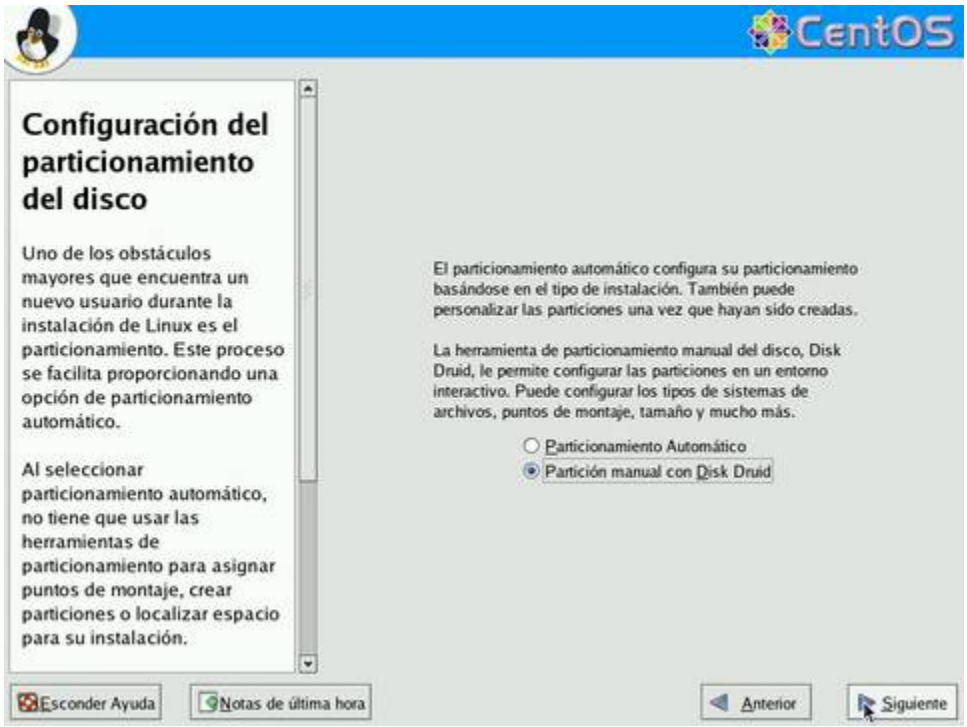
Si es necesario, el mapa **«Latin American»** corresponde a la disposición del teclado Español Latino Americano. Al terminar, haga clic sobre el botón **«Siguiente»**.

Haga clic sobre el botón **«Siguiente»** y espere a que el sistema intente detectar instalaciones previas de CentOS.

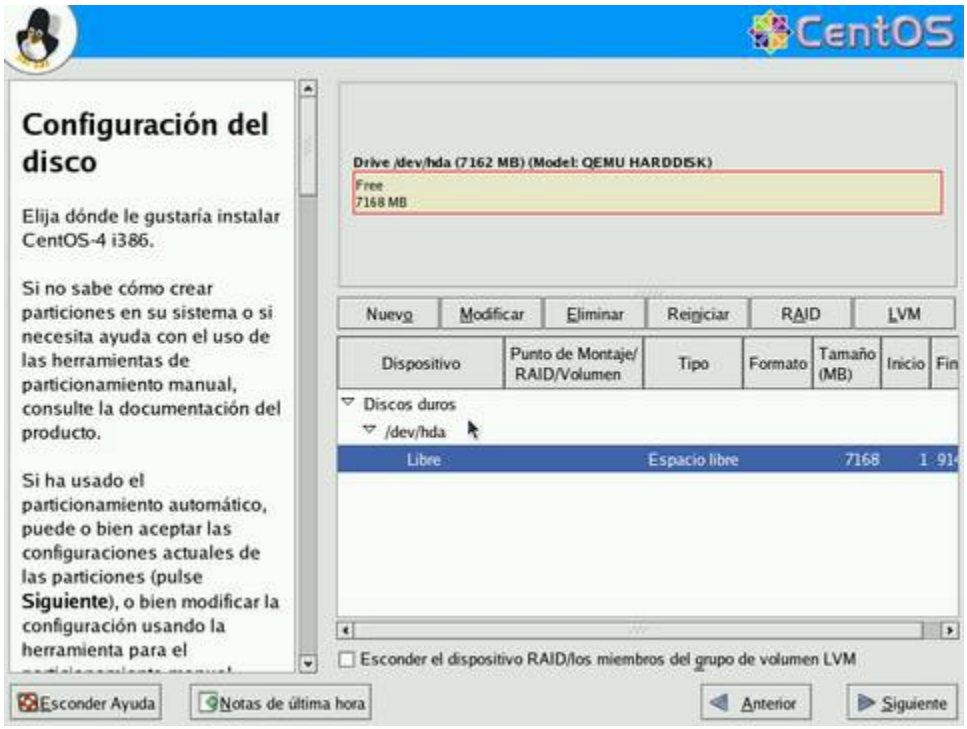


Seleccione el tipo de instalación **«Personalizada»** para realizar esta con un mayor control de las opciones disponibles. Al terminar, haga clic sobre el botón **«Siguiente»**.

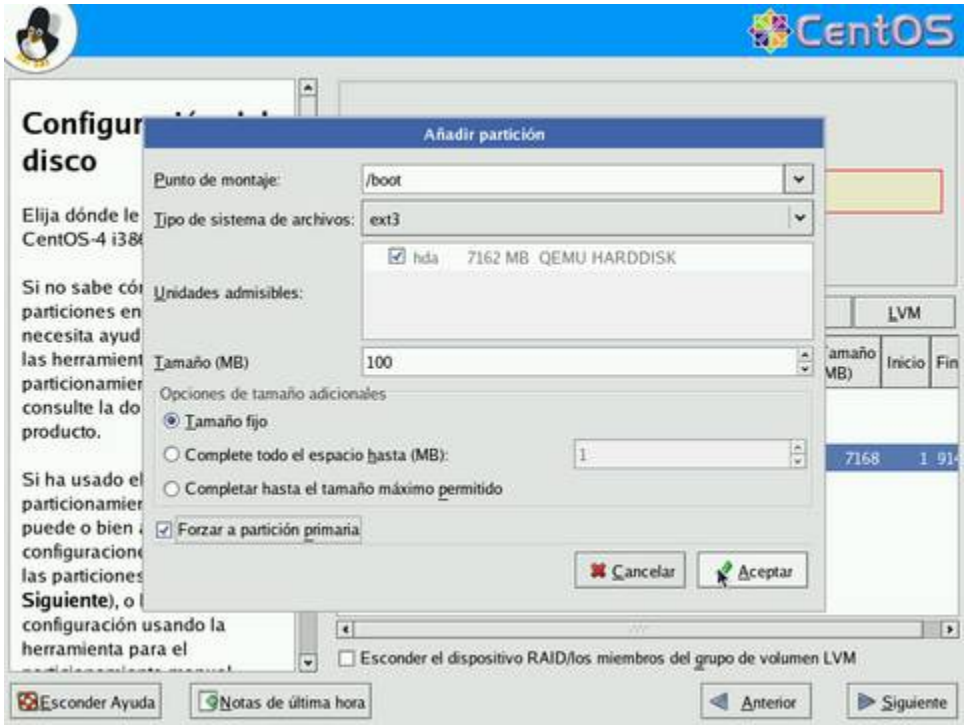
No utilice **«Particionamiento Automático»**, a menos de que disponga de muy poco espacio en disco duro. Seleccione **«Disk Druid»**. Al terminar, haga clic sobre el botón **«Siguiente»** para ingresar a la herramienta para particiones del disco duro.



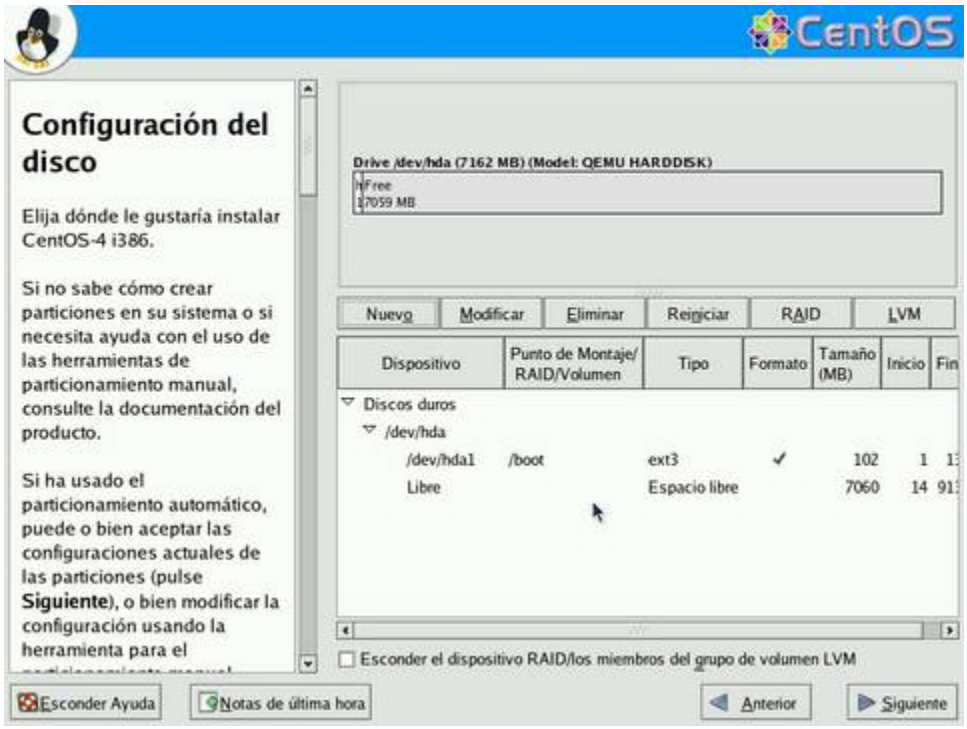
La herramienta de particiones mostrará el espacio disponible. Haga clic en el botón «**Nuevo**».



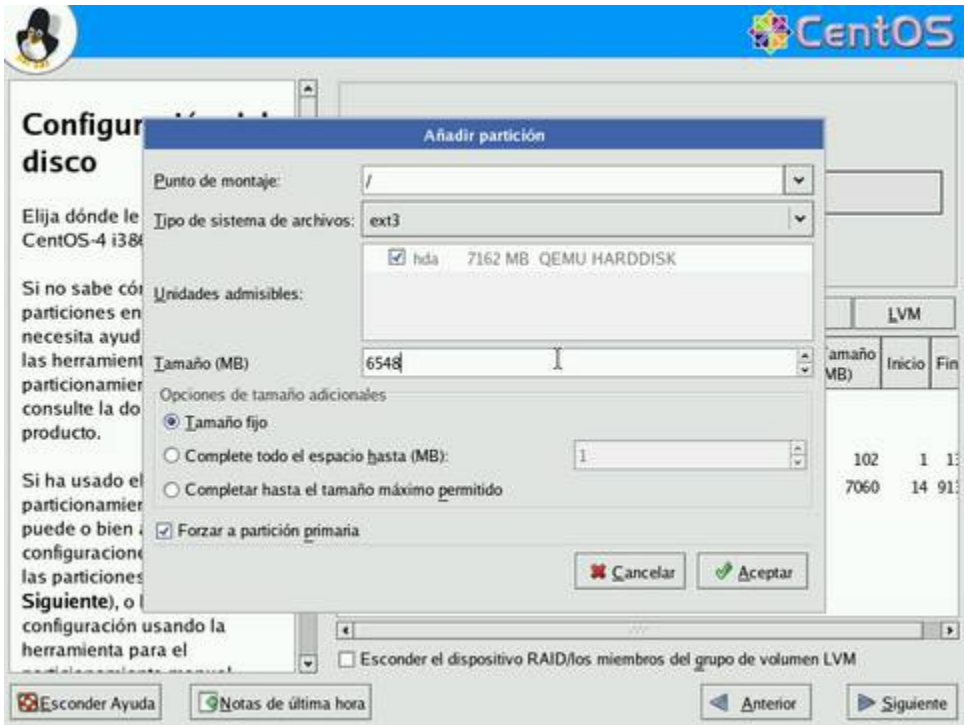
Asigne 100 MB a la partición /boot y defina ésta como partición primaria, siempre que la tabla de particiones lo permita.



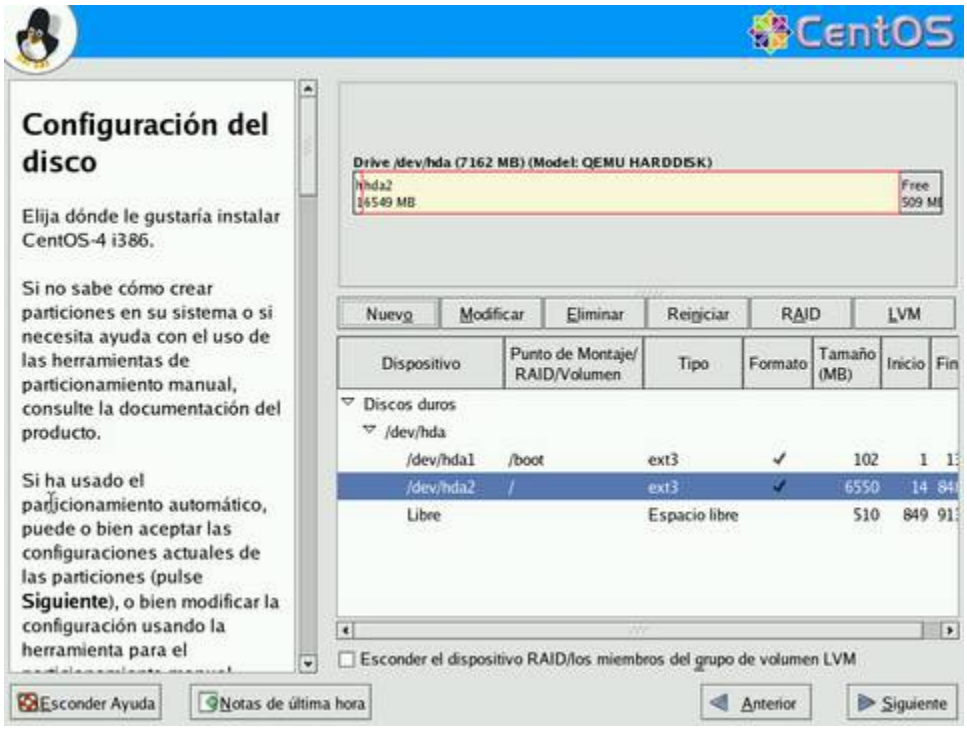
Si está conforme, haga clic otra vez en el botón **«Nuevo»** y proceda a crear la siguiente partición.



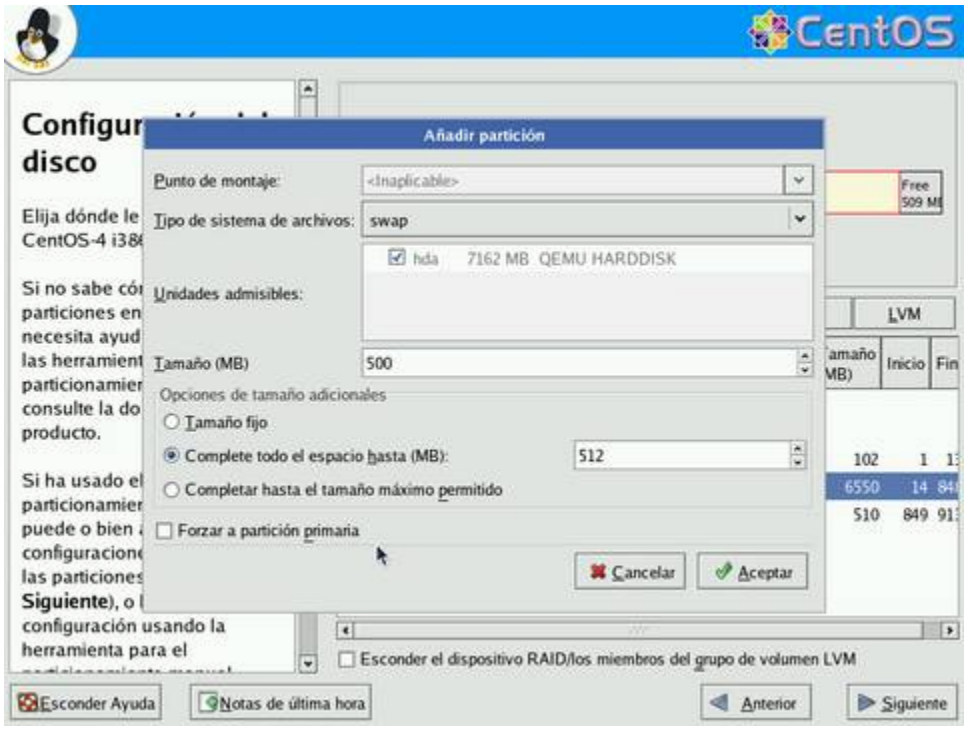
Asigne a la partición / el resto del espacio disponible menos lo que tenga calculado asignar para la partición de intercambio (200% de la memoria física, o cuanto baste para 2 GB). Se recomienda asignar / como partición primaria, siempre que la tabla de particiones lo permita.



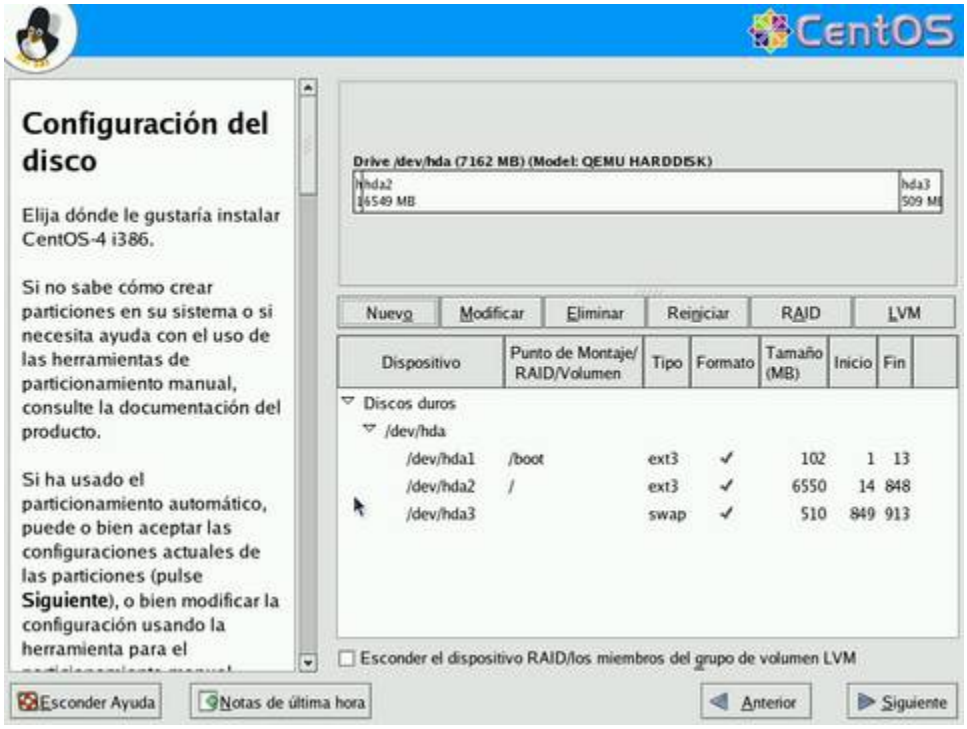
Si está conforme, haga clic otra vez en el botón **«Nuevo»** y proceda a crear la siguiente partición.



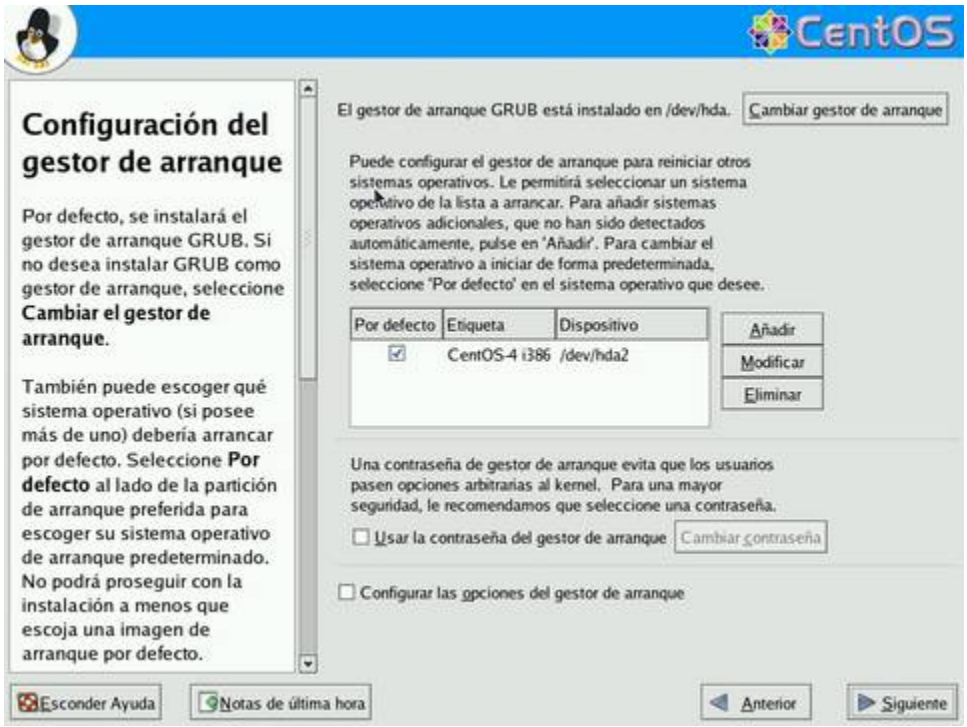
La partición para la memoria de intercambio no requiere punto de montaje. Seleccione en el campo de **«Tipo de sistema de archivos»** la opción **«swap»**, asigne el 200% de la memoria física (o cuanto basta para 2 GB). Por tratarse de la última partición de la tabla, es buena idea asignarle el espacio por rango, especificando valores ligeramente por debajo y ligeramente por arriba de lo planeado.



Si está conforme con la tabla de particiones creada, seleccione **«ACEPTAR»** y haga clic sobre el botón **«siguiente»** para pasar a la siguiente pantalla.

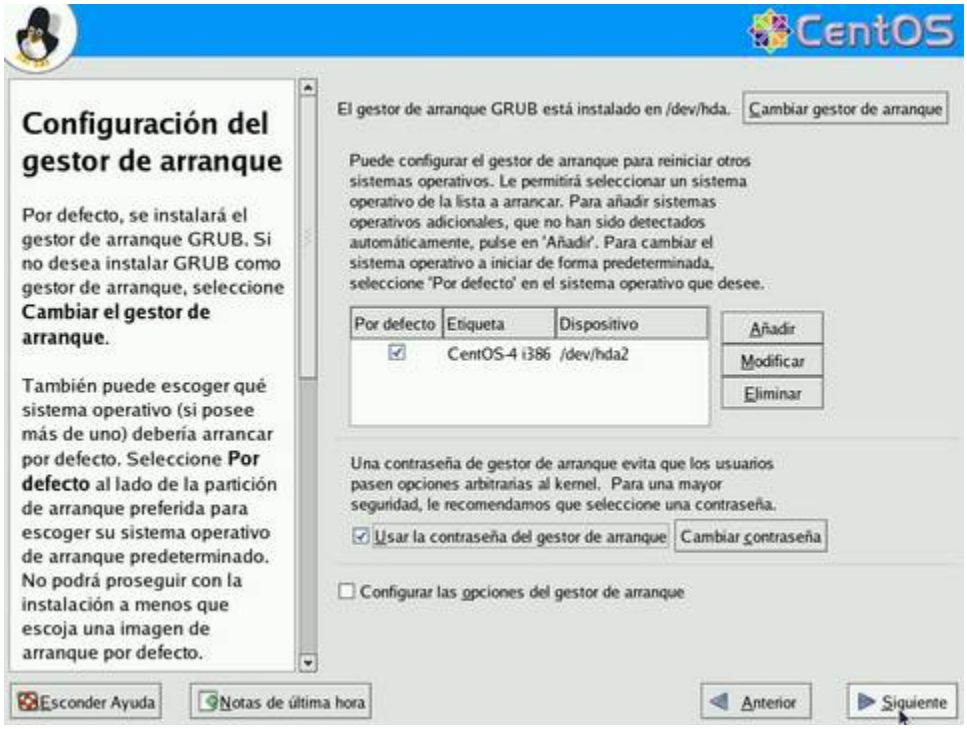


Por motivos de seguridad, y principalmente con la finalidad de impedir que alguien sin autorización y con acceso físico al sistema pueda iniciar el sistema en nivel de corrida 1, o cualquiera otro, haga clic en la casilla **«Usar la contraseña del gestor de arranque»**.

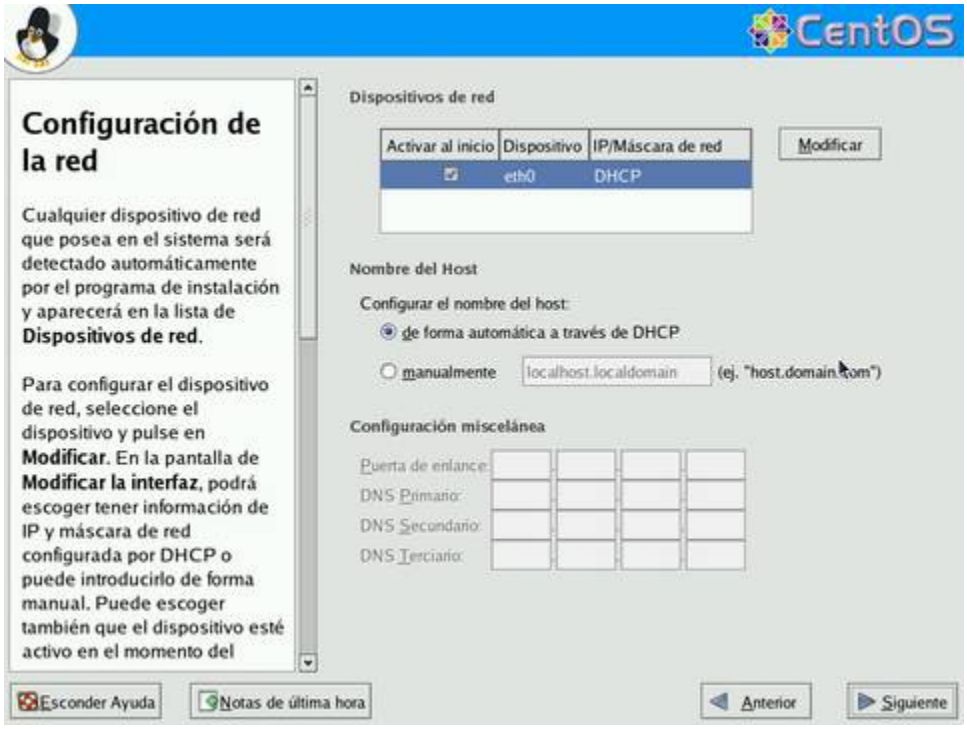


Se abrirá una ventana emergente donde deberá ingresar, con confirmación, la clave de acceso exclusiva para el gestor de arranque. Al terminar, haga clic sobre el botón **«Aceptar»**.

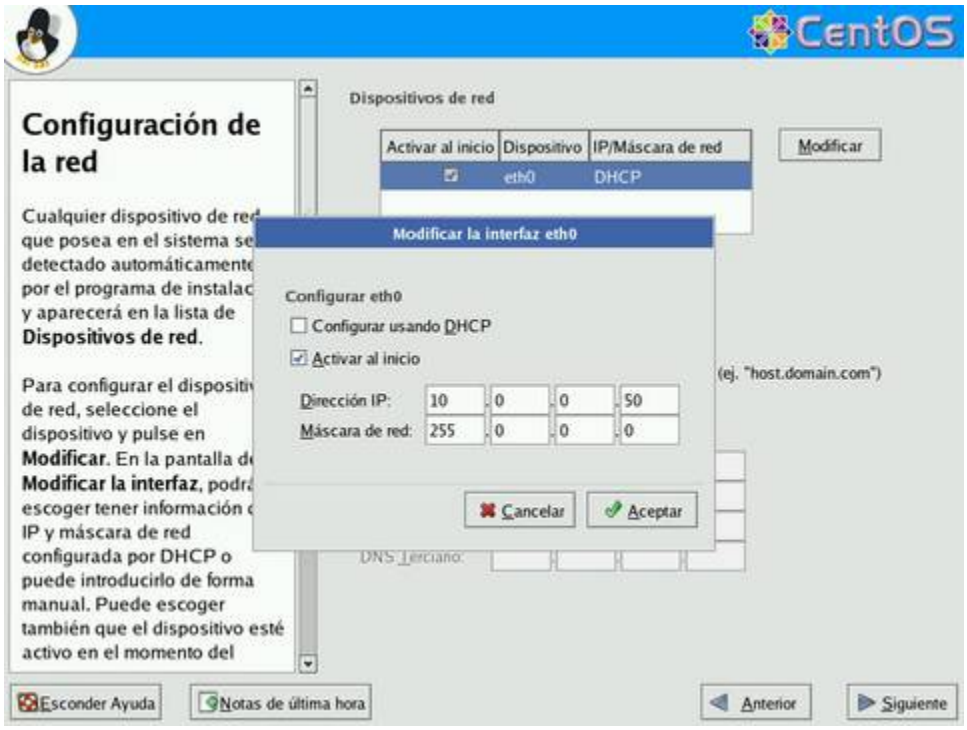
Al terminar, haga clic sobre el botón **«Siguiente»**.



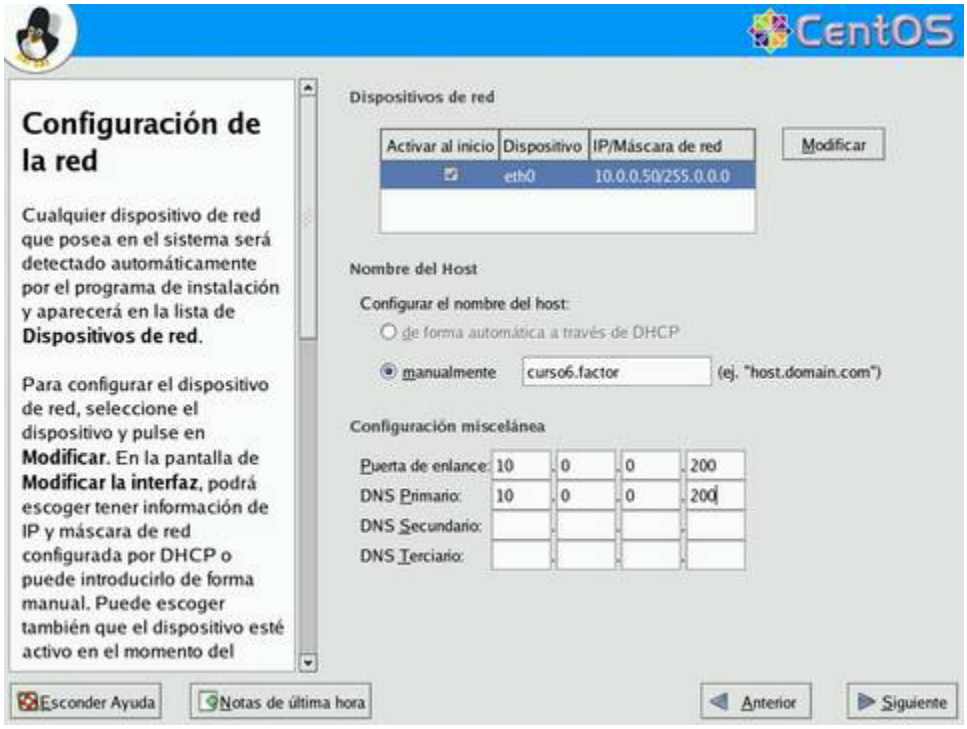
Para configurar los parámetros de red del sistema, haga clic sobre el botón **«Modificar»** para la interfaz eth0.



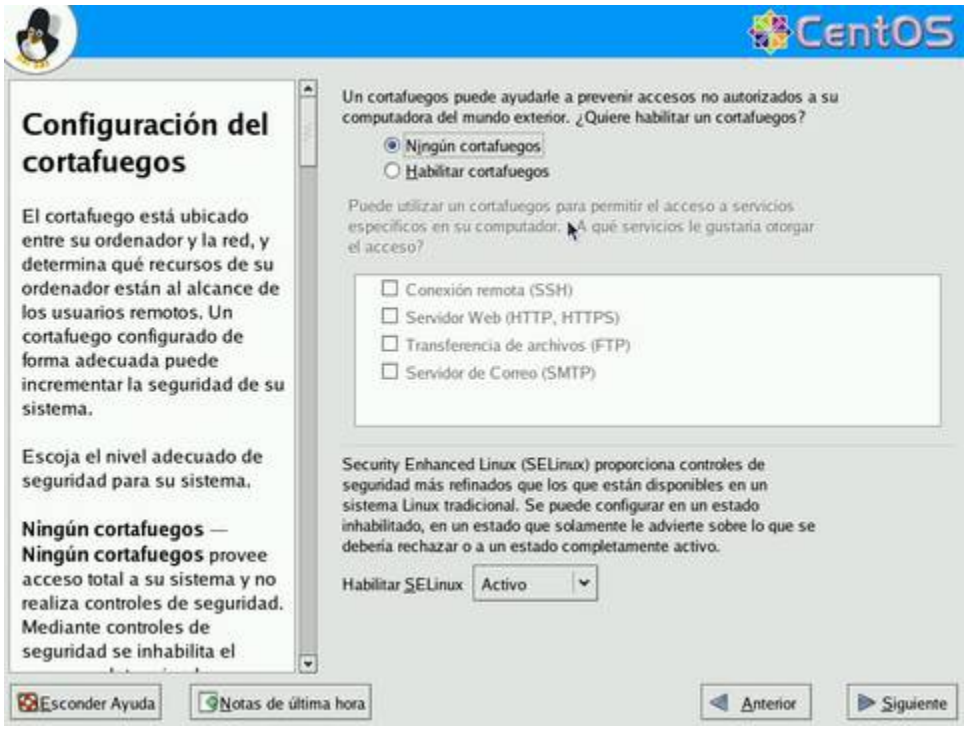
En la ventana emergente para modificar la interfaz eth0, desactive la casilla **«Configurar usando DHCP»** y especifique la dirección IP y máscara de subred que utilizará en adelante el sistema. Confirme con el administrador de la red donde se localice que estos datos sean correctos antes de continuar. Al terminar, haga clic sobre el botón **«Aceptar»**.



Asigne un nombre de anfitrión (HOSTNAME) para el sistema. Se recomienda que dicho nombre sea un **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) resuelto al menos en un DNS local. Defina, además, en esta misma pantalla, la dirección IP de la puerta de enlace y las direcciones IP de los servidores DNS de los que disponga. Al terminar, haga clic sobre el botón **«Siguiente»**.



No configure cortafuegos en este momento. La herramienta utilizada para tal fin, **system-config-securitylevel**, crea un cortafuegos simple y con muchas limitaciones. Se recomienda considerar otras alternativas como Firestarter o Shorewall. Deje activo SELinux, ya que éste proveerá al sistema de seguridad adicional. Al terminar, haga clic sobre el botón **«Siguiente»**.

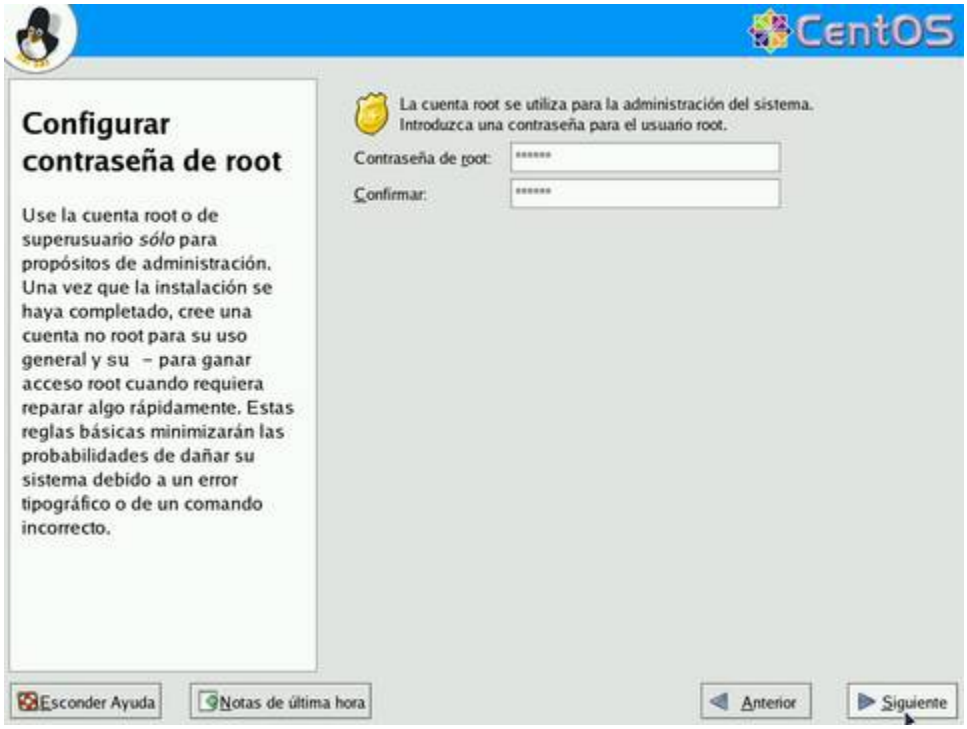


Haga clic sobre el botón **«Proceder»** a fin de saltar la configuración del cortafuegos.

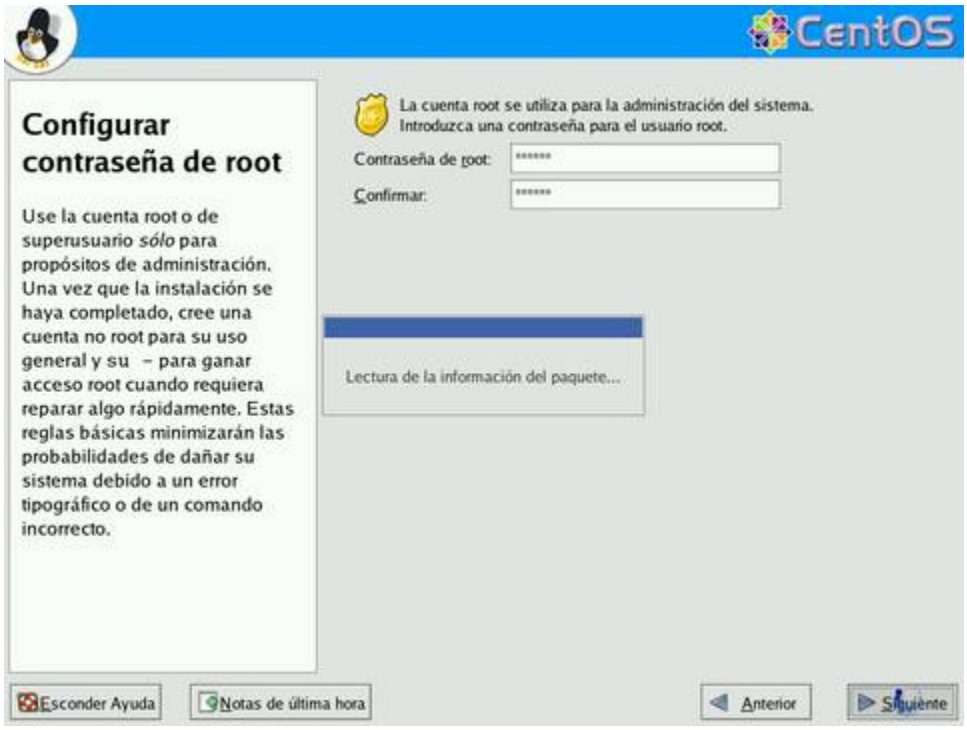
Agregue el soporte para idiomas adicionales de acuerdo al país donde se hospedará el sistema. Si elimina **«Spanish (Spain)»**, se eliminará la documentación y soporte para español genérico, por lo que lo es conveniente dejar dicha casilla habilitada. Finalmente, seleccione el idioma predeterminado a utilizar en el sistema. Al terminar, haga clic sobre el botón **«Siguiente»**.

Seleccione la casilla **«El sistema horario usará UTC»**, que significa que el reloj del sistema utilizará **UTC** (**T**iempo **U**niversal **C**oordinado), que es el sucesor de **GMT** (b>Greenwich **M**ean **T**ime, que significa Tiempo Promedio de Greenwich), y es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Haga clic con el ratón sobre la región que corresponda en el mapa mundial o seleccione en el siguiente campo la zona horaria que corresponda a la región donde se hospedará físicamente el sistema.

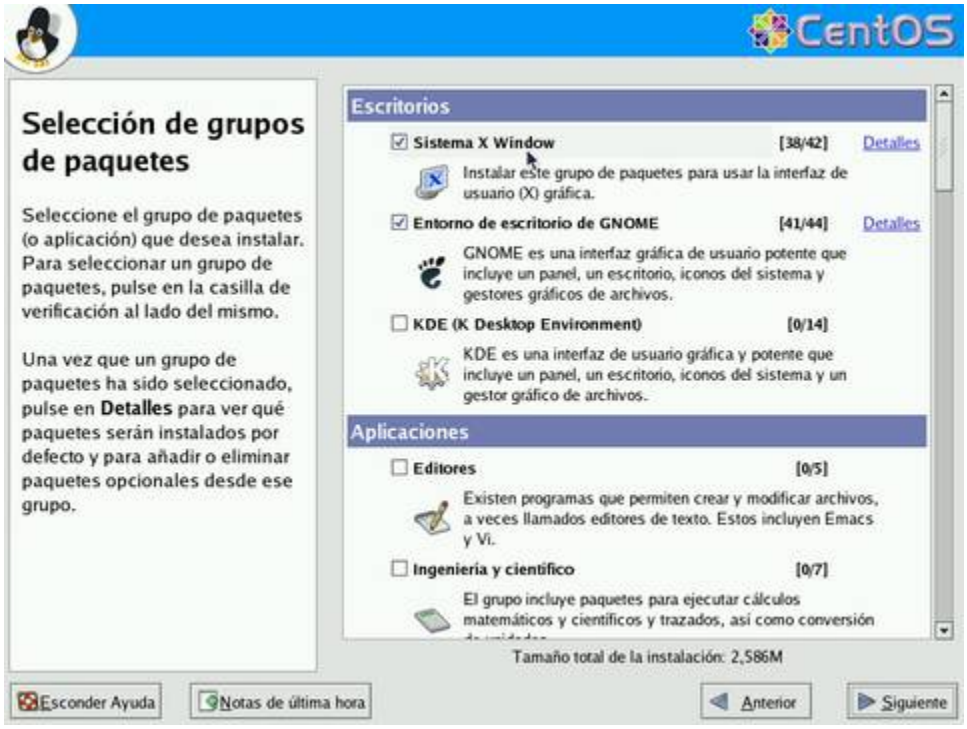
Asigne una clave de acceso al usuario **root**. Debe escribirla dos veces a fin de verificar que está coincide con lo que realmente se espera. Por razones de seguridad, se recomienda asignar una clave de acceso que evite utilizar palabras provenientes de cualquier diccionario, en cualquier idioma, así como cualquier combinación que tenga relación con datos personales.



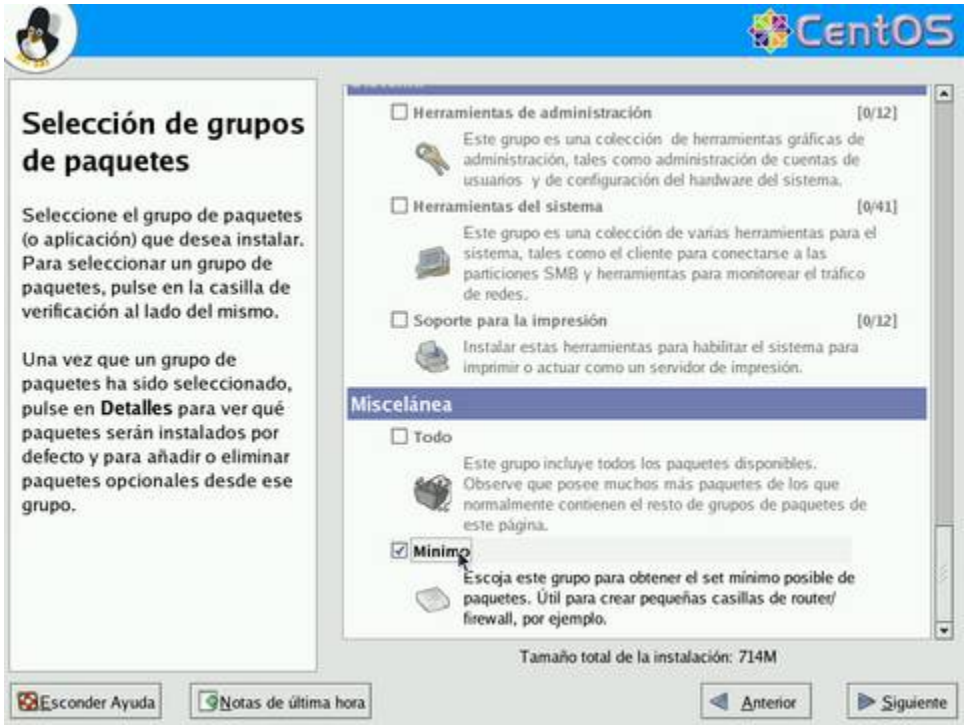
Al terminar, haga clic sobre el botón «**Siguiente**», y espere a que el sistema haga la lectura de información de los grupos de paquetes.



En la siguiente pantalla podrá seleccionar los grupos de paquetes que quiera instalar en el sistema. Añada o elimine a su conveniencia.



Lo recomendado, sobre todo si se trata de un servidor, es realizar una instalación con el mínimo de paquetes, activando la casilla **«Mínimo»** que está al final de la lista de grupos de paquetes. El objeto de esto es solo instalar lo mínimo necesario para el funcionamiento del sistema operativo, y permitir instalar, posteriormente, solo aquello que realmente se requiera de acuerdo a la finalidad productiva que tendrá el sistema. Al terminar, haga clic sobre el botón **«Siguiente»**.



Una vez hecho lo anterior, haga clic sobre el botón **«Siguiente» a fin de iniciar el proceso.**

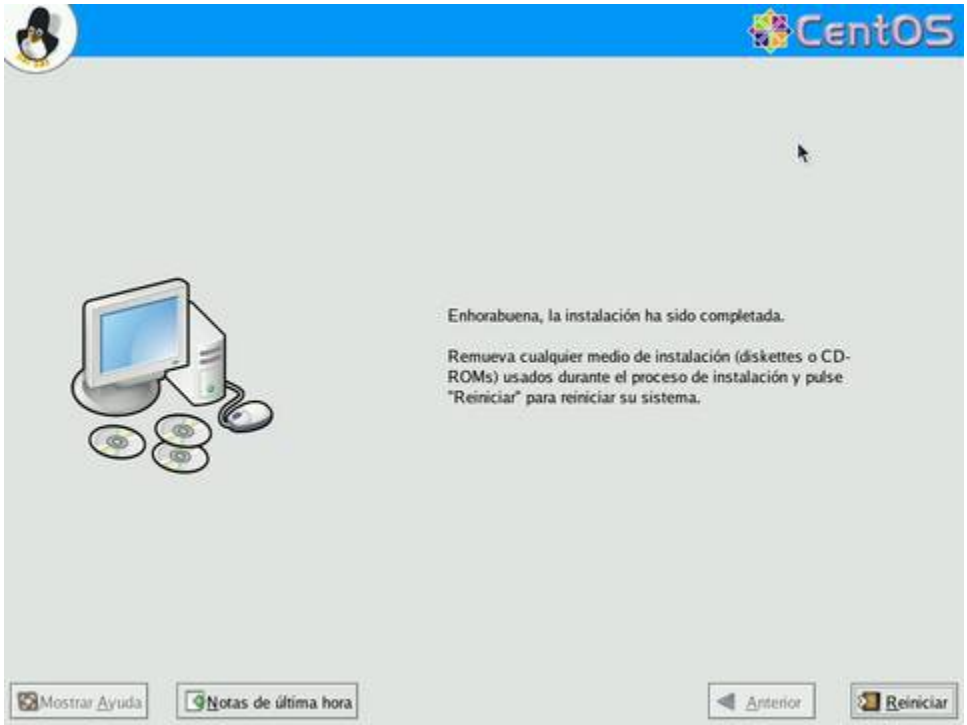
Si iniciará de forma automática el proceso de formato de las particiones que haya creado para instalar el sistema operativo.

Se realizará de forma automática la transferencia de de una imagen del programa de instalación hacia el disco duro, con la finalidad de agilizar el procedimiento.

Espere a que se terminen los preparativos del proceso de instalación.

Iniciará la instalación de los paquetes necesarios para el funcionamiento del sistema operativo. Espere algunos minutos hasta que concluya el proceso.

Una vez concluida la instalación de los paquetes, haga clic sobre el botón «**Reiniciar**».



5. Instalación en modo texto de CentOS 5.

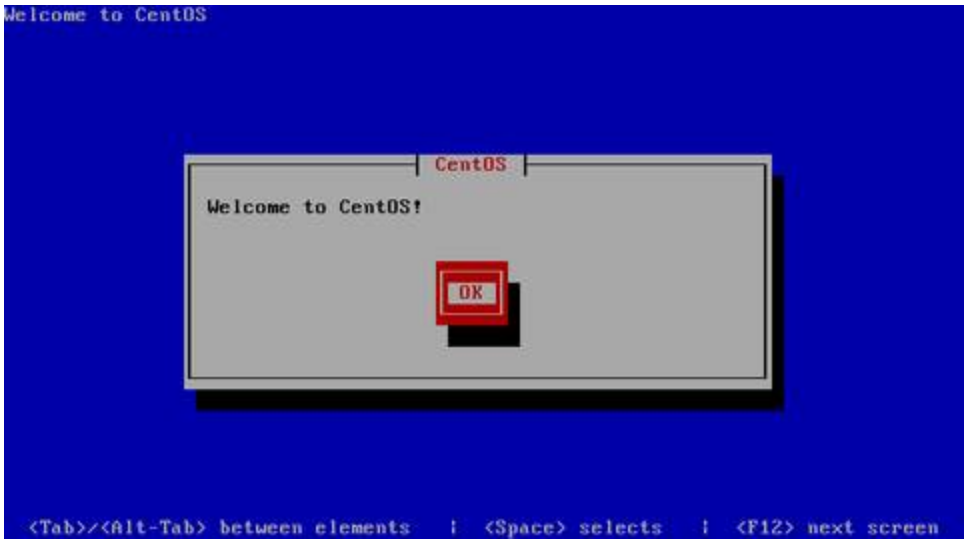
Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

5.1. Procedimientos.

Inserte el **disco DVD** de instalación de **CentOS 5** y en cuanto aparezca el diálogo de inicio (boot:), ingrese **«linux text»** para iniciar la instalación en modo texto.

Si desea verificar la integridad del disco a partir del cual se realizará la instalación, seleccione **«OK»** y pulse la tecla **ENTER**, considere que esto puede demorar varios minutos. Si está seguro de que el disco o discos a partir de los cuales se realizará la instalación están en buen estado, seleccione **«Skip»** y pulse la tecla **ENTER**.

Pulse la tecla **ENTER** en la pantalla de bienvenida al programa de instalación de CentOS.



Seleccione **«Spanish»** como idioma para ser utilizado durante la instalación.

Seleccione el mapa de teclado que corresponda al dispositivo utilizado. El mapa **«es»** corresponde a la disposición del teclado Español España. El mapa **«latin-1»** corresponde a la disposición del teclado Español Latino Americano.

Si se trata de un **disco duro nuevo y/o sin particiones**, el sistema le advertirá que es necesario inicializar la unidad. Seleccione **«Si»** y pulse la tecla **ENTER** para realizar la operación.

Para crear las particiones de forma automática, lo cual puede funcionar para la mayoría de los usuarios, puede seleccionar:

- **«Remover particiones en dispositivos seleccionados y crear disposición», lo cual eliminaría cualquier partición de cualquier otro sistema operativo presente**, y creará de forma automática las particiones necesarias.
- **«Remover particiones de linux en dispositivos seleccionados y crear disposición», lo cual eliminaría cualquier partición otra instalación de Linux presente**, y creará de forma automática las particiones necesarias.
- **«Usar espacio disponible en dispositivos seleccionados y crear disposición»**, lo cual creará de forma automática las particiones necesarias en el espacio disponible.

Conviene crear una disposición que permita un mayor control. Seleccione **«Crear disposición personalizada»** y pulse la tecla **ENTER**.

Hecho lo anterior, ingresará hacia la herramienta para gestionar particiones del disco duro. Proceda a crea una nueva partición seleccionado **«Nuevo»** y pulsando la tecla **ENTER**.

Asigne 100 MB a la partición /boot, con formato **ext3** y defina ésta como partición primaria, siempre que la tabla de particiones lo permita.

Al terminar, se mostrará la tabla de particiones actualizada. Si está conforme, seleccione otra vez «**Nuevo**» y proceda a crear la siguiente partición.

Asigne a la partición / el resto del espacio disponible menos lo que tenga calculado asignar para la partición de intercambio (200% de la memoria física, o cuanto baste para 2 GB). Se recomienda asignar / como partición primaria, siempre que la tabla de particiones lo permita.

Al terminar, se mostrará la tabla de particiones actualizada. Si está conforme, seleccione otra vez **«Nuevo»** y proceda a crear la siguiente partición.

La partición para la memoria de intercambio no requiere punto de montaje. Seleccione en el campo de **«Tipo de sistema de archivos»** la opción **«swap»**, asigne el 200% de la memoria física (o cuanto basta para 2 GB). Por tratarse de la última partición de la tabla, es buena idea asignarle el espacio por rango.

Otras particiones que se recomienda asignar, si se dispone del espacio en disco duro suficiente, son:

/usr	Requiere al menos 1.5 GB en instalaciones básicas. Debe considerarse el sustento lógico a utilizar a futuro. Para uso general, se recomiendan no menos de 5 GB y, de ser posible, considere un tamaño óptimo de hasta 8 GB en instalaciones promedio.
/tmp	Requiere al menos 350 MB y puede asignarse hasta 2 GB o más dependiendo de la carga de trabajo y tipo de aplicaciones. Si por ejemplo el sistema cuenta con un grabador de DVD, será necesario asignar a /tmp el espacio suficiente para almacenar una imagen de disco DVD, es decir, al menos 4.2 GB.
/var	Requiere **al menos** 512 MB en estaciones de trabajo **sin servicios**. En servidores regularmente se le asigna **al menos la mitad del disco duro**.
/home	En estaciones de trabajo se asigna al menos la mitad del disco duro a esta partición.

Si está conforme con la tabla de particiones creada, seleccione **«ACEPTAR»** y pulse la tecla **ENTER** para saltar a la siguiente pantalla.

Seleccione que se utilizará el gestor de arranque GRUB y pulse la tecla **ENTER** para saltar a la siguiente pantalla.

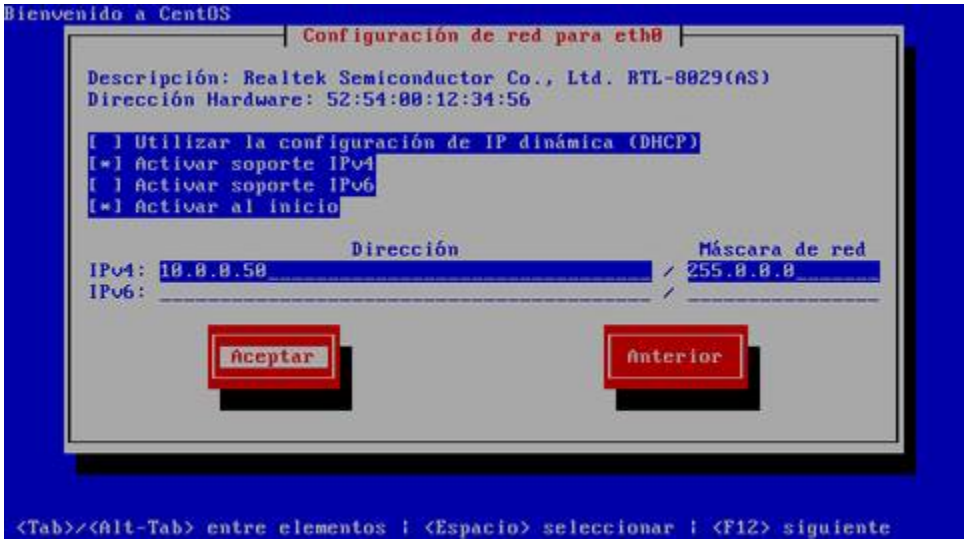
Si necesita pasar algún parámetro en particular al núcleo (kernel), como por ejemplo **acpi=off** o **nolapic** cuando hay problemas de compatibilidad de sustento físico, ingrese en el campo correspondiente aquello que sea necesario. **En la mayoría de los casos no necesitará ingresar parámetro alguno**.

Por motivos de seguridad, y principalmente con la finalidad de impedir que alguien sin autorización y con acceso físico al sistema pueda iniciar el sistema en nivel de corrida 1, o cualquiera otro, asigne, con confirmación, una clave de acceso exclusiva para el gestor de arranque. Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.

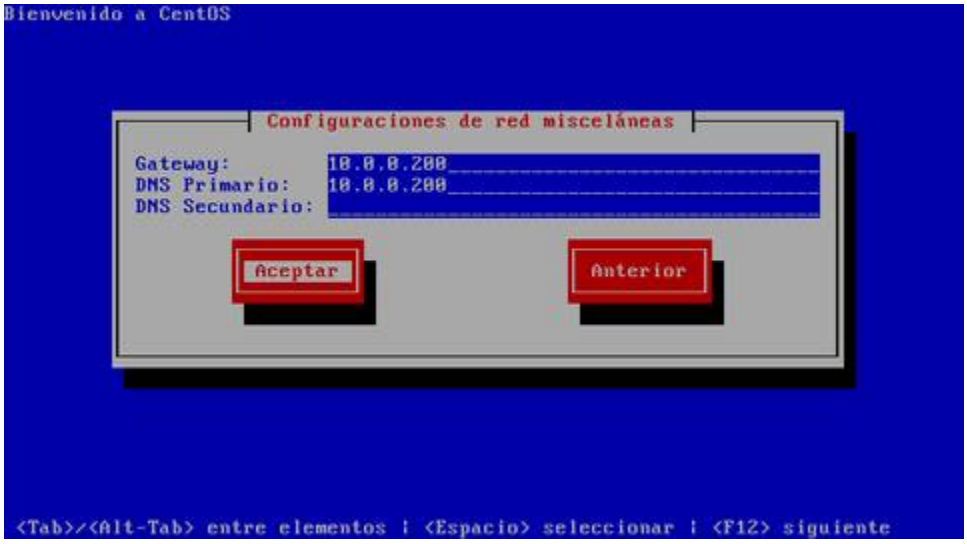
De haber otro sistema operativo instalado en el sistema, seleccione el que utilizará para iniciar de forma predeterminada. Si solo está instalando Linux, solo pulse la tecla **ENTER** para saltar a la siguiente pantalla.

Seleccione que el gestor de arranque se instale en el sector maestro del disco duro (**MBR** o **M**aster **B**oot **R**ecord). Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.

Defina la dirección IP y máscara de subred que utilizará en adelante el sistema. Confirme con el administrador de la red donde se localice que estos datos sean correctos antes de continuar. Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.



Defina la dirección IP de la puerta de enlace y las direcciones IP de los servidores DNS de los que disponga. Al terminar, pulse la tecla **ENTER** para pasar a la siguiente pantalla.

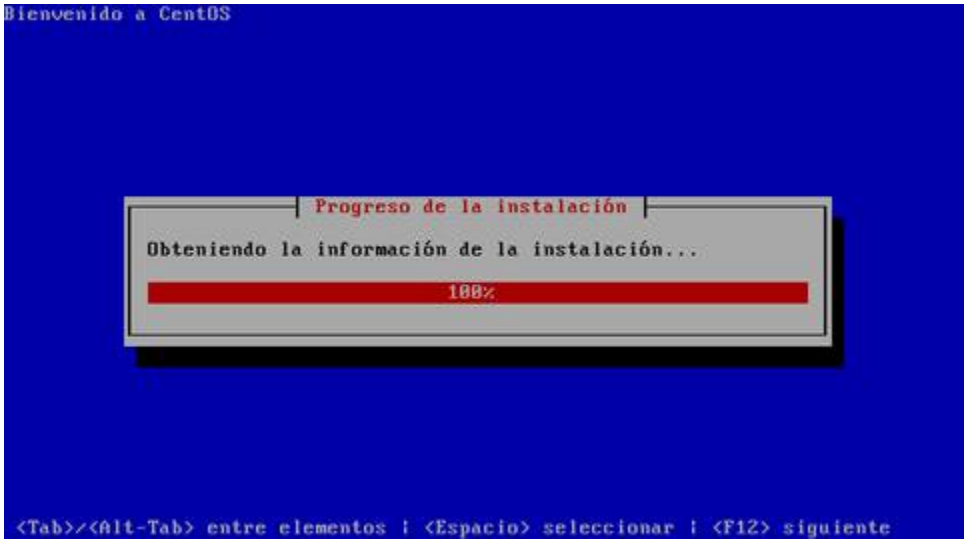


Asigne un nombre de anfitrión (HOSTNAME) para el sistema. Se recomienda que dicho nombre sea un **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) resuelto al menos en un DNS local. Si desconoce que dato ingresar, defina éste como **localhost.localdomain**. Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.

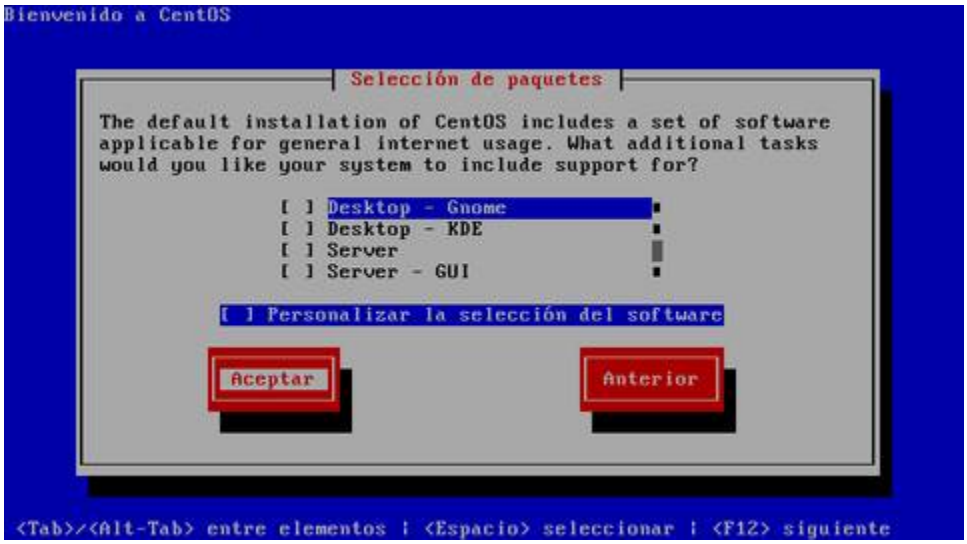
Seleccione la casilla **«System clock uses UTC»**, que significa que el reloj del sistema utilizará **UTC** (**T**iempo **U**niversal **C**oordinado), que es el sucesor de **GMT** (b>Greenwich **M**ean **T**ime, que significa Tiempo Promedio de Greenwich), y es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Pulse la tecla de tabulación una vez y seleccione la zona horaria que corresponda a la región donde se hospedará físicamente el sistema.

Asigne una clave de acceso al usuario root. Debe escribirla dos veces a fin de verificar que está coincide con lo que realmente se espera. Por razones de seguridad, se recomienda asignar una clave de acceso que evite utilizar palabras provenientes de cualquier diccionario, en cualquier idioma, así como cualquier combinación que tenga relación con datos personales.

Al terminar se realizará un calculo de la paquetería a instalar. Puede demorar algunos minutos.



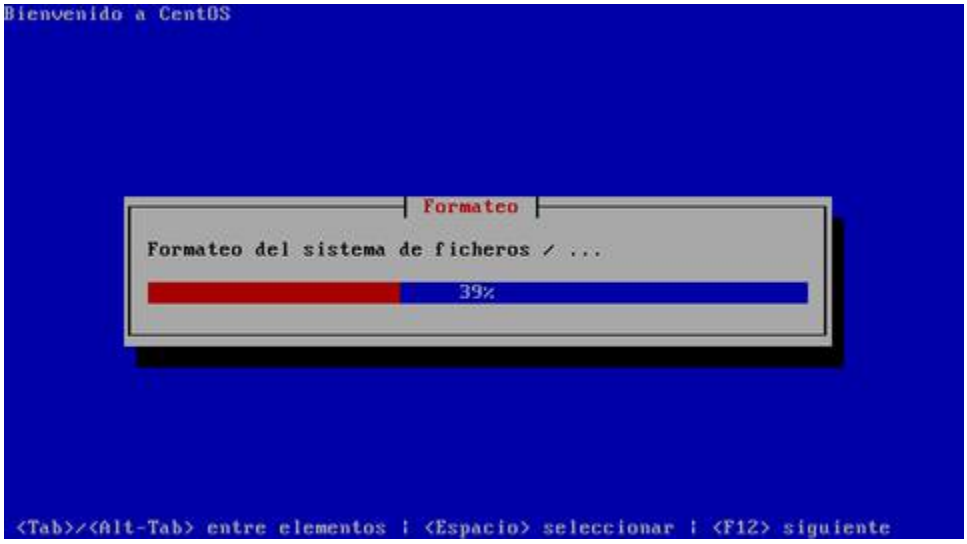
Realice una instalación con el mínimo de paquetes, desactivando todas las casillas de cada grupo de paquetes. El objeto de esto es solo instalar lo mínimo necesario para el funcionamiento del sistema operativo, y permitir instalar, posteriormente, **solo aquello que realmente se requiera** de acuerdo a la finalidad productiva que tendrá el sistema.



Al terminar se realizará un calculo de las dependencias correspondientes a la paquetería que se va a instalar. Puede demorar algunos minutos.

Antes de iniciar la instalación sobre el disco duro, el sistema le informará respecto a que se guardará un registro del proceso en si en el fichero **/root/install.log**. Solo pulse la tecla **ENTER** mientras esté seleccionado **«ACEPTAR»**.

Si iniciará de forma automática el proceso de formato de las particiones que haya creado para instalar el sistema operativo. Dependiendo de la capacidad del disco duro, este proceso puede demorar algunos minutos.



Se realizará automáticamente una copia de la imagen del programa de instalación sobre el disco duro a fin de hacer más eficiente el proceso. Dependiendo de la capacidad del microprocesador y cantidad de memoria disponible en el sistema, este proceso puede demorar algunos minutos.

Iniciará la instalación de los paquetes necesarios para el funcionamiento del sistema operativo. El proceso puede demorar varios minutos.

Se podrá supervisar el proceso de instalación de cada paquete, así como los tiempos correspondientes al tiempo total estimado del procesos, tiempo completado y tiempo restante.

Una vez concluida la instalación de los paquetes, proceda a pulsar la tecla **ENTER** para reiniciar el sistema.


Bienvenido a CentOS
Completado
Enhorabuena, su instalación de CentOS ha finalizado.
Remueva cualquier medio de instalación usado durante este proceso y pulse <Intro> para reiniciar su sistema.
Reiniciar
<Intro> para reinicializar

6. Instalación en modo gráfico de CentOS 5.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

6.1. Procedimientos.

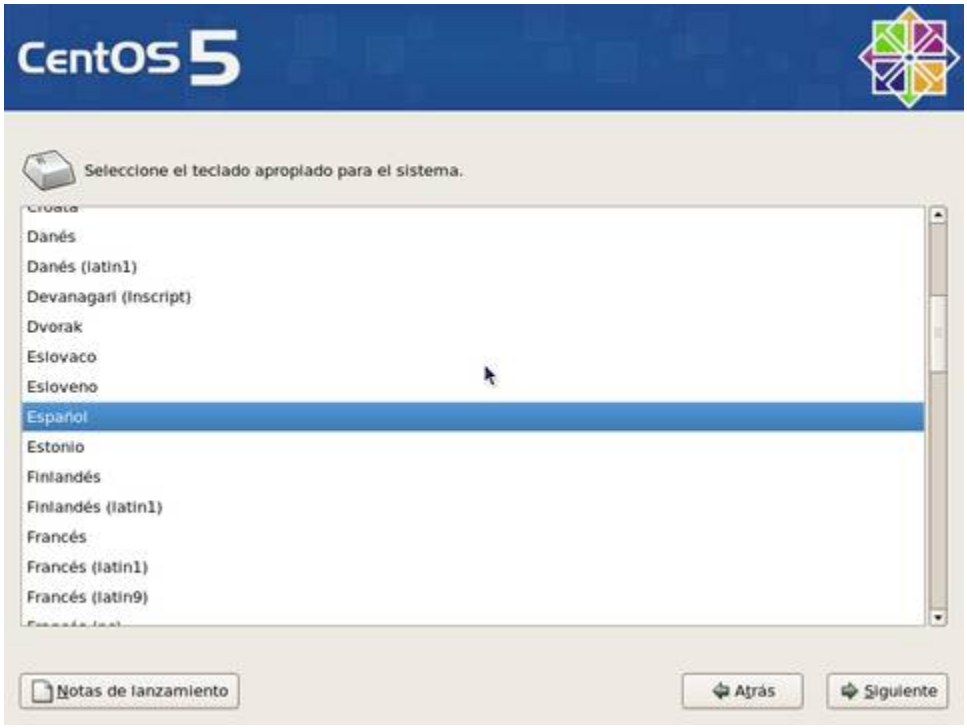
Inserte el **disco DVD** de instalación de **CentOS 5** y en cuanto aparezca el diálogo de inicio (boot:), pulse la tecla **ENTER** o bien ingrese las opciones de instalación deseadas.

Si desea verificar la integridad del disco a partir del cual se realizará la instalación, seleccione **«OK»** y pulse la tecla **ENTER**, considere que esto puede demorar varios minutos. Si está seguro de que el disco o discos a partir de los cuales se realizará la instalación están en buen estado, seleccione **«Skip»** y pulse la tecla **ENTER**.

Haga clic sobre el botón **«Next»** en cuanto aparezca la pantalla de bienvenida de CentOS.

Seleccione **«Spanish»** como idioma para ser utilizado durante la instalación.

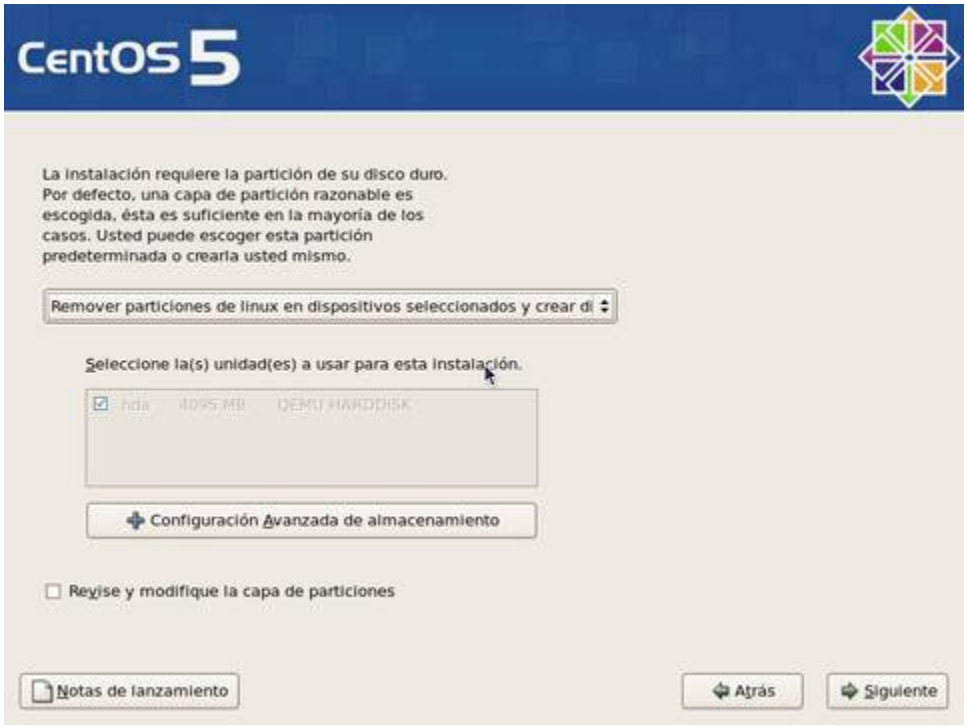
Seleccione el mapa de teclado que corresponda al dispositivo utilizado. El mapa **«Español»** o bien **«Latinoamericano»** de acuerdo a lo que corresponda. Al terminar, haga clic sobre el botón **«Siguiente»**.



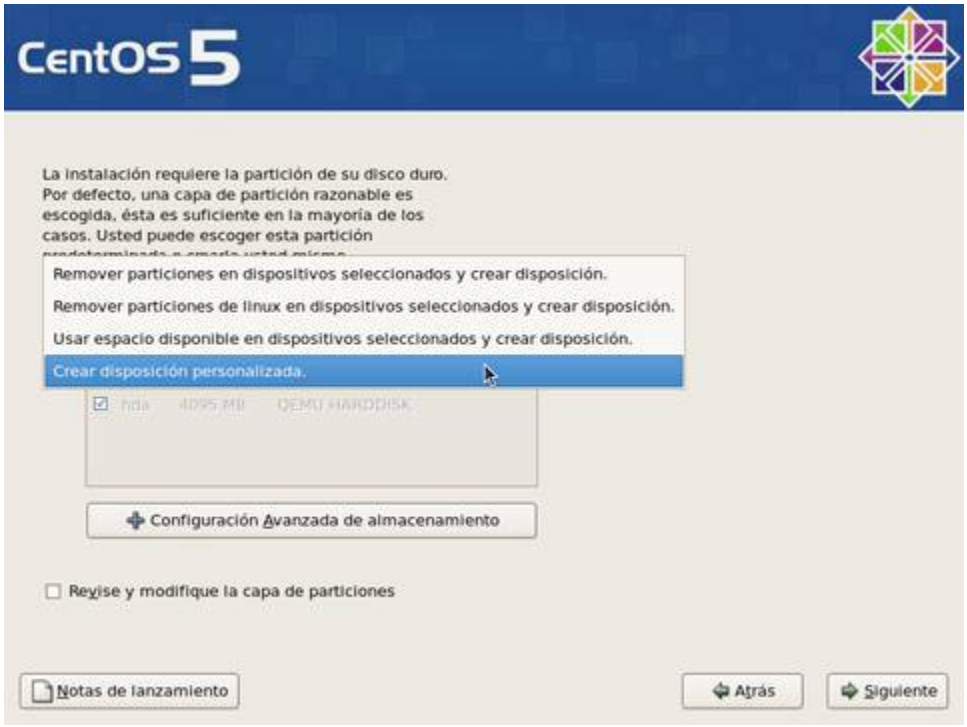
Salvo que exista una instalación previa que se desee actualizar (no recomendado), deje seleccionado **«Instalar CentOS»** y haga clic en el botón **«Siguiente»** a fin de realizar una instalación nueva.

Para crear las particiones de forma automática, lo cual puede funcionar para la mayoría de los usuarios, puede seleccionar:

- **«Remover particiones en dispositivos seleccionados y crear disposición», lo cual eliminaría cualquier partición de cualquier otro sistema operativo presente**, y creará de forma automática las particiones necesarias.
- **«Remover particiones de linux en dispositivos seleccionados y crear disposición», lo cual eliminaría cualquier partición otra instalación de Linux presente**, y creará de forma automática las particiones necesarias.
- **«Usar espacio disponible en dispositivos seleccionados y crear disposición»**, lo cual creará de forma automática las particiones necesarias en el espacio disponible.

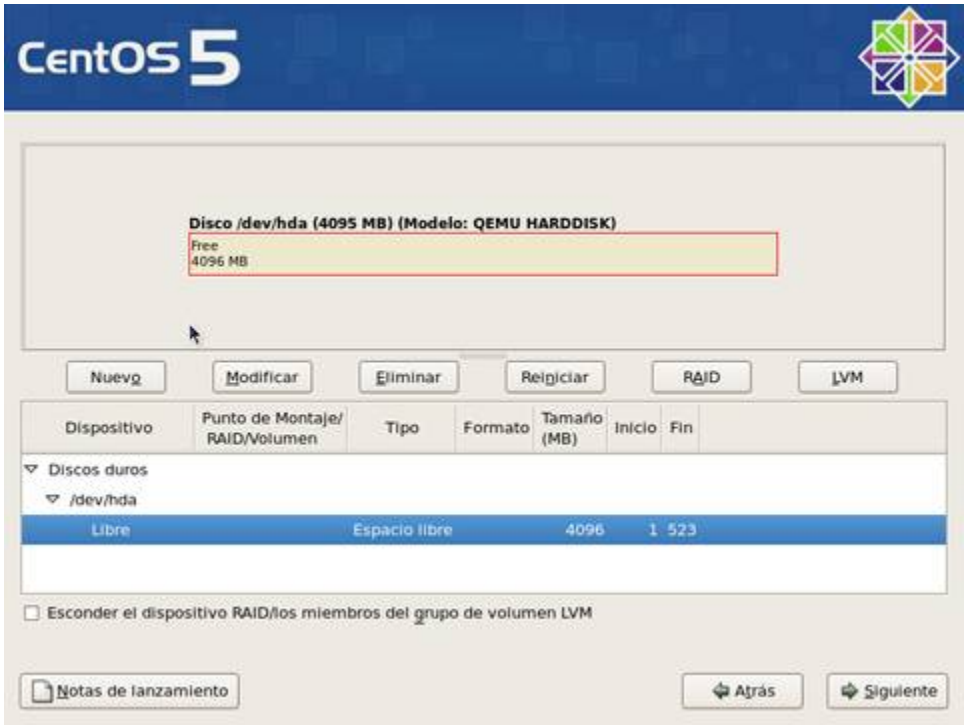


Conviene crear una disposición que permita un mayor control. Seleccione **«Crear disposición personalizada»**.

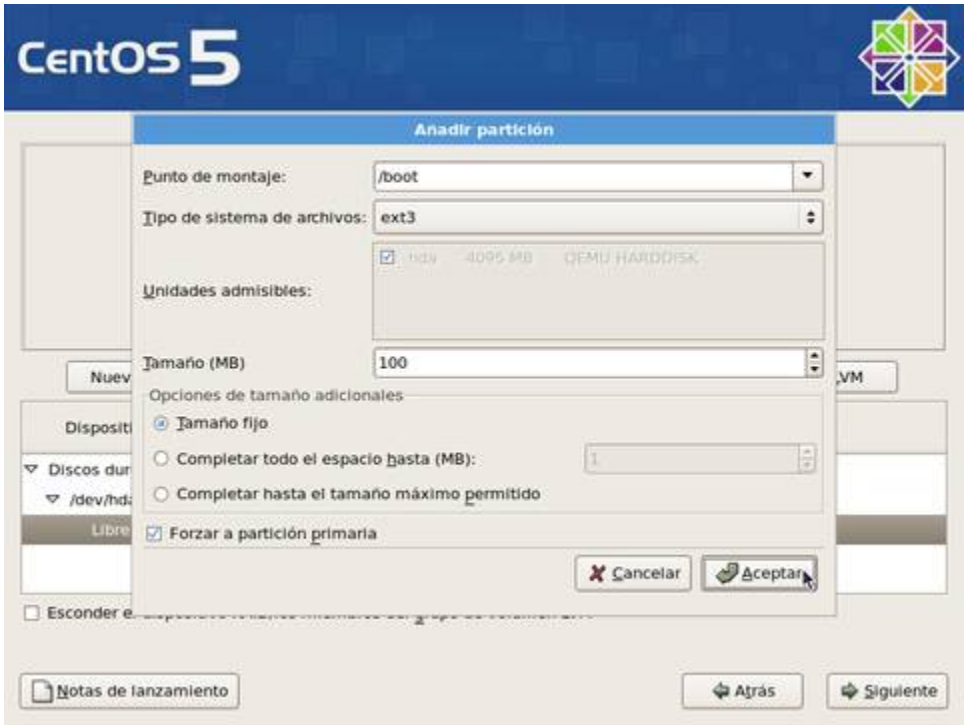


Una vez seleccionado **«Crear disposición personalizada»**, haga clic sobre el botón **«Siguiente»**.

La herramienta de particiones mostrará el espacio disponible. Haga clic en el botón «**Nuevo**».



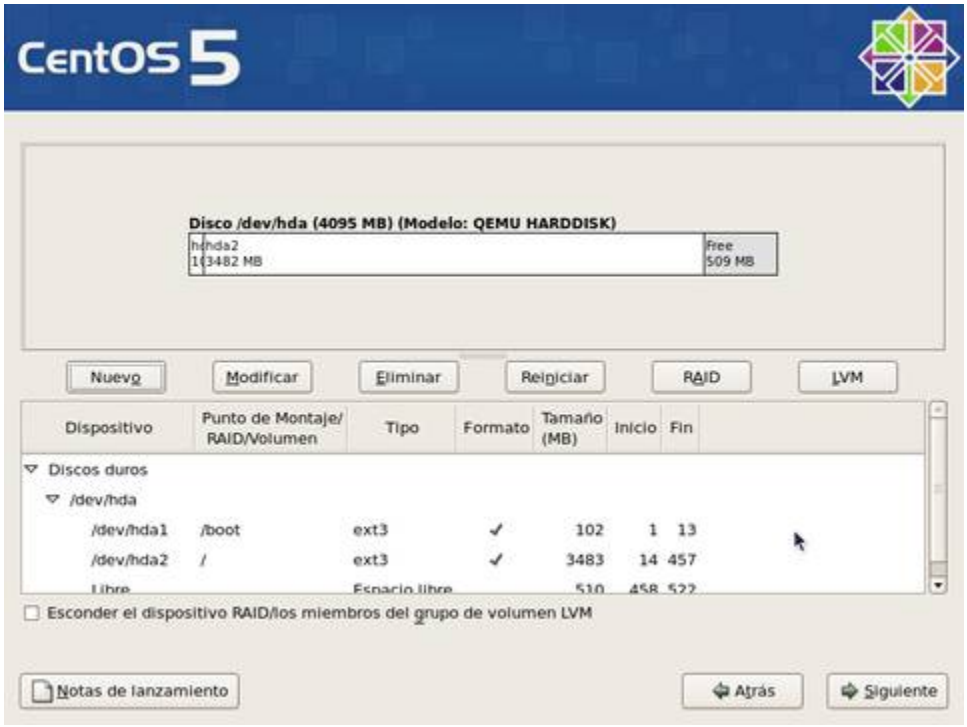
Asigne 100 MB a la partición /boot y defina ésta como partición primaria, siempre que la tabla de particiones lo permita.



Si está conforme, haga clic otra vez en el botón **«Nuevo»** y proceda a crear la siguiente partición.

Asigne a la partición / el resto del espacio disponible menos lo que tenga calculado asignar para la partición de intercambio (200% de la memoria física, o cuanto baste para 2 GB). Se recomienda asignar / como partición primaria, siempre que la tabla de particiones lo permita.

Si está conforme, haga clic otra vez en el botón **«Nuevo»** y proceda a crear la siguiente partición.

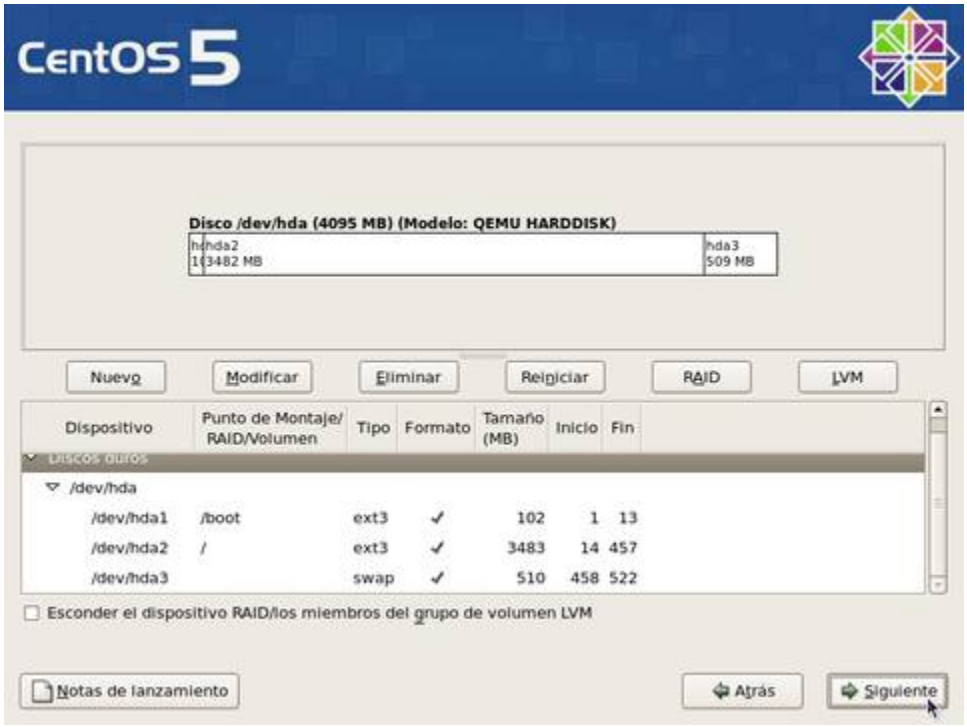


La partición para la memoria de intercambio no requiere punto de montaje. Seleccione en el campo de **«Tipo de sistema de archivos»** la opción **«swap»**, asigne el 200% de la memoria física (o cuanto basta para 2 GB). Por tratarse de la última partición de la tabla, es buena idea asignarle el espacio por rango, especificando valores ligeramente por debajo y ligeramente por arriba de lo planeado.

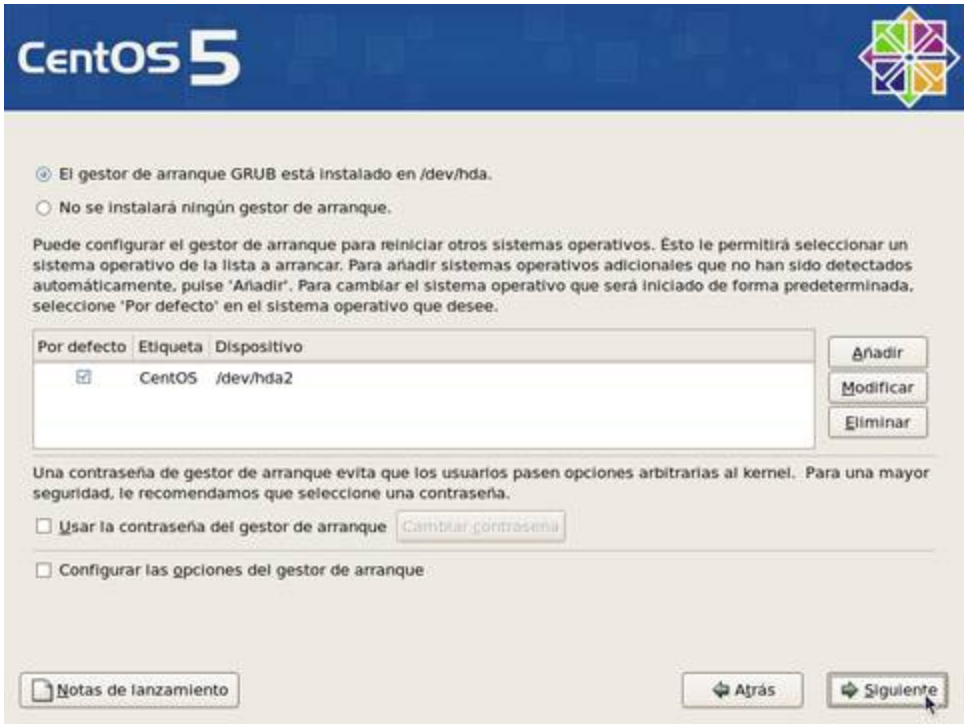
Otras particiones que se recomienda asignar, si se dispone del espacio en disco duro suficiente, son:

`/usr`	Requiere al menos 1.5 GB en instalaciones básicas. Debe considerarse el sustento lógico a utilizar a futuro. Para uso general, se recomiendan no menos de 5 GB y, de ser posible, considere un tamaño óptimo de hasta 8 GB en instalaciones promedio.
`/tmp`	Requiere al menos 350 MB y puede asignarse hasta 2 GB o más dependiendo de la carga de trabajo y tipo de aplicaciones. Si por ejemplo el sistema cuenta con un grabador de DVD, será necesario asignar a /tmp el espacio suficiente para almacenar una imagen de disco DVD, es decir, al menos 4.2 GB.
`/var`	Requiere **al menos** 512 MB en estaciones de trabajo **sin servicios**. En servidores regularmente se le asigna **al menos la mitad del disco duro**.
`/home`	En estaciones de trabajo se asigna al menos la mitad del disco duro a esta partición.

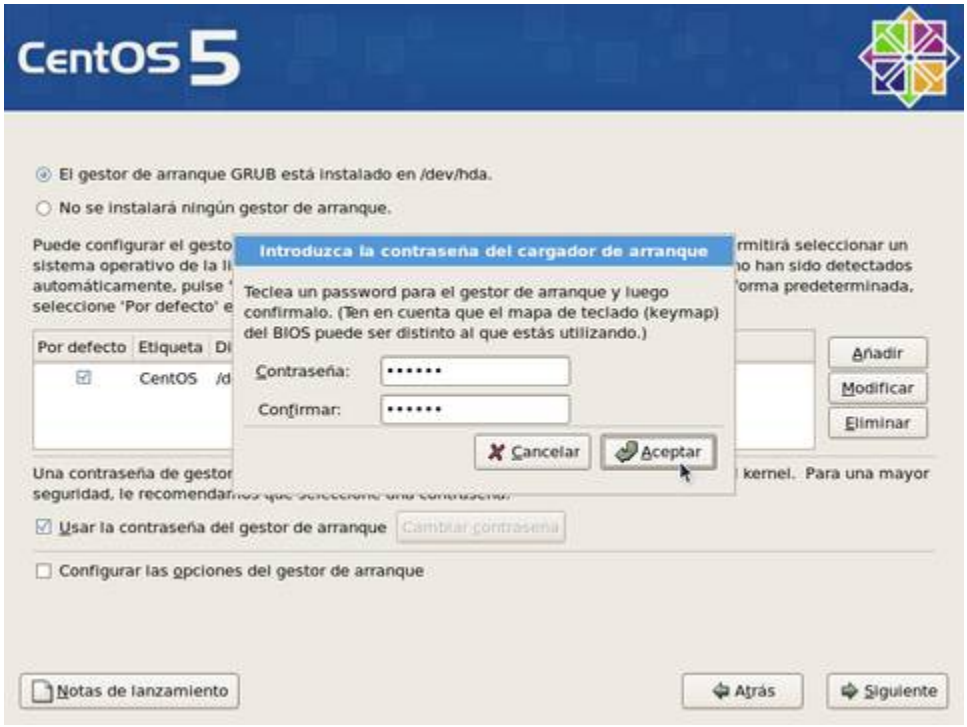
Si está conforme con la tabla de particiones creada, haga clic sobre el botón **«siguiente»** para pasar a la siguiente pantalla.



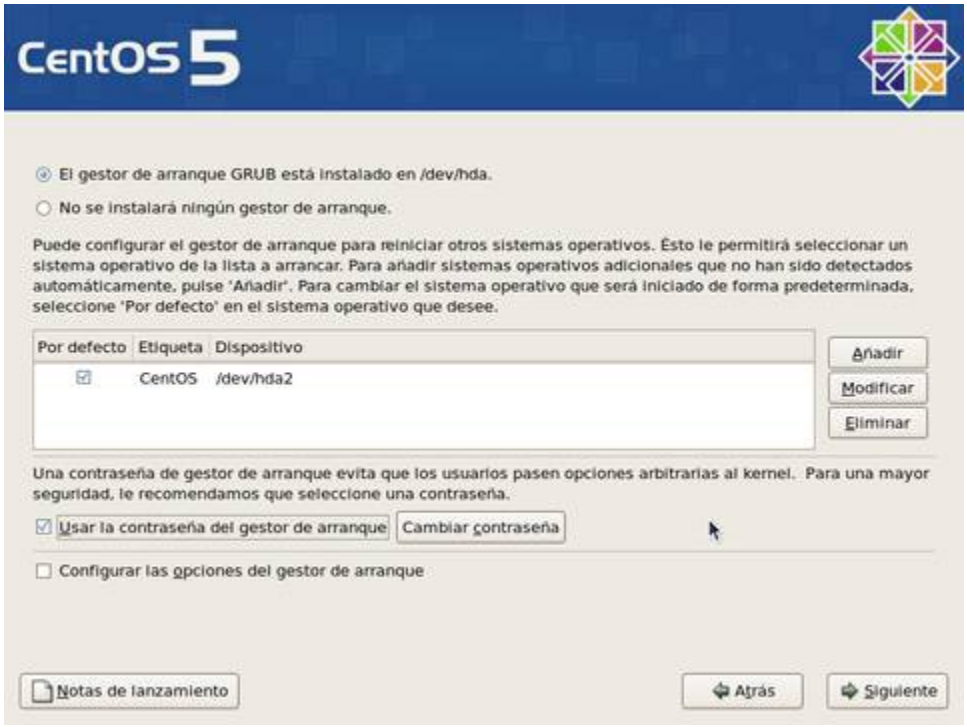
Ingresará a la configuración del gestor de arranque. Por motivos de seguridad, y principalmente con la finalidad de impedir que alguien sin autorización y con acceso físico al sistema pueda iniciar el sistema en nivel de corrida 1, o cualquiera otro, haga clic en la casilla **«Usar la contraseña del gestor de arranque»**.



Se abrirá una ventana emergente donde deberá ingresar, con confirmación, la clave de acceso exclusiva para el gestor de arranque. Al terminar, haga clic sobre el botón **«Aceptar»**.



Al terminar, haga clic sobre el botón **«Siguiente»**.



Para configurar los parámetros de red del sistema, haga clic sobre el botón **«Modificar»** para la interfaz eth0.

En la ventana emergente para modificar la interfaz eth0, desactive la casilla **«Configurar usando DHCP»** y especifique la dirección IP y máscara de subred que utilizará en adelante el sistema. Si no va a utilizar IPv6, también desactive la casilla. Confirme con el administrador de la red donde se localice que estos datos sean correctos antes de continuar. Al terminar, haga clic sobre el botón **«Aceptar»**.

Asigne un nombre de anfitrión (HOSTNAME) para el sistema. Se recomienda que dicho nombre sea un **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) resuelto al menos en un DNS local. Defina, además, en esta misma pantalla, la dirección IP de la puerta de enlace y las direcciones IP de los servidores DNS

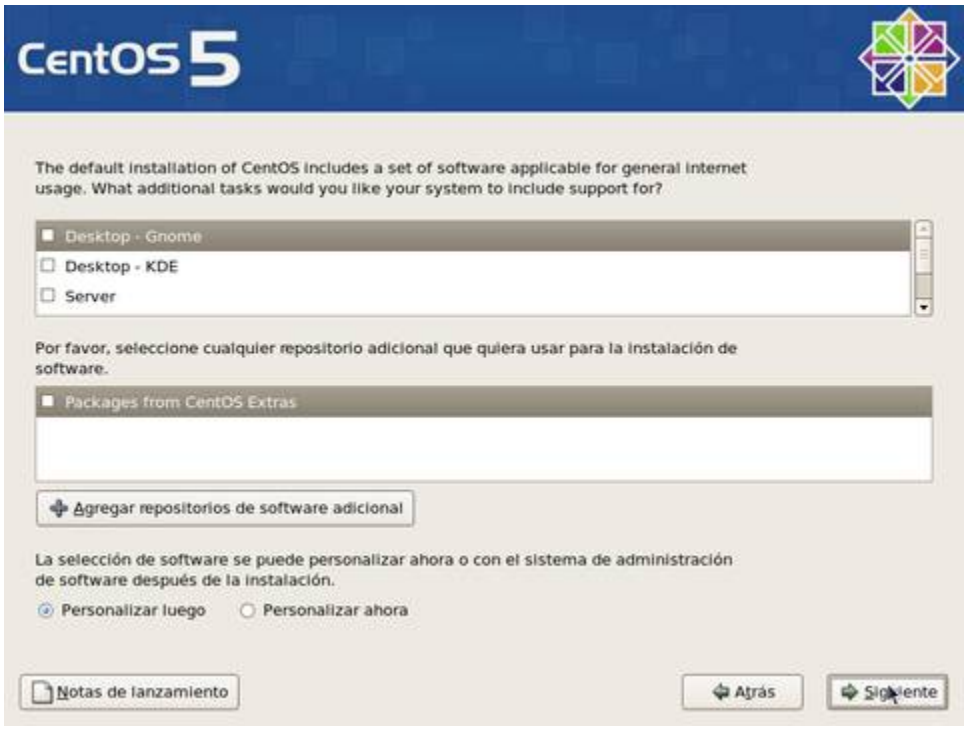
de los que disponga. Si desconoce que dato ingresar, defina éste como **localhost.localdomain**. Al terminar, haga clic sobre el botón **«Siguiente»**.

Seleccione la casilla **«El sistema horario usará UTC»**, que significa que el reloj del sistema utilizará **UTC** (**T**iempo **U**niversal **C**oordinado), que es el sucesor de **GMT** (b>Greenwich **M**ean **T**ime, que significa Tiempo Promedio de Greenwich), y es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Haga clic con el ratón sobre la región que corresponda en el mapa mundial o seleccione en el siguiente campo la zona horaria que corresponda a la región donde se hospedará físicamente el sistema.

Asigne una clave de acceso al usuario **root**. Debe escribirla dos veces a fin de verificar que está coincide con lo que realmente se espera. Por razones de seguridad, se recomienda asignar una clave de acceso que evite utilizar palabras provenientes de cualquier diccionario, en cualquier idioma, así como cualquier combinación que tenga relación con datos personales.

Al terminar, haga clic sobre el botón «**Siguiente**», y espere a que el sistema haga la lectura de información de los grupos de paquetes.

En la siguiente pantalla podrá seleccionar los grupos de paquetes que quiera instalar en el sistema. Añada o elimine a su conveniencia. Lo recomendado, sobre todo si se trata de un servidor, es realizar una instalación con el mínimo de paquetes, desactivando todas las casillas para todos los grupos de paquetes. El objeto de esto es solo instalar lo mínimo necesario para el funcionamiento del sistema operativo, y permitir instalar posteriormente solo aquello que realmente se requiera de acuerdo a la finalidad productiva que tendrá el sistema. Al terminar, haga clic sobre el botón **«Siguiente»**.



Se realizará una comprobación de dependencias de los paquetes a instalar. Este procesos puede demorar algunos minutos.

Antes de iniciar la instalación sobre el disco duro, el sistema le informará respecto a que se guardará un registro del proceso en si en el fichero **/root/install.log**. Para continuar, haga clic sobre el botón **«Siguiente»**.

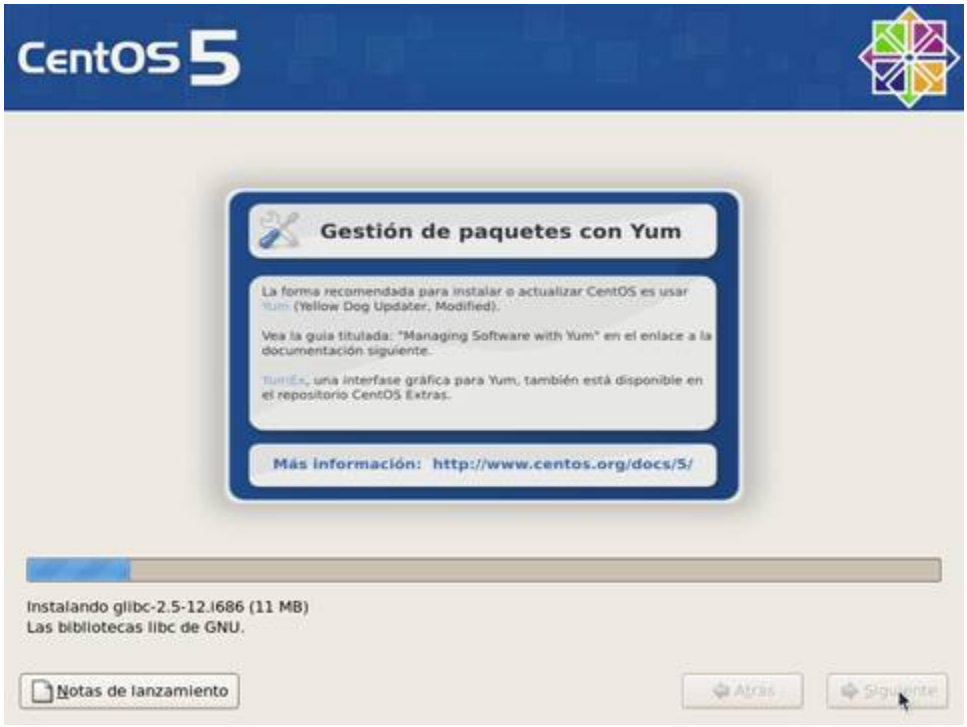
Si iniciará de forma automática el proceso de formato de las particiones que haya creado para instalar el sistema operativo. Dependiendo de la capacidad del disco duro, este proceso puede demorar algunos minutos.

Se realizará automáticamente una copia de la imagen del programa de instalación sobre el disco duro a fin de hacer más eficiente el proceso. Dependiendo de la capacidad del microprocesador y cantidad de memoria disponible en el sistema, este proceso puede demorar algunos minutos.

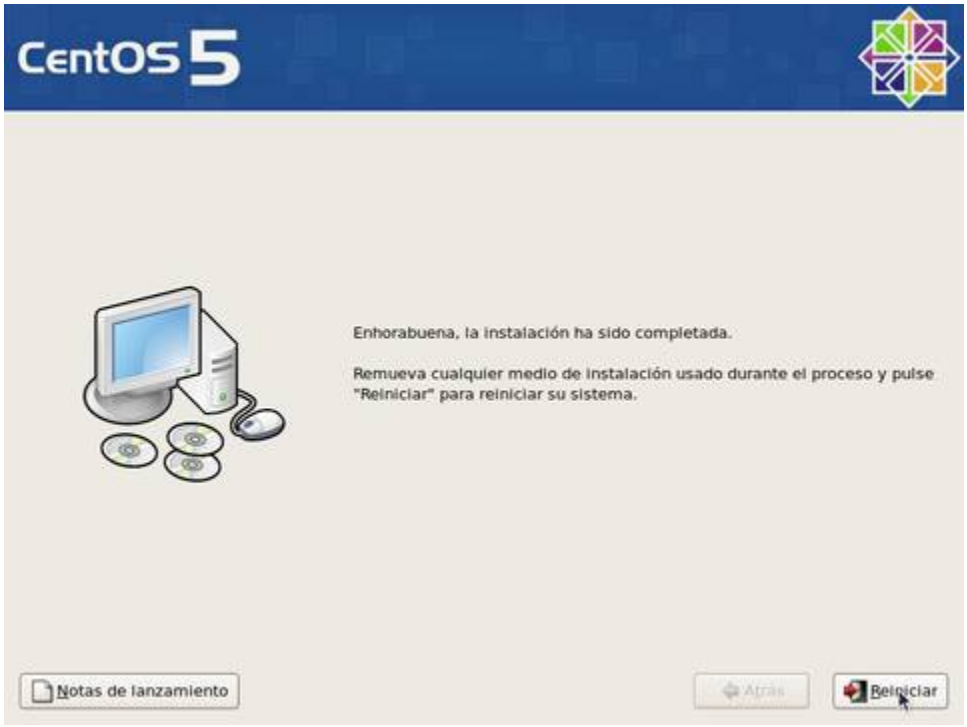
Espere a que se terminen los preparativos de inicio del proceso de instalación.

Se realizarán preparativos para realizar las transacciones de instalación de paquetes.

Iniciará la instalación de los paquetes necesarios para el funcionamiento del sistema operativo. Espere algunos minutos hasta que concluya el proceso.



Una vez concluida la instalación de los paquetes, haga clic sobre el botón «**Reiniciar**».



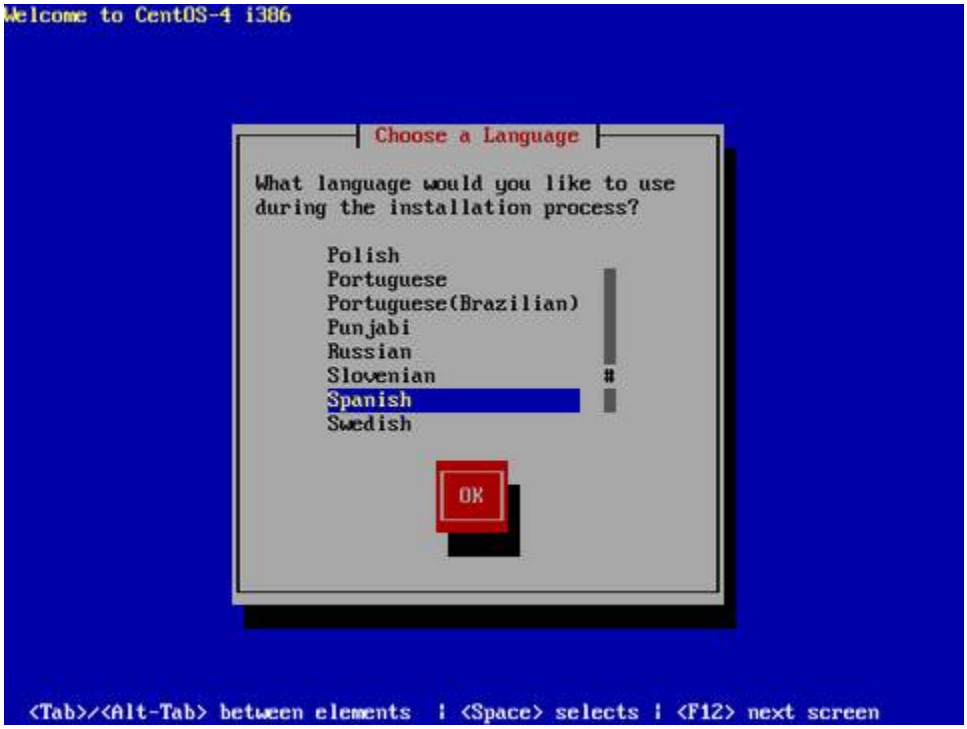
7. Cómo iniciar el modo de rescate en CentOS 4.

utor: Joel Barrios Dueñas
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

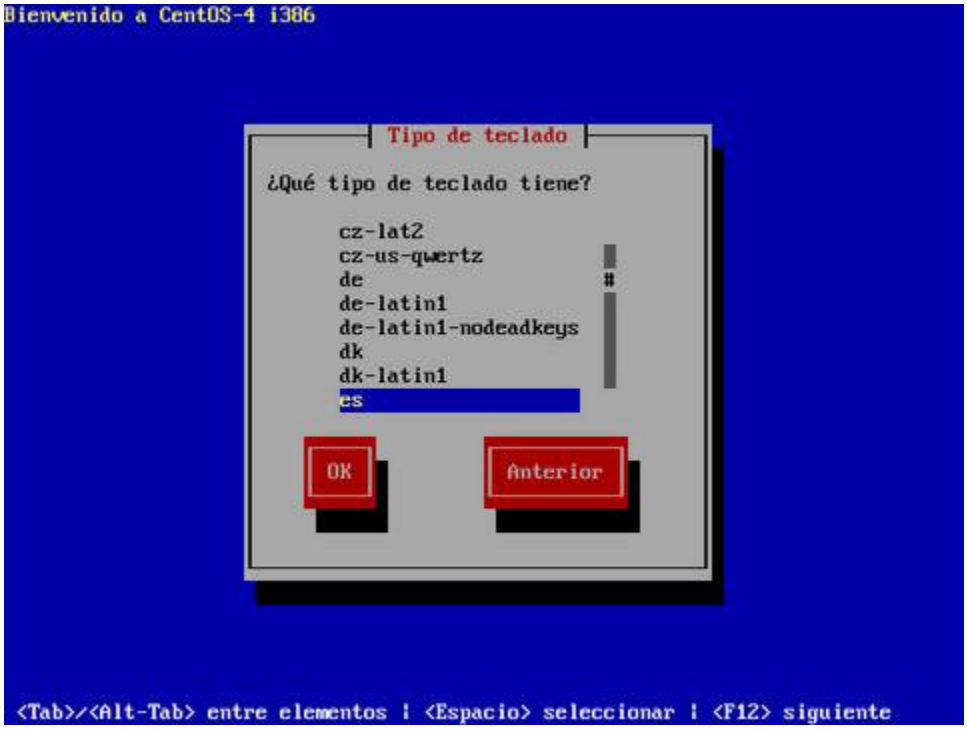
7.1. Procedimientos.

Inserte el disco de instalación de CentOS y en cuanto aparezca el diálogo de inicio (boot:), ingrese **linux rescue** para dar comienzo al modo de rescate.

En cuanto inicie el programa, elija **«Spanish»** (español) como el idioma a utilizar.

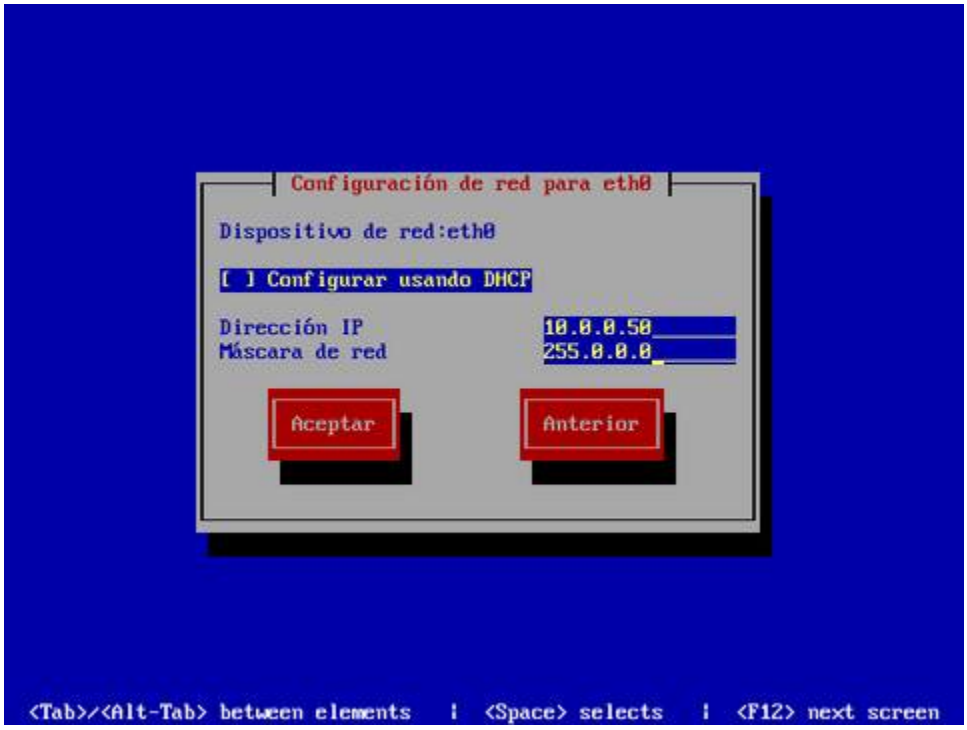


Seleccione el mapa de teclado que corresponda al dispositivo utilizado. El mapa **«es»** corresponde a la disposición del teclado Español España. El mapa **«latin-1»** corresponde a la disposición del teclado Español Latino Americano.

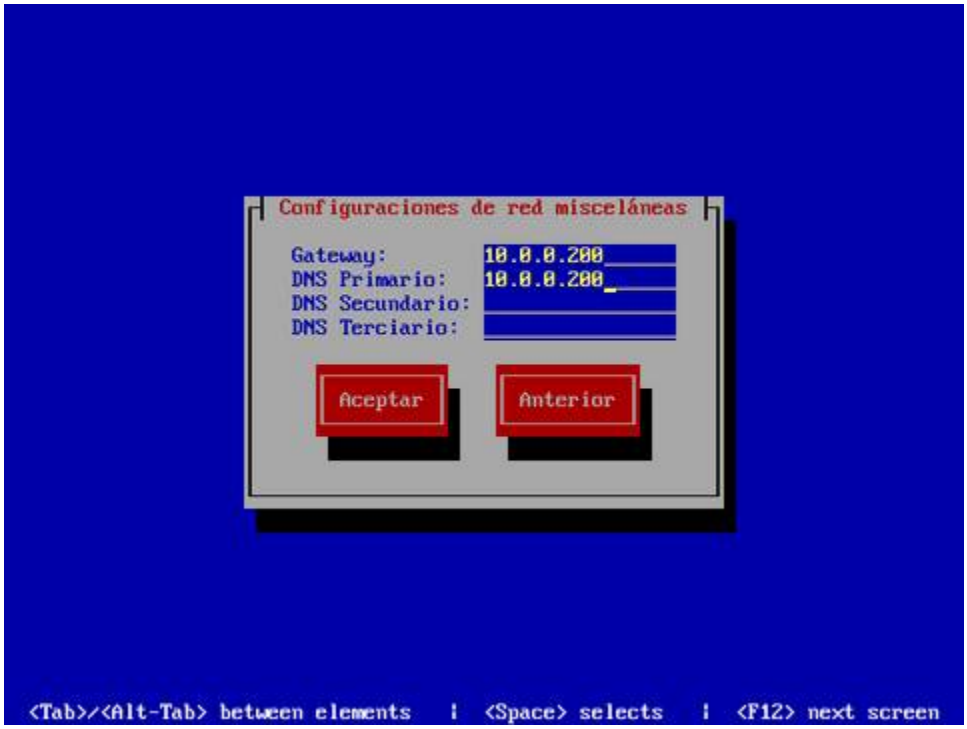


El programa preguntará si desea activar las tarjetas de red presentes en el sistema. Responda que **si**. Resulta muy conveniente, para algunas tareas de mantenimiento y reparaciones, contar con conectividad.

Defina la dirección **IP** y máscara de subred que utilizará en adelante el sistema. Confirme con el administrador de la red donde se localice que estos datos sean correctos antes de continuar. Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.



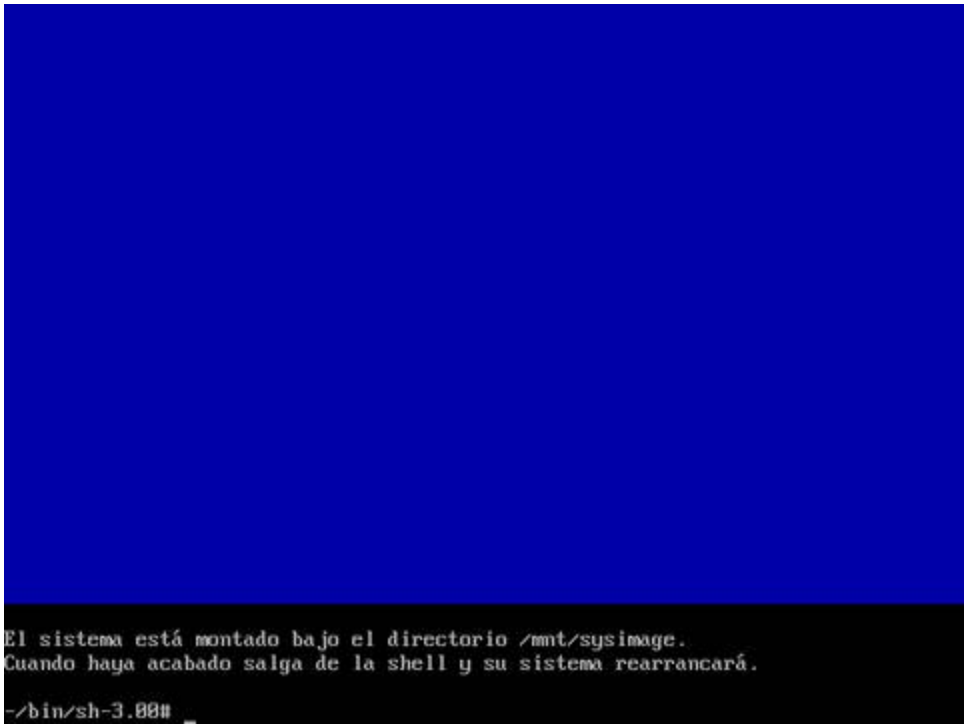
Defina la dirección **IP** de la puerta de enlace y las direcciones IP de los servidores **DNS** de los que disponga. Al terminar, pulse la tecla **ENTER** para saltar a la siguiente pantalla.



Puede elegir **Continuar** para montar el sistema en modo de lectura y escritura, para realizar tareas administrativas y modificaciones en configuraciones, o bien en modo de **Solo Lectura**, para realizar verificación y reparación de sistema de ficheros.

Una vez hecha la elección, el sistema le indicará que el sistema se ha montado bajo **/mnt/sysimage** y que si desea que éste sistema de ficheros sea el entorno de **root**, solo deberá utilizar **chroot /mnt/sysimage**. Solo pulse la tecla **ENTER** para salir al intérprete de mandatos.

Desde el intérprete de mandatos se pueden realizar tareas administrativas y correctivas, dependiendo de la situación y las condiciones. Utilice **chroot /mnt/sysimage** para cambiar el entorno de root hacia el sistema de ficheros en disco duro, o bien utilice herramientas, como **fsck**, para realizar otras operaciones.



8. Iniciando el sistema en nivel de corrida 1 (nivel mono-usuario).

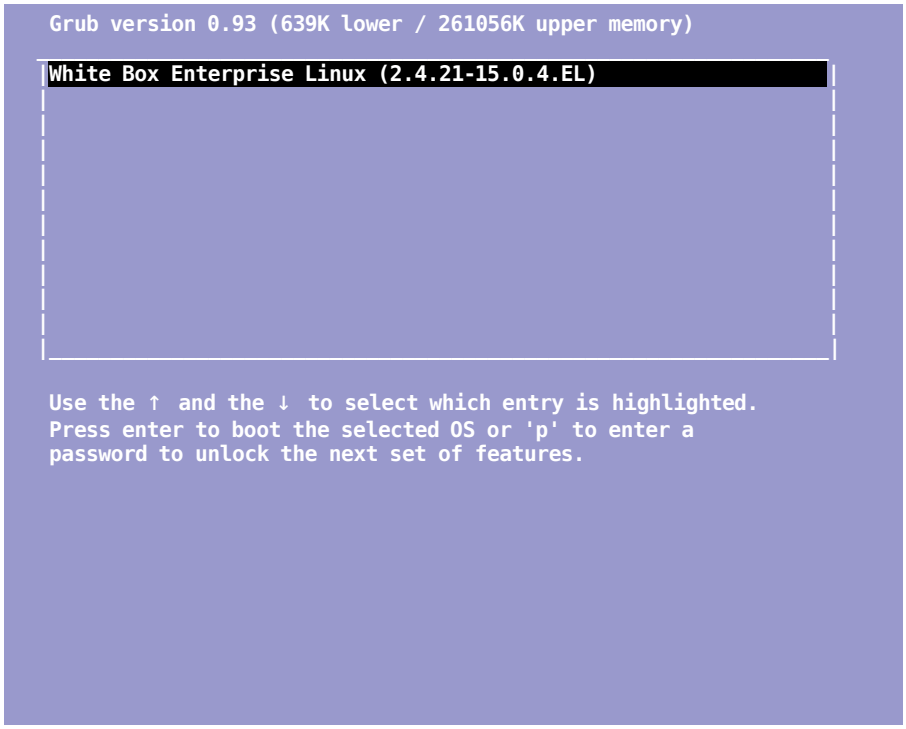
Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

8.1. Introducción.

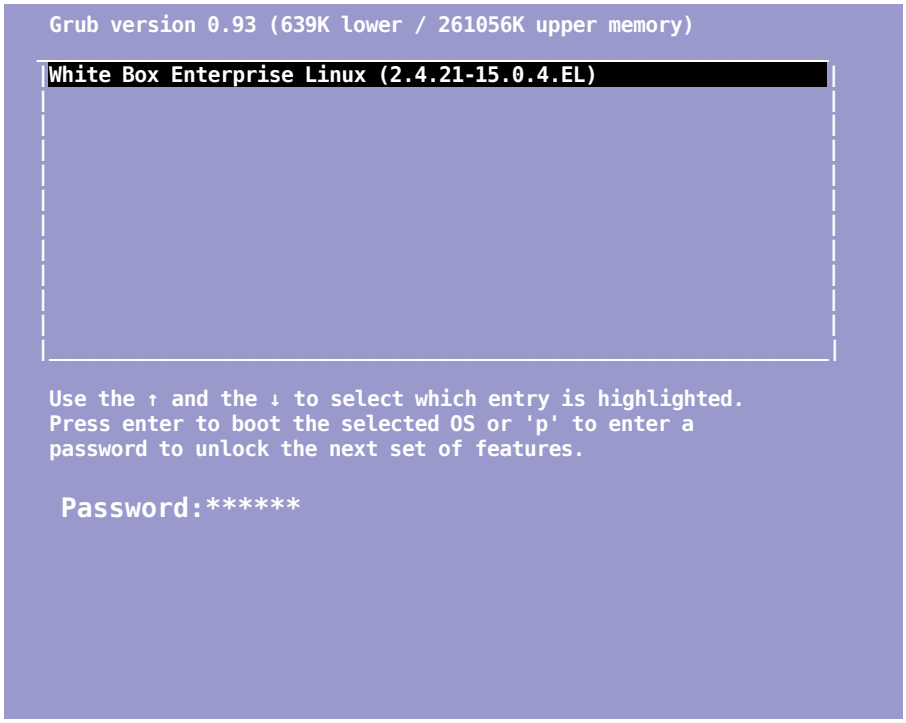
Existen situaciones en las cuales se puede requerir el inicio del sistema en nivel de corrida 1 o nivel mono-usuario a fin de realizar tareas de mantenimiento o, en su defecto, reparaciones.

8.2. Procedimientos.

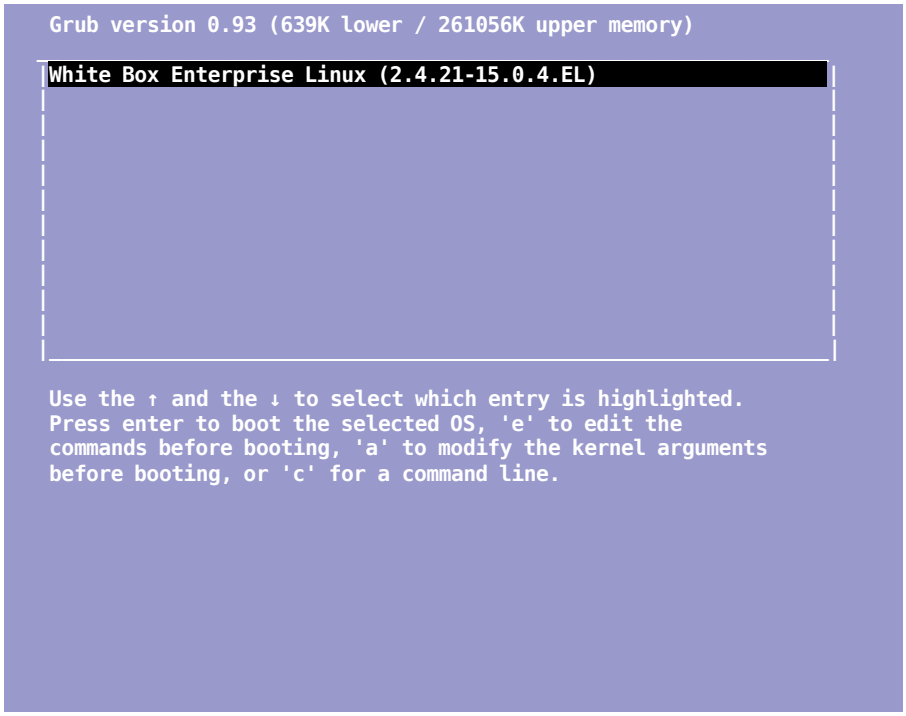
Al iniciar el sistema, éste lo hará presentando la pantalla del gestor de arranque conocido como Grub presentando una pantalla similar a la siguiente:



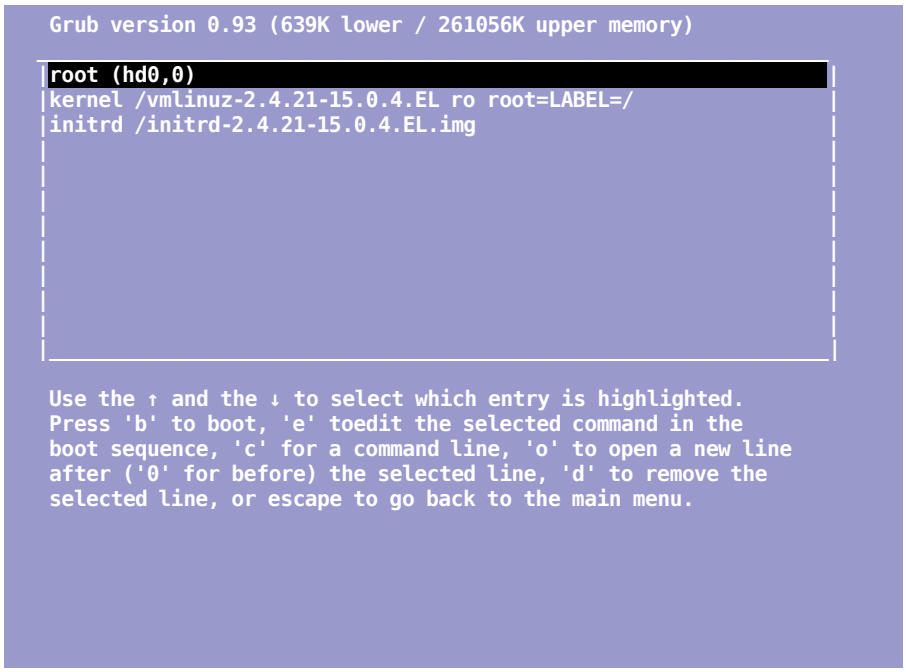
Pulse la tecla 'p' e ingrese la clave de acceso definida desde el programa de instalación del sistema operativo:



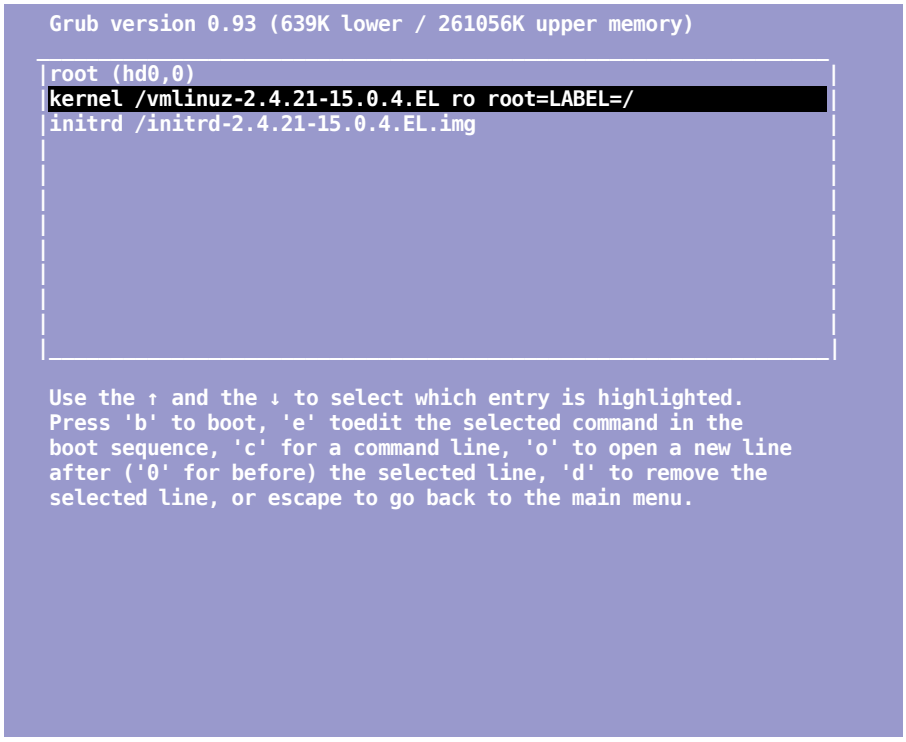
El texto de opciones cambiará después de ingresar la clave de acceso correcta:



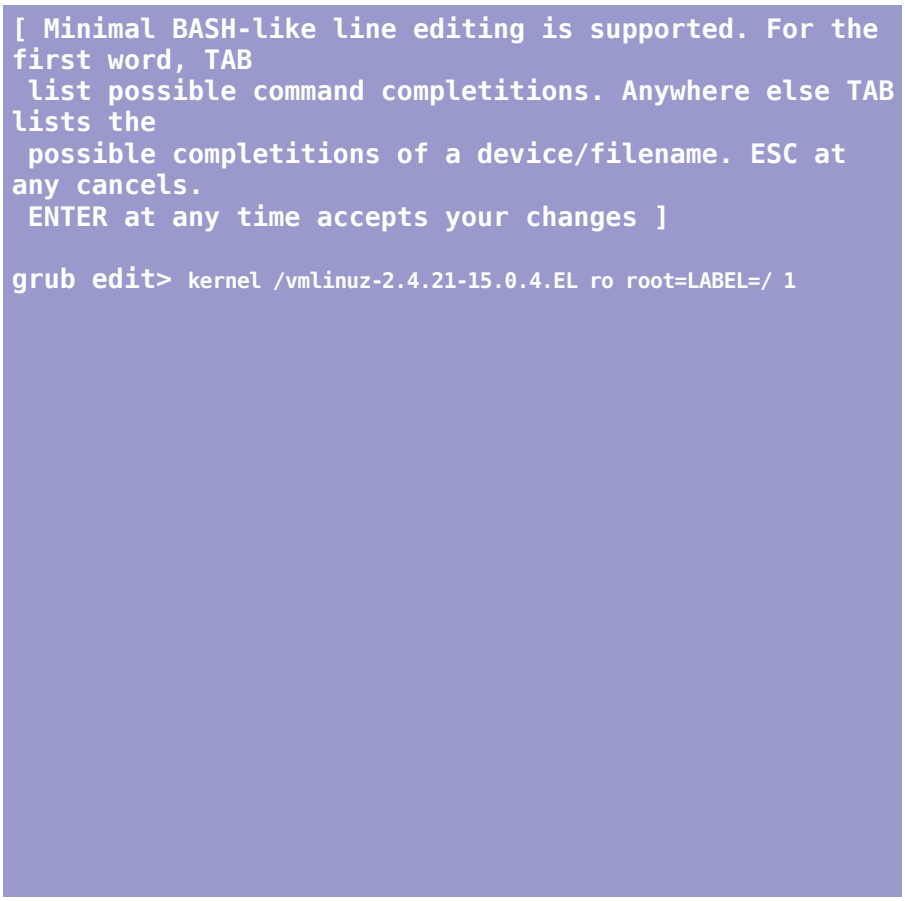
Pulse la tecla 'e' para modificar las opciones de arranque del núcleo seleccionado:



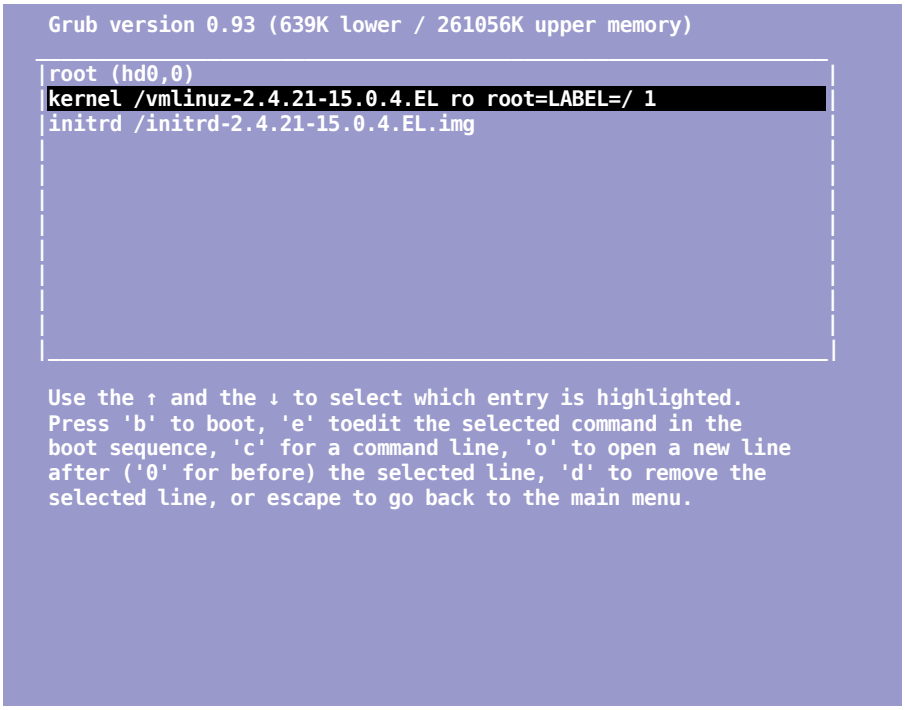
Seleccione la línea referente al núcleo y vuelva a pulsar la tecla 'e' a fin de modificar dicha línea:



Agregue un espacio y un número 1 al final de la línea y pulse la tecla ENTER



Regresará a la pantalla anterior. Simplemente pulse la tecla 'b' para iniciar el sistema en nivel de corrida 1:



9. Procedimientos de emergencia

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

9.1. Introducción

En ocasiones suele ser necesario realizar tareas de mantenimiento y de reparación en el sistema de archivos. Estas situaciones requieren que el administrador conozca al menos las herramientas correspondientes.

9.2. Disco de rescate

El primer disco de instalación de Red Hat™ Enterprise Linux 3 y White Box Enterprise Linux 3 incluye la opción de iniciar el sistema en modo de rescate desde éste. Solo bastará digitar «linux rescue» en el aviso de inicio (prompt) que aparece al arrancar el sistema con el disco 1:

```
boot: linux rescue
```

Después de iniciar, configurar el teclado y, de forma opcional, la conectividad a través de dispositivos de red, se ingresará a un interprete de mandatos (BASH) con un conjunto básico de herramientas que permitirán realizar tareas de mantenimiento y reparación.

Digite lo siguiente a fin de mostrar en pantalla las particiones del sistema:

```
df -h
```

Lo anterior deberá mostrar algo parecido a lo siguiente:

```
S.ficheros          Tamaño Usado  Disp Uso% Montado en
/dev/sda2              15G  4.8G  9.2G  34% /
/dev/sda1              76M  8.1M   64M  12% /boot
none                  507M     0  507M   0% /dev/shm
/dev/hda5              40G   35G  2.6G  94% /home
/dev/sdb3             2.0G   36M  1.9G   2% /tmp
/dev/sdb1             6.4G  4.0G  2.2G  66% /usr/local
/dev/sdb5             6.4G  4.3G  1.8G  71% /usr/src
/dev/sdb2             2.0G  570M  1.4G  30% /var
/dev/hda6              19G   17G  998M  95% /var/ftp
/dev/hda2             6.0G  257M  5.4G   5% /var/lib
/dev/hda1             6.9G  792M  5.8G  12% /var/www
```

9.3. Verificación de la integridad del disco

La verificación de cualquier partición del disco duro requiere, necesariamente, desmontar antes ésta. Una vez hecho esto es posible realizar una verificación utilizando lo siguiente, considerando en el ejemplo que se intenta verificar la partición **/dev/hda1**:

```
fsck -fy /dev/hda1
```

De ser necesaria una verificación de superficie en busca de sectores dañados, **considerando que dicho proceso puede demorar incluso varias horas**, se puede utilizar lo siguiente:

```
fsck -fyc /dev/hda1
```

9.4. Asignación de formato de las particiones

Cuando la situación lo amerite, será posible dar formato a una partición en particular utilizando lo siguiente, considerando en el ejemplo que se intenta proporcionar formato EXT3 a la partición **/dev/hda1**:

```
mkfs.ext3 /dev/hda1
```

Se encuentran también disponibles las siguientes herramientas para asignación de formato:

- mkfs.ext2
- mkfs.vfat (fat32)
- mkfs.msdos (fat16)
- mkswap

Si se necesita dar un formato de bajo nivel a fin de eliminar toda la información del disco duro, puede utilizarse lo siguiente, considerando en el ejemplo que se intenta dar formato de bajo nivel al disco duro **/dev/hda**, para escribir 0 (ceros) en cada sector del disco duro.

```
dd if=/dev/zero of=/dev/hda
```

Si se requiere, también es posible dar formato de bajo nivel escribiendo números aleatorios en todos los sectores del disco duro:

```
dd if=/dev/urandom of=/dev/hda
```

10. Cómo configurar y utilizar Sudo

Joel Barrios Dueñas
darkshram@gmail.com
http://www.linuxparatodos.net/

10.1. Introducción.

Sudo es una herramienta de sistema que permite a los usuarios realizar la ejecución de mandatos como superusuario u otro usuario de acuerdo a como se especifique en el fichero **/etc/sudoers**, donde se determina quien está autorizado. Los números de identidad de usuario y de grupo (UID y GID) reales y efectivas se establecen para igualar a aquellas del usuario objetivo como esté especificado en el fichero **/etc/passwd**.

De modo predeterminado sudo requiere que los usuarios se autentiquen así mismos con su propia clave de acceso (**nunca la clave de acceso de root**). Una vez que el usuario se ha autenticado, el usuario podrá utilizar nuevamente sudo sin necesidad de volver a autenticarse durante 5 minutos, salvo que se especifique lo contrario en el fichero **/etc/sudoers**. Si el usuario ejecuta el mandato **sudo -v** podrá refrescar éste periodo de tiempo sin necesidad de tener que ejecutar un mandato, en cuyo caso contrario expirará esta autenticación y será necesario volver a realizarla.

Si un usuario no listado en el fichero **/etc/sudoers**. trata de ejecutar un mandato a través de sudo, se registra la actividad en la bitácora de sistema (a través de **syslogd**) y se envía un mensaje de correo electrónico al administrador del sistema (root).

10.1.1. Historia.

Sudo fue inicialmente concebido en 1980 por Bob Coggeshall y Cliff Spencer del departamento de ciencia computacional en SUNY (State University of New York o Universidad Estatal de Nueva York), en Buffalo.

En 1985 se publicó el grupo de noticias *net.sources* una versión mejorada acreditada a Phil Betchel, Cliff Spencer, Gretchen Phillips, John LoVerso y Don Gworek. Garth Snyder publicó otra versión mejorada en el verano de 1986 y durante los siguientes cinco años fue mantenido con al colaboración de muchas personas, incluyendo Bob Coggeshall, Bob Manchek, y Trent Hein.

En 1991 Dave Hieb y Jeff Nieusma escribieron una nueva versión con un formato mejorado para el fichero **/etc/sudoers** bajo contrato con la firma consultora The Root Group, versión que posteriormente fue publicada bajo los términos de la Licencia Pública General de GNU (GNU/GPL).

Desde 1996 el proyecto es mantenido por Todd Miller con la colaboración de Chris Jepeway y Aaron Spangler.

10.2. Fichero /etc/sudoers

El fichero **/etc/sudoers** se edita con el mandato **visudo**, herramienta que a través de vi permite realizar cambios y verificar sintaxis y errores. Si se trata de modificar directamente **/etc/sudoers**,

éste tiene permisos de solo lectura.

La sintaxis básica de una lista sería:

```
XXXX_Alias NOMBRELISTA = elemento1, elemento2, elemento3
```

La sintaxis básica de una regla sería:

```
[usuario, %grupo, NOMBRELISTA] [anfitrión] = (id de usuario a usar) mandatos
```

Se pueden definir Aliases y reglas. Los aliases permiten definir una lista de mandatos , una lista de usuarios, un alista de anfitriones o bien ejecutar como otros usuarios.

10.2.1. Cmnd_Alias.

```
Cmnd_Alias MANDATOSHTTPD = /sbin/service httpd restart, \
        /usr/bin/vim /etc/httpd/conf.d/variables.conf, \
        /usr/bin/vim /etc/php.ini
```

Lo anterior define una lista de mandatos que podrían utilizarse para reiniciar el servicio de httpd, modificar un fichero de configuración en la ruta **/etc/httpd/conf.d/varables.conf** y modificar el fichero

```
fulano ALL = MANDATOSHTTPD
```

Lo anterior define que el usuario fulano puede utilizar los mandatos de la lista MANDATOSHTTPD desde cualquier anfitrión.

10.2.2. User_Alias.

```
User_Alias USUARIOSHTTP = fulano, mengano, zutano
```

Lo anterior define una lista denominada **HTTPUSERS**, integrada por los usuarios fulano, mengano y zutano.

```
USUARIOSHTTP ALL = /usr/bin/vim
```

La regla anterior define que los usuarios que conforman la lista **USUARIOSHTTP** pueden utilizar el mandato vim desde cualquier anfitrión.

10.2.3. Host_Alias.

```
Host_Alias HOSTSHTTPD = 192.168.0.25, 192.168.0.26, 192.168.0.23
```

Lo anterior define que la lista **HOSTSHTTPD** está integrada por las 3 direcciones IP listadas anteriormente. Si además se añade la siguiente regla:

```
USUARIOSHTTPD HOSTSHTTPD =  ADMINHTTPD
```

Lo anterior define que los usuarios de la lista **HTTPDUSERS** pueden utilizar los mandatos listados en **ADMINHTTPD** solamente si están conectados desde las direcciones IP listadas en **HOSTSHTTPD**.

10.2.4. Runas_Alias.

Si por ejemplo se quisiera que los usuarios de la lista **USUARIOSHTTP** pudieran además utilizar los mandatos ls, rm, chmod, cp, mv, mkdir, touch y vim como el usuarios juan, pedro y hugo, se requiere definir una lista para estos mandatos y otra para los aliases de usuarios alternos, y la regla correspondiente.

```
Runas_Alias CLIENTES1 = juan, pedro, hugo
Cmnd_Alias MANDATOSCLIENTES = /bin/ls, \
        /bin/rm, \
        /bin/chmod, \
        /bin/cp, /bin/mv, \
        /bin/mkdir, \
        /bin/touch, \
        /usr/bin/vim
USUARIOSHTTPD HOSTSHTTPD = (CLIENTES1) MANDATOSCLIENTES
```

Lo anterior permite a los usuarios definidos en **USUARIOSHTTPD** (fulano, mengano y zutano), utilizar los mandatos definidos en **MANDATOSCLIENTES** (ls, rm, chmod, cp, mv, mkdir, touch y vim) identificándose como los usuarios definidos en **CLIENTES1** (juan, pedro y hugo) solamente si se realiza desde las direcciones IP listadas en **HOSTSHTTPD** (192.168.0.25, 192.168.0.26, 192.168.0.23).

10.3. Candados de seguridad.

Sudo incluye varios candados de seguridad que impiden se puedan realizar tareas peligrosas.

Si se define el mandato **/usr/bin/vim** en **/etc/sudoers**, se podrá hacer uso de éste de los siguientes modos:

```
$ sudo /usr/bin/vim
$ sudo vim
```

Sin embargo, no podrá ser utilizado así:

```
$ cd /usr/bin
$ sudo ./vim
```

Si se define el mandato **/bin/echo**, el usuario podrá utilizarlo de los siguientes modos:

```
$ sudo /bin/echo "Hola"
$ sudo echo "Hola"
```

Pero no podrá utilizarlo de la siguiente forma:

```
$ sudo echo "Hola" > algo.txt
```

Para poder realizar la operación anterior, tendría que utilizar:

```
$ sudo bash -c "echo 'Hola' > algo.txt"
```

Sudo le permitirá realizar una tarea sobre cualquier fichero dentro de cualquier directorio aún si no tiene permisos de acceso para ingresar a dicho directorio siempre y cuando especifique **la ruta exacta** de dicho fichero.

```
$ sudo chown named /var/named/dominio.zone
```

Pero no podrá utilizarlo así:

```
$ sudo chown named /var/named/*.zone
```

10.4. Lo que no se recomienda.

Si se quiere permitir a un usuario utilizar **lo que sea**, desde cualquier anfitrión, cómo cualquier usuario del sistema y **sin necesidad de autenticar**, se puede simplemente definir:

```
fulano ALL = (ALL) NOPASSWD: ALL
```

10.5. Facilitando la vida a través de ~/.bash_profile.

BASH (**B**ourne-**A**gain **Sh**ell) permite utilizar variables de entorno y aliases definidas en **~/.bash_profile** al iniciar la sesión, siendo que el administrador utilizará activamente muchos mandatos diversos, estos se pueden simplificar a través de aliases que resuman éstos. Por ejemplo, si se quiere definir que se utilice sudo cada vez que se invoque al mandato **chkconfig**, se puede añadir lo siguiente al fichero **~/.bash_profile**:

```
alias chkconfig="sudo /sbin/chkconfig"
```

Lo anterior permitirá ejecutar directamente el mandato **chkconfig** sin necesidad de preceder éste con el mandato **sudo**. A continuación só diversos aliases que pueden ser de utilidad en el fichero **~/.bash_profile** y que permitirán utilizar mandatos diversos con sudo.

```
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
        . ~/.bashrc
fi

# User specific environment and startup programs

PATH=$PATH:$HOME/bin:/sbin:/usr/sbin

export PATH
unset USERNAME

alias chkconfig="sudo /sbin/chkconfig"
alias service="sudo /sbin/service"
alias route="sudo /sbin/route"
alias depmod="sudo /sbin/depmod"
alias ifconfig="sudo /sbin/ifconfig"
alias chmod="sudo /bin/chmod"
alias chown="sudo /bin/chown"
alias chgrp="sudo /bin/chgrp"
alias useradd="sudo /usr/sbin/useradd"
alias userdel="sudo /usr/sbin/userdel"
alias groupadd="sudo /usr/sbin/groupadd"
alias groupdel="sudo /usr/sbin/groupdel"
alias edquota="sudo /usr/sbin/edquota"
alias vi="sudo /usr/bin/vim"
alias less="sudo /usr/bin/less"
alias tail="sudo /usr/bin/tail"
alias yum="sudo /usr/bin/yum"
alias saslpasswd2="sudo /usr/sbin/saslpasswd2"
alias htpasswd="sudo /usr/bin/htpasswd"
alias openssl="sudo /usr/bin/openssl"
alias smbpasswd="sudo /usr/bin/smbpasswd"
alias system-config-printer="sudo /usr/sbin/system-config-printer"
alias system-config-network="sudo /usr/sbin/system-config-network"
alias system-config-display="sudo /usr/bin/system-config-display"
```

Para que surtan efectos los cambios, hay que salir de la sesión y volver a ingresar al sistema con la misma cuenta de usuario, en cuyo fichero **~/.bash_profile** se añadieron estos aliases.

11. Cómo crear cuentas de usuario

Joel Barrios Dueñas
darkshram@gmail.com
http://www.linuxparatodos.net/

11.1. Introducción

GNU/Linux® es un sistema operativo con muchas características y una de ellas es que se diseñó para ser utilizado por múltiples usuarios. Aún cuando se tenga una PC con un único usuario, es importante recordar que no es conveniente realizar el trabajo diario desde la cuenta de ***root***, misma que sólo debe utilizarse para la administración del sistema.

Una cuenta de ***usuario*** contiene las restricciones necesarias para impedir que se ejecuten mandatos que puedan dañar el sistema *-programas troyanos como el Bliss-*, se altere accidentalmente la configuración del sistema, los servicios que trabajan en el trasfondo, los permisos y ubicación de los archivos y directorios de sistema, etc.

11.2. Procedimientos

Generalmente el paso que procede a una instalación de GNU/Linux® es la creación de cuentas de usuario. Para ello existen distintos métodos, todos sencillos que permiten crear una cuenta con su propio directorio de trabajo y los archivos necesarios.

Actualmente existen recursos como el programa instalador de Red Hat™ Linux® y programas que funcionan desde un entorno gráfico, como es Linuxconf y Webmin, así como recursos que funcionan en modo de texto o desde una ventana terminal, como son los mandatos tradicionales, *useradd* y *passwd*, y algunos otros programas, como YaST y la versión correspondiente de Linuxconf o Webmin.

11.2.1. Creando una cuenta en el modo de texto: *useradd* y *passwd*

Este procedimiento puede realizarse de forma segura tanto fuera de X Window® como desde una ventana terminal en el entorno gráfico del que se disponga. Fue el método comúnmente utilizado antes de la aparición de programas como YaST y Linuxconf. Sin embargo aún resulta útil para la administración de servidores, cuando no se tiene instalado X Window®, no se tienen instalados YaST o Linuxconf *-o las versiones de estos que se han instalado no trabajan correctamente-*, o bien se tienen limitaciones o problemas para utilizar un entorno gráfico.

11.2.1.1. Lo primero: el mandato *useradd*

El primer paso para crear una nueva cuenta consiste en utilizar el mandato ***useradd*** del siguiente modo:

```
useradd nombre_del_usuario
```

Ejemplo:

```
useradd fulano
```

11.2.1.2. Lo segundo: el mandato *passwd*

El paso siguiente después de crear la nueva cuenta con ***useradd*** es especificar una contraseña para el usuario. Determine una que le resulte fácil de recordar, que mezcle números, mayúsculas y minúsculas y que, preferentemente, no contenga palabras que se encontrarían fácilmente en el diccionario. Existen otras recomendaciones, por lo que es conveniente leer, antes de continuar, los comentarios finales acerca de la seguridad incluidos en este mismo artículo.

Aunque el sistema siempre tratará de prevenirlo cuando se escoja una *mala* contraseña, éste no le impedirá que lo haga. Especificar una nueva contraseña para un usuario, o bien cambiar la existente, se puede realizar utilizando el mandato ***passwd*** del siguiente modo:

```
passwd nombre_del_usuario
```

Ejemplo:

```
passwd fulano
```

El sistema solicitará entonces que proceda a escribir la nueva contraseña para el usuario y que repita ésta para confirmar. Por seguridad, el sistema no mostrará los caracteres tecleados, por lo que debe hacerlo con cuidado. Si se considera que tal vez se cometieron errores de tecleado, puede presionarse las veces que sean necesarias la tecla <Backspace> o <Retroceso>. De cualquier forma el sistema le informará si coincide o no lo tecleado. Si todo salió bien recibirá como respuesta del sistema ***code 0***. Si en cambio recibe ***code 1***, significará que deberá repetir el procedimiento, en virtud de haberse producido un error.

Este procedimiento también puede utilizarse para cambiar una contraseña existente.

11.2.1.3. Opciones avanzadas

En muchos casos las opciones pueden no ser necesarias, pero si se está administrando un servidor o estación de trabajo, o bien se es un usuario un poco más experimentado, y se quiere crear una cuenta con mayores o menores restricciones, atributos y/o permisos, pueden utilizarse las siguientes opciones de ***useradd***:

-c comment
: Se utiliza para especificar el archivo de comentario de campo para la nueva cuenta.

-d home dir
: Se utiliza para establecer el directorio de trabajo del usuario. Es conveniente, a fin de tener un sistema bien organizado, que este se localice dentro del directorio */home*.

-e expire date
: Se utiliza para establecer la fecha de expiración de una cuenta de usuario. Ésta debe ingresarse en el siguiente formato: AAAA-MM-DD.

-g initial group
: Se utiliza para establecer el grupo inicial al que pertenecerá el usuario. De forma predeterminada se establece como único grupo ***1***. Nota: el grupo asignado debe existir.

-G group,[...]
: Se utiliza para establecer grupos adicionales a los que pertenecerá el usuario. Éstos deben separarse utilizando una coma y sin espacios. Lo anterior es muy conveniente cuando se desea que el usuario tenga acceso a determinados recursos del sistema, como acceso a la unidad de disquetes, administración de cuentas PPP y POP. Nota: los grupos asignado deben de existir.

-m
: Se utiliza para especificar que el directorio de trabajo del usuario debe ser creado si acaso este no existiese, y se copiarán dentro de éste los archivos especificados en */etc/skel*.

-s shell
: Se utiliza para establecer el intérprete de mandatos que podrá utilizar el usuario. De forma predeterminada, en Red Hat™ Linux® y Fedora™ Core, se establece *bash* como intérpete de mandatos predefinido.

-u uid
: Se utiliza para establecer el UID, es decir, la ID del usuario. Este debe ser único. De forma predeterminada se establece como UID el número mínimo mayor a 99 y mayor que el de otro usuario existente. Cuando se crea una cuenta de usuario por primera vez, como ocurre en Red Hat™ Linux® y Fedora™ Core generalmente se asignará *500* como UID del usuario. Los UID entre 0 y 99 son reservados para las cuentas de los servicios del sistema.

Ejemplo:

```
useradd -u 500 -d /home/fulano -G floppy,pppusers,popusers fulano
```

Lo anterior creará una cuenta de usuario llamada «fulano», que se encuentra incluida en los grupos floppy, pppusers y popusers, que tendrá un UID=500; utilizará Bash como intérprete de mandatos y tendrá un directorio de trabajo en /home/fulano.

Existen más opciones y comentarios adicionales para el mandato useradd, las que se encuentran especificadas en los manuales. Para acceder a esta información, utilice el mandato man useradd desde una ventana terminal.

11.2.2. Eliminar una cuenta de usuario

En ocasiones un administrador necesitará eliminar una o más cuentas de usuario. Este es un procedimiento principalmente utilizado en servidores y estaciones de trabajo a los cuales acceden múltiples usuarios. Para tal fin nos valdremos del mandato **userdel**. La sintaxis básica de este mandato es la siguiente:

```
userdel nombre_del_usuario
```

Ejemplo:

```
userdel fulano
```

Si se desea eliminar también todos los archivos y directorios subordinados contenidos dentro del directorio de trabajo del usuario a eliminar, se deberá agregar la opción ***-r***:

```
userdel -r nombre_del_usuario
```

Ejemplo:

```
userdel -r fulano
```

11.3. Manejo de grupos

11.3.1. Alta de grupos

```
groupadd grupo-que-sea
```

11.3.2. Alta de grupos de sistema

Un grupo de sistema es aquel que tiene un número de identidad de grupo (GID) por debajo de 500. Regularmente se asigna automáticamente el número de identidad de grupo más bajo disponible.

```
groupadd -r grupo-que-sea
```

11.3.3. Baja de grupos

```
groupdel grupo-que-sea
```

11.3.4. Asignación de usuarios existentes a grupos existentes

```
gpasswd -a usuario-que-sea grupo-que-sea
```

11.4. Comentarios finales acerca de la seguridad

Cuando, en la mayoría de los casos, un delincuente informático consigue infiltrarse en un sistema GNU/Linux® o Unix® no es porque éste cuente con un hueco de seguridad, sino porque el intruso pudo vulnerar alguna de las contraseñas de las cuentas existentes. Si usted especificó durante el proceso de instalación de Linux® una *mala* contraseña de ***root***, algo muy común entre usuarios novicios, es altamente recomendado cambiarla.

- Evite especificar contraseñas fáciles de adivinar. Con esto nos referimos particularmente a utilizar contraseñas que utilicen palabras incluidas en cualquier diccionario de cualquier idioma, datos relacionados con el usuario o empresa, como son el registro federal de causantes (R.F.C.), fechas de nacimiento, números telefónicos, seguro social, números de cuentas de académicos o alumnos y nombres de mascotas, la palabra *Linux*®, nombres de personajes de ciencia ficción, etc.

- Evite escribir las contraseñas sobre medios físicos, prefiera siempre limitarse a memorizarlas.

- Si necesita almacenar contraseñas en un archivo, hágalo utilizando cifrado.

- Si se le dificulta memorizar contraseñas complejas, utilice entonces contraseñas fáciles de recordar, pero **cámbielas periódicamente**.

- Jamás proporcione una contraseña a personas o instituciones que se la soliciten. Evite proporcionarla en especial a personas que se identifiquen como miembros de algún servicio de soporte o ventas. Este último caso lo menciona con énfasis la página de manual del mandato ***passwd***.

Consideraremos como una *buena* contraseña aquella se compone de una combinación de números

y letras mayúsculas y minúsculas y que contiene al menos 8 caracteres. También es posible utilizar pares de palabras con puntuación insertada y frases o secuencias de palabras, o bien acrónimos de éstas.

Observar estas recomendaciones, principalmente en sistemas con acceso a redes locales y/o públicas como Internet, hará que el sistema sea más seguro.

11.5. Apéndice: Configurando valores predefinidos para el alta de cuentas de usuario

11.5.1. Fichero /etc/default/useradd para definir variables utilizadas por el mandato useradd

Como *root*, utilice un editor de texto sobre **/etc/default/useradd**. Encontrará, invariablemente, el siguiente contenido:

```
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
```

Puede cambiar lo valores que considere convenientes.

11.5.1.1. Variable HOME

El directorio de inicio del usuario será creado dentro de /home, de acuerdo a como se estipula en **Estándar de Jerarquía de Sistema de Ficheros** o FHS (**F**ilesystem **H**ierarchy **S**tandard). El valor de esta variable puede ser cambiado de acuerdo a las necesidades o preferencias del administrador.

Por ejemplo, en el caso de un sistema dedicado al servicio de hospedaje de sitios de red virtuales a través de HTTPD, pudiera preferirse utilizar `/var/www` para este fin a modo de simplificar tareas para el administrador del sistema.

En otros casos, específicamente en servidores de correo, donde se quiere aplicar una sola **cuota de disco** general para buzón de correo y carpetas de correo en el directorio de inicio, pudiera crearse un directorio dentro de `/var`, como por ejemplo `/var/home` o `/var/users`, de modo que al aplicar cuota de disco sobre la partición `/var`, ésta involucraría tanto el buzón de entrada del usuario, localizado en `/var/spool/mail/usuario`, como las carpetas de correo en el directorio de inicio del usuario, localizados dentro del directorio `/var/home/usuario/mail/`.

11.5.1.2. Variable SHELL

El intérprete de mandatos a utilizar para las nuevas cuentas que sean creadas en adelante se define a través de la variable **SHELL**. De modo predefinido el sistema asigna `/bin/bash` (BASH o **B**ourne **A**gain **Sh**ell) como intérprete de mandatos; sin embargo lo cierto es que si el sistema se utilizará como servidor, lo más conveniente sería asignarle de modo predefinido otro valor.

El más utilizado es **`/sbin/nologin`**, el cual es un programa que de forma cortés rechaza el ingreso en el sistema (login). Muestra un mensaje respecto a que la cuenta no está disponible (o bien lo que se defina en `/etc/nologin.txt`) y da salida. Se utiliza como reemplazo de un intérprete de mandatos en cuentas que han sido desactivadas o bien que no se quiere accedan hacia un intérprete de mandatos. Este programa registra en la bitácora del sistema todo intento de acceso. Para utilizarlo como valor para la variable SHELL, sólo hay que cambiar **SHELL=/bin/bash** por **SHELL=/sbin/nologin**.

```
# useradd defaults file
```

```
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/sbin/nologin
SKEL=/etc/skel
```

En adelante todo nuevo usuario que sea dado de alta en el sistema con el mandato *useradd* sin parámetro alguno, de modo predefinido no podrá acceder al sistema a través de intérprete de mandatos (shell), es decir, acceso en terminal local o remotamente. Los usuarios con estas características podrán, sin embargo, utilizar cualquier otro servicios como FTP, correo o Samba sin problema alguno.

Otros valores para la variable SHELL pueden ser:

- **/sbin/nologin**, programa que de forma cortés rechaza el ingreso en el sistema (login).
- **/bin/false**, programa que realiza salida inmediata indicando falla. Es decir, que no permite la realización de cosa alguna y además con falla. Ideal si se quiere tener cuentas de usuario con acceso hacia FTP, correo, Samba, etc., aunque sin permitir el acceso hacia un intérprete de mandatos.
- **/dev/null**, el dispositivo nulo que descarta todos los datos escritos sobre éste y no provee datos para cualquier proceso que lo lea. Ideal para definirse cuando se quiere utilizar una cuenta que sólo tenga acceso a correo (SMTP, POP3, IMAP y/o cliente de correo con interfaz HTTP).
- **/bin/bash**, intérprete de mandatos desarrollado por el proyecto GNU. Es el intérprete de mandatos predefinido en Linux y Mac OS X (a partir de Tiger).
- **/bin/sh**, un enlace simbólico que apunta hacia /bin/bash y ofrece una versión simplificada de Bash muy similar a Bourne Shell (sh).
- **/bin/tcsh**, una versión mejorada del de mandatos de C (csh).
- **/bin/ash**, un clon de Bourne shell (sh) que utiliza menos memoria.
- **/bin/zsh**, una versión mejorada de sh con funciones útiles encontradas en Bash y tcsh.

11.5.2. Directorio /etc/skel como molde para crear los directorios de inicio de los usuarios

De modo predefinido las cuentas de usuario del sistema utilizarán como molde al directorio `/etc/skel` para crear el directorio de inicio de todos los usuarios del sistema. En sistemas basados sobre Red Hat™, regularmente y como mínimo, el directorio `/etc/skel` incluye los siguientes guiones de inicio:

```
.bash_logout  .bash_profile  .bashrc  .gtkrc
```

Si, por ejemplo, se desea que cada cuenta de usuario incluya un directorio subordinado para carpetas de correo y suscripción a éstas a través del servicio de IMAP, se debe realizar el siguiente procedimiento:

```
mkdir /etc/skel/mail/
touch /etc/skel/mail/Borradores
touch /etc/skel/mail/Enviados
touch /etc/skel/mail/Papelera
```

Y ,finalmente, **crear con el editor de texto** el fichero `/etc/skel/.mailboxlist` que sirve para registrar las suscripciones hacia carpetas de correo que serán utilizadas por el servicio IMAP con un servidor UW-IMAP, utilizando el siguiente contenido:

```
mail/Borradores
mail/Enviados
mail/Papelera
```

Si se pretende utilizar modo gráfico en el sistema, de forma adicional se puede corregir un problema con algunas versiones de Firefox que generan un directorio ~/.mozilla con permisos de acceso sólo para root, de modo tal que al añadirlo en /etc/skel se incluya un directorio ~/.mozilla con permisos de acceso para el usuario al crear cada cuenta de usuario.

```
mkdir /etc/skel/.mozilla
```

11.6. Apéndice: Ejercicio: Creando cuentas de usuario

11.6.1. Introducción

A fin de poder trabajar con comodidad, se crearán algunos grupos y cuentas de usuario con diversas características.

11.6.2. Procedimientos

1. Genere contenido predefinido para los directorios de inicio a fin de que el de cada usuario contenga los directorio subordinados ~/Desktop, ~/Documents, ~/mail y ~/.mozilla:

```
ls -a /etc/skel
mkdir /etc/skel/{Desktop,Documents,mail,.mozilla}
ls -a /etc/skel
```

2. Genere, si no lo ha hecho aún como parte de los procedimientos del curso, al usuario denominado «fulano» con derecho a intérprete de mandatos, directorio de inicio **/home/fulano** y grupo principal fulano (valores por defecto):

```
useradd -s /bin/bash fulano
passwd fulano
```

3. Genere al usuario denominado «mengano» sin derecho a intérprete de mandatos, asignando el directorio de inicio **/home/mengano** y grupo principal «mengano» (valores por defecto):

```
useradd -s /sbin/nologin mengano
passwd mengano
```

4. Genere el grupo denominado «desarrollo»:

```
groupadd desarrollo
```

5. Genere el grupo denominado «sistemas» como grupo de sistema:

```
groupadd -r sistemas
```

6. Genere los directorios subordinados **/home/desarrollo** y **/home/sistemas/** del siguiente modo:

```
mkdir -p /home/desarrollo
mkdir -p /home/sistemas
```

7. Genere al usuario denominado «perengano» con derecho a intérprete de mandatos, asignando el directorio de inicio /home/**desarrollo**/perengano, grupo principal de desarrollo y grupo adicional sistemas:

```
useradd -s /bin/bash -m -d /home/desarrollo/perengano -g desarrollo -G
sistemas perengano
passwd perengano
```

8. Genere al usuario denominado «zutano» con derecho a intérprete de mandatos, asignando el directorio de inicio /home/**sistemas**/zutano, grupo principal sistemas y grupo adicional de desarrollo:

```
useradd -s /bin/bash -m -d /home/sistemas/zutano -g sistemas -G
desarrollo zutano
passwd zutano
```

9. Visualice el contenido de los ficheros **/etc/group** y **/etc/passwd** y compare y determine las diferencias entre los grupos «desarrollo» y «sistemas» y los usuarios «fulano», «mengano», «perengano» y «zutano».

```
cat /etc/group
cat /etc/passwd
```

12. Breve lección de mandatos básicos.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

12.1. Introducción.

Por favor **siga los procedimientos al pie de la letra**.

12.2. Procedimientos.

Ingrese al sistema como usuario (fulano).

Una vez que ha ingresado al sistema, realice lo siguiente:

```
pwd
```

Lo anterior le mostrará la ruta actual donde se localiza (**~/**).

Realice lo siguiente:

```
cd /usr/local
pwd
```

Lo anterior lo cambiará al directorio **/usr/local** y le mostrará la ruta actual.

Realice lo siguiente:

```
cd
pwd
```

Lo anterior lo regresará a **~/** mostrará que ahora se localiza en el directorio **~/ (directorio de inicio).**

Realice lo siguiente:

```
ls /usr/local
```

Lo anterior mostrará el contenido del directorio **/usr/local** y además mostrará que no es necesario cambiarse a un directorio en particular para ver su contenido.

Realice lo siguiente:

```
ls
ls -a
```

Lo anterior primeramente mostrará que aparentemente no hay contenido en el directorio ~/; después se mostrará lo siguiente y que en realidad si hay contenido; los ficheros y directorios de convierten a ocultos al renombrarles y ponerles un punto al inicio.

```
  .bash_logout  .bash_profile  .bashrc
```

Realice lo siguiente:

```
ls -la
```

Lo anterior deberá de mostrar todo el contenido de ~/ y mostrará además los atributos y permisos:

```
drwxr-xr-x    2 fulano     fulano         4096 ago 13 00:16 .
drwxr-xr-x   26 root       root           8192 ago 29 11:09 ..
-rw-r--r--    1 fulano     fulano           24 dic 11  2003 .bash_logout
-rw-r--r--    1 fulano     fulano          191 dic 11  2003 .bash_profile
-rw-r--r--    1 fulano     fulano          124 dic 11  2003 .bashrc
```

Realice lo siguiente:

```
ls --help
```

Lo anterior le mostrará la ayuda rápida del ls. Pulse simultáneamente en su teclado los botones <SHIFT> y <Re Pág> y luego pulse simultáneamente en su teclado los botones <SHIFT> y <Av Pág>; ésto hará que se desplace la pantalla permitiendo leer toda la información.

Pulse el botón <ENTER> y realice lo siguiente:

```
man ls
```

Lo anterior le mostrará el manual en español. Pulse las teclas de <Av Pág> y <Reg Pág> para avanzar en el manual. Pulse la tecla **/** y a continuación ingrese inmediatamente la palabra «directorio» y luego pulse la tecla <ENTER>:

```
:/directorio
```

Lo anterior le mostrará que se ha realizado una búsqueda y resaltado de la palabra «directorio» en el manual de ls. Para salir del manual de ls, pulse la tecla **q**.

Realice lo siguiente para crear un nuevo directorio:

```
mkdir ejemplos1
```

Realice lo siguiente para intentar generar un subdirectorio denominado «uno» dentro del directorio «ejemplos2» (el cual no existe ú;n).

```
mkdir ejemplos2/uno/
```

Lo anterior deberá devolver un mensaje de error como el siguiente:

```
mkdir: no se puede crear el directorio «ejemplos2/uno»: No existe el fichero o el directorio
```

A fin de poder crear el subdirectorio «uno» dentro del directorio «ejemplos2», es necesario crear primero «ejemplos2». Sin embargo puede indicarle a mkdir que genere toda la ruta añadiendo la opción -p (path):

```
mkdir -p ejemplos2/uno
ls
ls ejemplos2
```

Lo anterior creo el directorio «ejemplos2» junto con el subdirectorio «uno» en su interior y mostró que fue creado «ejemplos2» y posteriormente el contenido de «ejemplos2» para verificar que también fue creado «uno».

Ahora copiaremos algunos ficheros para experimentar un poco dentro de esta carpeta utilizando el mandato *cp*:

```
cp /etc/fstab ~/ejemplos1/
```

Luego vuelva a utilizar el mandato **cp** de este modo:

```
cp /etc/passwd ~/ejemplos1/
```

Con los dos anteriores procedimientos habrá copiado dos distintos ficheros (**/etc/fstab** y **/etc/passwd**) dentro del directorio *ejemplos1*. Proceda entonces a jugar con estos. Utilice de nuevo el mandato **mkdir** y genere una carpeta denominada **adicional** dentro del directorio de **ejemplos1**.

```
mkdir ~/ejemplos1/adicional
```

Ahora acceda hacia el directorio de *ejemplos1* para continuar. Realice lo siguiente:

```
cd ~/ejemplos1/
```

Y ahora proceda a ver el contenido de esta carpeta. Utilice el siguiente mandato:

```
ls
```

Observará en la pantalla algo como esto:

```
[fulano@localhost ejemplos1]$
adicional fstab  passwd
[fulano@localhost ejemplos1]$
```

Ahora está visualizando los ficheros **fstab** y **passwd** y el directorio **adicional**

Mueva uno de estos ficheros dentro del directorio **adicional** utilizando el mandato **mv**:

```
mv fstab adicional
```

Para ver el resultado, primero vea que ocurrió en el directorio **ejemplos1** utilizando de nuevo el mandato **ls**:

```
ls
```

Verá una salida en pantalla similar a la siguiente:

```
[fulano@localhost ejemplos1]$
adicional  passwd
[fulano@localhost ejemplos1]$
```

Acceda hacia el directorio **adicional** con el mandato **cd**

```
cd adicional
```

Se observará una salida similar a la siguiente:

```
[fulano@localhost adicional]$
fstab
[fulano@localhost adicional]$
```

Regrese hacia el directorio **ejemplos1** que se encuentra en el nivel superior utilizando el mandato **cd**:

```
cd ../
```

Ahora proceda a eliminar el fichero **passwd** que se encuentra en el directorio **ejemplos1**

```
rm passwd
```

Haga lo mismo con **fstab**, el cual se localiza dentro del directorio **adicional**:

```
rm adicional/fstab
```

Elimine el directorio **adicional**:

```
rmdir adicional
```

12.2.1. Visualizando contenido de ficheros.

Si utiliza el mandato **cat** sobre un fichero, la salida devolverá el contenido de este. utilice lo siguiente para ver el contenido del fichero **/etc/crontab**:

```
cat /etc/crontab
```

Lo anterior debe devolver una salida **similar** a la siguiente:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

Si solo se quisiera ver las lineas que contengan la cadena de caracteres **root**, se utiliza el mandato grep como subrutina del siguiente modo:

```
cat /etc/crontab | grep root
```

Lo anterior debe devolver una salida similar a la siguiente:

```
MAILTO=root
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

Si se quisiera hacer lo contrario, y solo visualizar las líneas que no contengan la cadena de caracteres **root**, se utiliza el mandato **grep** como subrutina del siguiente modo:

```
cat /etc/crontab | grep -v "root"
```

Lo anterior debe devolver una salida similar a la siguiente:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
HOME=/

# run-parts
```

Lo anterior incluye también las lineas vacías. Para mostrar el mismo resultado sin líneas vacías, se utiliza el mismo mandato agregando sed -e '/^$/d' como subrutina del siguiente modo, donde sed es un editor para filtrado y transformación de texto, ejecutando (**-e**) **/^$/d** que se refiere a líneas vacías:

```
cat /etc/crontab | grep -v "root" | sed -e '/^$/d'
```

Lo anterior debe devolver una salida similar a la siguiente:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
HOME=/
# run-parts
```

12.2.2. Generación de texto por bucles.

Realice lo siguiente, donde se utiliza el mandato **perl** ejecutando (**-e**) el guión for($i=1;$i<10;$i++){print "$in";}, en el cual se genera la variable **i** que es igual a 1 y menor a 10 y a la cual se va sumando y devuelve una salida con el valor de **i con retorno de carro**.

```
perl -e 'for($i=1;$i<10;$i++){print "$i\n";}'
```

Lo anterior debe devolver una salida similar a la siguiente:

```
1
2
3
4
5
6
7
8
9
```

Modifique el guión del mandato anterior y reemplace **"$in"** por **"Número $in"** del siguiente modo:

```
perl -e 'for($i=1;$i<10;$i++){print "Número $i\n";}'
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Número 1
Número 2
Número 3
Número 4
Número 5
Número 6
Número 7
Número 8
Número 9
```

Para guardar ésto en un fichero, añada al mandato anterior >> ~/texto.txt del siguiente modo para cambiar la salida estándar de la pantalla hacia el fichero ~/texto.txt:

```
perl -e 'for($i=1;$i<10;$i++){print "Número $i\n";}' >> ~/texto.txt
```

Lo anterior solo regresa el símbolo de sistema. Utilice elmandato **cat** para visualizar el contenido del fichero ~/texto.txt del siguiente modo:

```
cat ~/texto.txt
```

Lo anterior debe devolver una salida similar a la siguiente y que corresponde al contenido del fichero ~/texto.txt:

```
Número 1
Número 2
```

```
Número 3
Número 4
Número 5
Número 6
Número 7
Número 8
Número 9
```

12.2.3. Bucles.

A continuación aprenderá a utilizar funciones más avanzadas. En el siguiente caso usted creará respaldos de un conjunto de ficheros de imágenes, asignando a cada uno un nombre distinto al que tenían en su directorio de origen. Primero creará un nuevo directorio:

```
mkdir ~/respaldos
```

Realice los siguientes mandatos:

```
cd /usr/share/pixmaps/
for f in *.png
do
cp $f ~/respaldos/copia-$f
done
cd
```

Lo anterior realizará la copia en serie de los ficheros dentro de **/usr/share/pixmaps/** dentro de **~/respaldos/** anteponiendo en el nombre de las copias la palabra «copia». Mire el contenido del **~/respaldos/** del siguiente modo:

```
ls ~/respaldos/
```

En el siguiente caso usted definirá dos variables ($hombre y $mujer) cuyos datos serán obtenidos a partir de un fichero de texto simple (parejas.txt) y obtendrá una salida por cada juego de variables.

```
cd
echo "Juan Josefina" >> parejas.txt
echo "Pedro Julieta" >> parejas.txt
echo "Pablo Miriam" >> parejas.txt
echo "Jorge Antonia" >> parejas.txt
echo "Ernesto Carmen" >> parejas.txt
while read hombre mujer
do
echo "$hombre es pareja de $mujer"
echo "---------------------------------------"
done < parejas.txt
```

12.2.4. Aliases.

Realice lo siguiente:

```
touch algo-nuevo.txt
touch otro-nuevo.txt
```

```
cp algo-nuevo.txt otro-nuevo.txt
```

En lo anterior se crearon con el mandato **touch** los ficheros **algo-nuevo.txt** y **otro-nuevo.txt** y se realizó una copia de **algo-nuevo.txt** sobreescribiendo **otro-nuevo.txt**. Note que se sobreescribió a **otro-nuevo.txt** sin preguntar.

Ejecute ahora lo siguiente:

```
alias cp="cp -i"
cp algo-nuevo.txt otro-nuevo.txt
```

En lo anterior se creo un alias denominado **cp** que corresponde en realidad al mandato **cp** con la opción **-i**, la cual corresponde a preguntar si se sobreescriben ficheros regulares destino existentes. Cuando se ejecuta de nuevo el mandato **cp**, éste lo directamente hace con la opción **-i**.

Para deshacer el alias sobre el mandato `cp`, solo se necesita ejecutar:

```
unalias cp
```

Realice lo siguiente para crear un nuevo mandato como **alias**:

```
alias mi-mandato="ls -l |less"
```

Lo anterior crea un **alias** denominado **mi-mandato**, el cual corresponderá a ejecutar el mandato ls con la opción -l y además ejecutará como subrutina al mandato less. ejecute **mi-mandato** del siguiente modo y estudie la salida.

```
mi-mandato /etc
```

Lo anterior debe haber mostrado el contenido del directorio **/etc** utilizando **less** para poder desplazar cómodamente la pantalla. Para salir de **less** solo pulse la tecla **q**.

Los aliases creados perduran hasta que es cerrada la sesión del usuario. Para que cualquier alias sea permanente para un usuario en particular, hay que especificar estos al final del fichero **~/.bash_profile**, o bien como root en algún fichero *.sh dentro del directorio **/etc/profile.d/** para que sea utilizado por todos los usuarios del sistema. Ejecute el mandato **alias** para ver la lista de aliases predefinidos en el sistema.

```
alias
```

12.2.5. Apagado y reinicio de sistema.

Finalmente, y para concluir la breve lección de mandatos, es importante saber que aunque no se vea nada en pantalla, en Linux®ñempeñan varios procesos en el trasfondo. Estos servicios deben ser finalizados apropiadamente. No es como en MS-DOS, en donde se podía apagar el sistema en cualquier momento. Hay que cerrar el sistema apropiadamente. Para tal fin se utilizan **poweroff** y **reboot**.

Para cerrar y apagar el sistema, debe utilizar el siguiente mandato:

```
poweroff
```

Para cerrar y reiniciar el sistema, debe utilizarse el siguiente mandato:

```
reboot
```

12.3. Resumen de mandatos básicos.

Puede y debe obtener mas detalles acerca de estos y otros muchos más mandatos utilizando la opción **--help** con cualquier casi cualquier mandato. Pude consultar el manual detallado de casi cualquier mandato conocido tecleando **man** precediendo del mandato a consultar:

```
man [nombre del mandato]
```

Para salir de las páginas del manual de mandatos solo teclee *q*.

Tabla 1. Resumen de mandatos básicos.

Si se necesita acceder hacia una carpeta en especial, utilice:	`cd [ruta exacta o relativa]`
Si se necesita crear una nueva carpeta, utilice:	`mkdir [nombre del directorio]`
Si se desea copiar un fichero, utilice:	`cp [origen] [destino]`
Si se desea mover una fichero, utilice:	`mv [ruta del fichero a mover] [directorio en donde se desea mover]`
Si se desea eliminar un fichero, utilice:	`rm [nombre del fichero o ruta exacta hacia el fichero]`
Si se desea eliminar una carpeta, utilice:	`rmdir [nombre del fichero o ruta exacta hacia el directorio]`
Si se desea apagar o reiniciar el sistema, utilice:	`poweroff` y `reboot` (pueden ser utilizados como usuario) `shutdown [-h -r] [now 1,2,3,4,5,6...]` (solo como **root**

13. Cómo utilizar lsof

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

13.1. Introducción.

13.1.1. Acerca de lsof.

Lsof es un mandato que significa *«listar ficheros abiertos»* (**l**i**s**t open **f**iles). Es utilizado ampliamente en sistemas operativos tipo **POSIX** para hacer reportes de ficheros y los procesos que están utilizando a éstos. Se puede utilizar para revisar que procesos están haciendo uso de directorios, ficheros ordinarios, tuberías (*pipes*), zócalos de red (*sockets*) y dispositivos. Uno de los principales usos de determinar que procesos están haciendo uso de ficheros en una partición cuando esta no se puede desmontar. **Lsof** fue desarrollado por **Vic Abell**, quien alguna vez fue director del Centro de Cómputo de la **Universidad de Purdue**.

13.2. Procedimientos.

En ausencia de parámetros, **lsof** mostrará **todos** los procesos haciendo uso de ficheros. En ejemplo de la salida típica sería como la siguiente:

```
COMMAND     PID      USER   FD      TYPE     DEVICE       SIZE       NODE NAME
init          1      root  cwd       DIR        9,3       4096          2 /
init          1      root  rtd       DIR        9,3       4096          2 /
init          1      root  txt       REG        9,3      38620     146434 /sbin/init
init          1      root  mem       REG        9,3     125736     175507 /lib/ld-2.5.so
init          1      root  mem       REG        9,3    1602164     175514
/lib/i686/nosegneg/libc-2.5.so
init          1      root  mem       REG        9,3      16428     175518 /lib/libdl-2.5.so
init          1      root  mem       REG        9,3      93508     175677 /lib/libselinux.so.1
init          1      root  mem       REG        9,3     242880     175573 /lib/libsepol.so.1
init          1      root   10u     FIFO       0,15                  1543 /dev/initctl
```

Para visualizar más cómodamente esta salida, se puede utilizar el mandato **less** o el mandato **more** como subrutinas. Ejemplo:

```
lsof | less
```

Puede especificarse que se muestren todos los procesos desde un directorio en particular, solamente especificando este luego de **lsof**. En el siguiente ejemplo se solicita a **lsof** mostrar todos los procesos que estén haciendo uso de algo dentro de /var.

```
lsof /var
```

La salida de la anterior puede ser similar a la siguiente:

```
COMMAND     PID   USER   FD   TYPE DEVICE      SIZE     NODE NAME
auditd     2247   root    5w   REG    9,1    408058  5341208 /var/log/audit/audit.log
syslogd    2281   root    1w   REG    9,1   1134708 17006593 /var/log/messages
syslogd    2281   root    2w   REG    9,1     12461 17006594 /var/log/secure
syslogd    2281   root    3w   REG    9,1      9925 17006595 /var/log/maillog
syslogd    2281   root    4w   REG    9,1      3339 17006598 /var/log/cron
syslogd    2281   root    5w   REG    9,1         0 17006596 /var/log/spooler
syslogd    2281   root    6w   REG    9,1       916 17006597 /var/log/boot.log
named      2350  named  cwd    DIR    9,1      4096 16351240 /var/named/chroot/var/named
named      2350  named  rtd    DIR    9,1      4096 16351236 /var/named/chroot
named      2350  named    9r   CHR    1,8           16351246 /var/named/chroot/dev/random
rpc.statd  2407   root  cwd    DIR    9,1      4096 15433729 /var/lib/nfs/statd
rpc.statd  2407   root    8w   REG    9,1         5 25591831 /var/run/rpc.statd.pid
```

Si se quiere mostrar solamente el fichero utilizado por un procesos en particular, se utiliza la opción -p seguida del número de proceso. En el siguiente ejemplose solicita a **lsof** mostrar los ficheros utilizados por el proceso 2281 que arbitrariamente se ejecuta en un sistema:

```
lsof -p 2281
```

Si hubiera un proceso 2281, la salida podría verse como la siguiente:

```
COMMAND  PID USER   FD   TYPE     DEVICE    SIZE     NODE NAME
syslogd 2281 root  cwd    DIR        9,3    4096        2 /
syslogd 2281 root  rtd    DIR        9,3    4096        2 /
syslogd 2281 root  txt    REG        9,3   35800   146392 /sbin/syslogd
syslogd 2281 root  mem    REG        9,3 1602164   175514 /lib/i686/nosegneg/libc-2.5.so
syslogd 2281 root  mem    REG        9,3   46680   175529 /lib/libnss_files-2.5.so
syslogd 2281 root  mem    REG        9,3  125736   175507 /lib/ld-2.5.so
syslogd 2281 root    0u  unix 0xc0acfc80             6909 /dev/log
syslogd 2281 root    1w   REG        9,1 1134708 17006593 /var/log/messages
syslogd 2281 root    2w   REG        9,1   12461 17006594 /var/log/secure
syslogd 2281 root    3w   REG        9,1    9925 17006595 /var/log/maillog
syslogd 2281 root    4w   REG        9,1    3339 17006598 /var/log/cron
syslogd 2281 root    5w   REG        9,1       0 17006596 /var/log/spooler
syslogd 2281 root    6w   REG        9,1     916 17006597 /var/log/boot.log
```

La opción **-i** hará que se muestren todos los ficheros de red (**Internet** y **x.25**) utilizados por procesos de red. Si se quiere mostrar los ficheros de red en uso por algún proceso de red en particular, se utilizan las opciones **-i** seguido de una subrutina con **grep** y el nombre de algún servicio. En el siguiente ejemplo se pide a **lsof** mostrar solamente los ficheros de red utilizados por los procesos de red derivados de **named**:

```
lsof -i | grep named
```

Lo anterior puede devolver una salida similar a la siguiente.

```
named      2350  named   20u  IPv4    7091       UDP localhost.localdomain:domain
named      2350  named   21u  IPv4    7092       TCP localhost.localdomain:domain (LISTEN)
named      2350  named   22u  IPv4    7093       UDP servidor.redlocal.net:domain
named      2350  named   23u  IPv4    7094       TCP servidor.redlocal.net:domain (LISTEN)
```

```
named      2350  named   24u  IPv4    7095       UDP *:filenet-tms
named      2350  named   25u  IPv6    7096       UDP *:filenet-rpc
named      2350  named   26u  IPv4    7097       TCP localhost.localdomain:rndc (LISTEN)
named      2350  named   27u  IPv6    7098       TCP localhost6.localdomain6:rndc (LISTEN)
named      2350  named   28u  IPv4 1153790       UDP 192.168.122.1:domain
```

14. Funciones básicas de vi

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

14.1. Introducción

vi es uno de los editores de texto más poderosos y añejos que hay en el mundo de la informática. Resulta sumamente útil conocer la funcionalidad básica de vi a fin de facilitar la edición de ficheros de texto simple, principalmente ficheros de configuración.

14.2. Procedimientos

14.2.1. Instalación y paquetes adicionales

Por lo general, vi se instala de modo predefinido en la mayoría de las distribuciones de GNU/Linux a través del paquete **vim-minimal**. Puede añadirse funcionalidad adicional a través de los siguientes paquetes:

- **vim-enhanced:** Una versión mejorada de vi que añade color a la sintaxis y otras mejoras en la interfaz.
- **vim-X11**: Versión de vi para modo gráfico que resulta más fácil de utilizar gracias a los menús y barra de herramientas.

Si lo desea, puede proceder a instalar vi y el resto de los paquetes relacionados realizando lo siguiente:

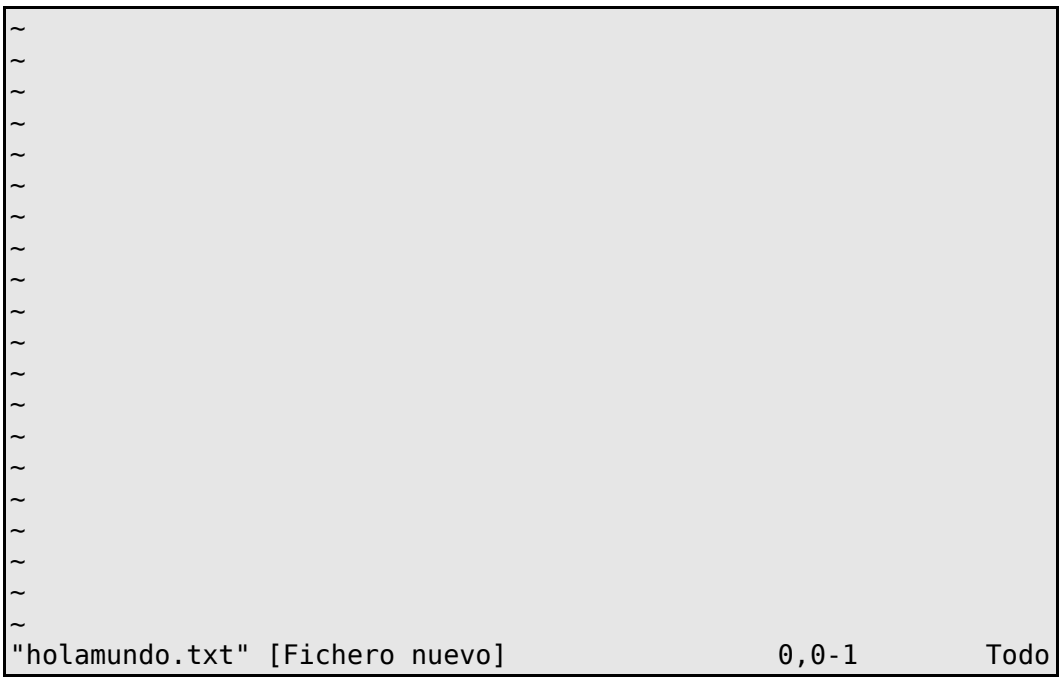
```
yum -y install vim vim-enhanced vim-common vim-minimal
```

14.3. Conociendo vi

Acceda al sistema autenticando como usuario (fulano) y realice lo siguiente:

```
vi holamundo.txt
```

Lo anterior mostrará una interfaz como la siguiente:



Pulse una vez el botón <INSERT> de su teclado y observe los cambios en la pantalla

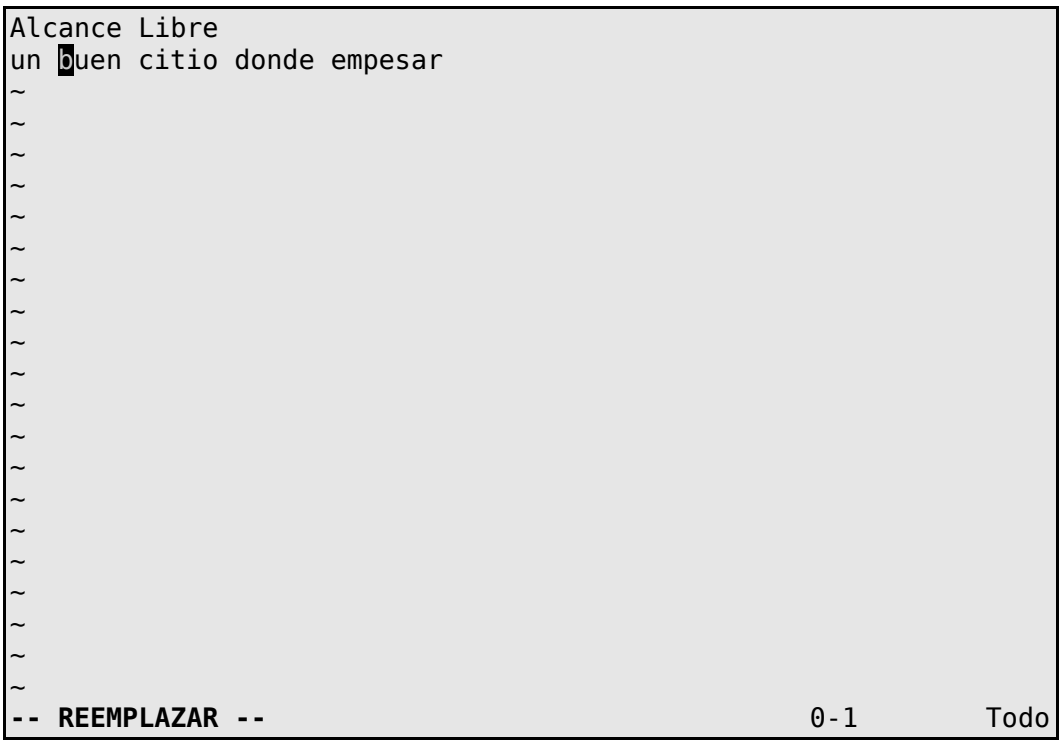
Note que en la parte inferior de la pantalla aparece la palabra «**INSERTAR**». Esto significa que, al igual que cualquier otro editor de texto conocido, puede comenzar a insertar texto en el fichero. Escriba la frase «Alcance Libre», pulse la tecla <ENTER> y **escriba** de forma propositiva la frase «un vuen citio donde empesa»:

```
Alcance Libre
un vuen citio donde empesar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERTAR --                                    0-1        Todo
```

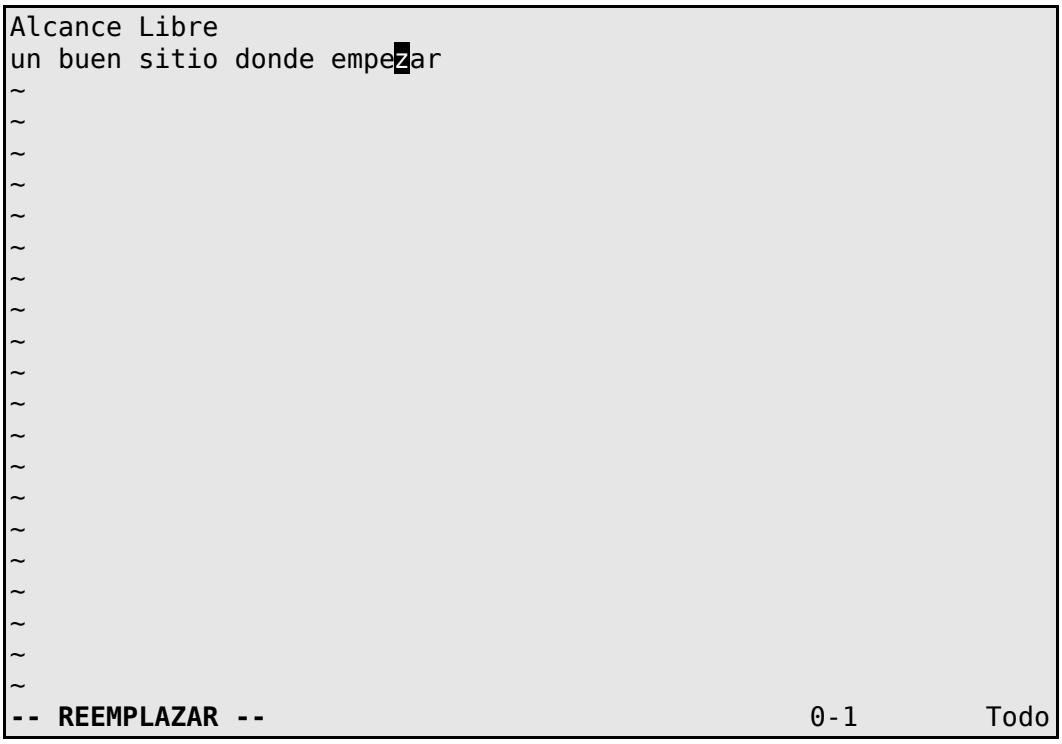
Posicione el cursor del teclado justo por debajo de la «v» de la palabra «vuen» y pulse de nuevo la tecla <INSERT> del teclado. Notará que ahora aparece la palabra «REEMPLAZAR»:

```
Alcance Libre
un vuen citio donde empesar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- REEMPLAZAR --                                  0-1        Todo
```

Pulse la tecla «b» y observe como se reemplaza la letra «v» dando como resultado que la palabra quede ortográficamente correcta como «buen»:



Mueva el cursor con las flechas del teclado y repita el procedimiento reemplazando la letra «c» por una «s» en la palabra «citio» de modo que quede como «sitio» y de igual modo reemplace la letra «s» por una «z» en la palabra «reemplasar» de modo que quede como «empezar»:



Pulse la tecla <ESC> para salir del modo de reemplazo e inmediatamente pulse la tecla : (dos puntos) seguido de la letra «w» a fin de proceder a guardar el fichero en el disco duro:

```
Alcance Libre
un buen sitio donde empezar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:w
```

Pulse la tecla <ENTER> y notará que aparece un mensaje en la parte inferior de la pantalla que indicará que el fichero ha sido guardado:

```
Alcance Libre
un buen sitio donde empezar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"holamundo.txt" [Nuevo] 2L, 44C escritos       2,3          Todo
```

Vuelva a pulsar la tecla **:** (dos puntos) e inmediatamente escriba «saveas adiosmundo.txt»:

```
Alcance Libre
un buen sitio donde empezar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:saveas adiosmunto.txt
```

Pulse nuevamente la tecla <ENTER> y observe el mensaje en la parte inferior de la pantalla que indica que el fichero acaba de ser guardado como adiosmundo.txt:

```
Alcance Libre
un buen sitio donde empezar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"adiosmundo.txt" [Nuevo] 2L, 44C escritos       2,3           Todo
```

Vuelva a pulsar la tecla «INSERT» para regresar al modo de inserción y escriba lo siguiente:

```
Alcance Libre
un buen sitio donde empezar
Creo que el mundo es un lugar muy malo
La gente que conozco es mala
Mi vida ha sido muy mala
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERTAR --                                5,24          Todo
```

A continuación pulse la tecla <ESC> e inmediatamente pulse la tecla **:** (dos puntos) seguido de la combinación de teclas **%s/mal/buen/g** del siguiente modo:

```
Alcance Libre
un buen sitio donde empezar
Creo que el mundo es un lugar muy malo
La gente que conozco es mala
Mi vida ha sido muy mala
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:%s/mal/buen/g
```

Pulse de nuevo la tecla <ENTER> y observe como ha sido reemplazada la cadena de caracteres «mal» por la cadena de caracteres «buen» en todo el fichero, quedando del siguiente modo:

```
Alcance Libre
un buen sitio donde empezar
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
3 sustituciones en 3 líneas                    5,1           Todo
```

En el procedimiento anterior, el símbolo «%» indicaba que se aplicaría un procedimiento a todo el fichero, no solo en la misma línea; la letra «s» indicaba que se realizaría la búsqueda de la cadena de caracteres «mal» definida después de la diagonal (/) por la cadena de caracteres «buen» en toda la línea, indicado por la letra «g».

A continuación, posicione el cursor del teclado utilizando las flechas del teclado hasta el primer carácter de la primera línea:

```
Alcance Libre
un buen sitio donde empezar
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
3 sustituciones en 3 líneas                    5,1           Todo
```

Ahora pulse dos veces consecutivas la tecla «d», es decir, pulsará «dd». Observe como desaparece la primera línea:

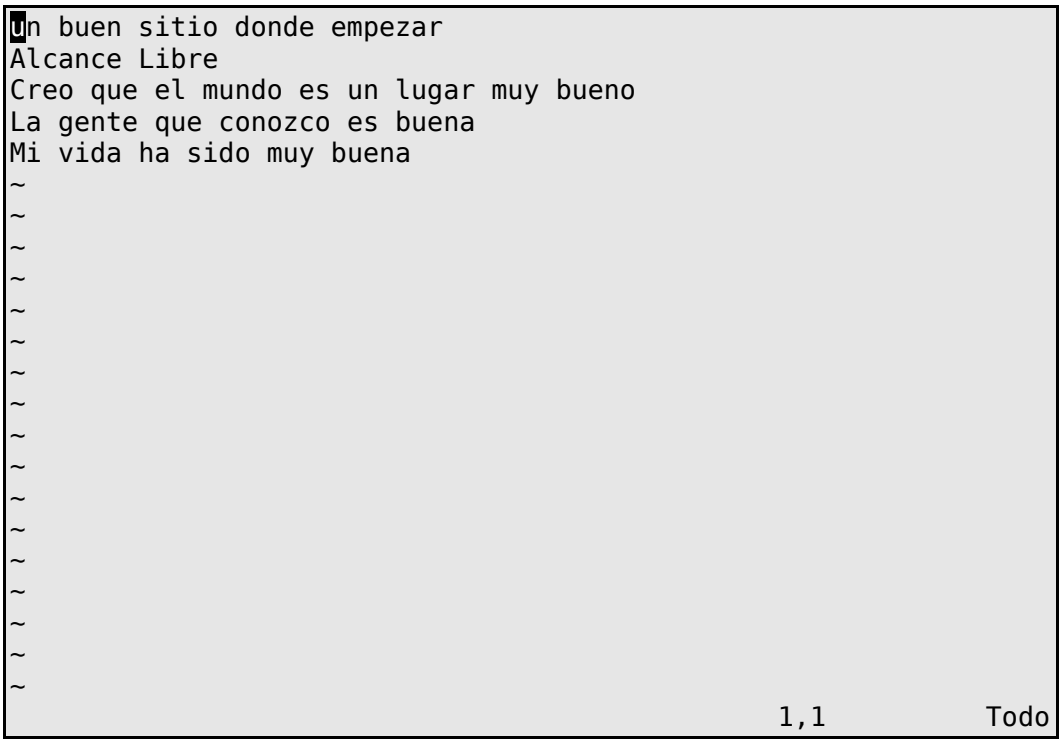
```
un buen sitio donde empezar
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

Pulse ahora la tecla «p» para volver a pegar la línea:

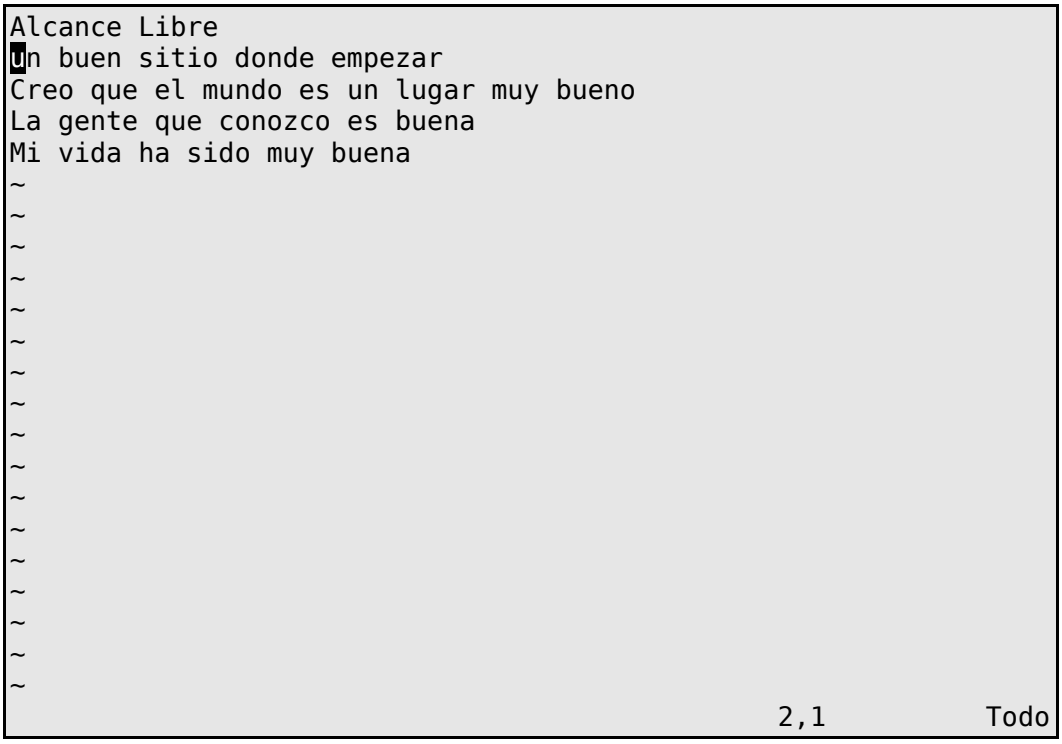
```
un buen sitio donde empezar
Alcance Libre
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

Observe que la línea «Alcance Libre» reapareció debajo de la línea «un buen sitio donde empezar». Utilizando las flechas del teclado, coloque el cursor del teclado nuevamente sobre el primer carácter de la primera linea del fichero, es decir, sobre la letra «u» de la línea «un buen sitio donde

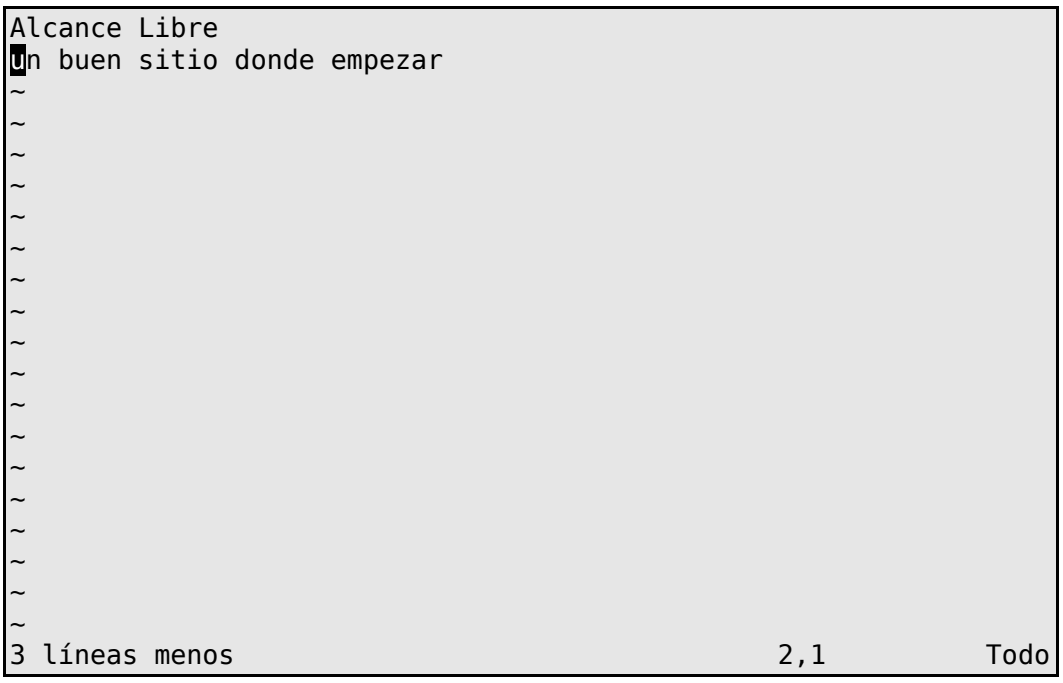
empezar»:



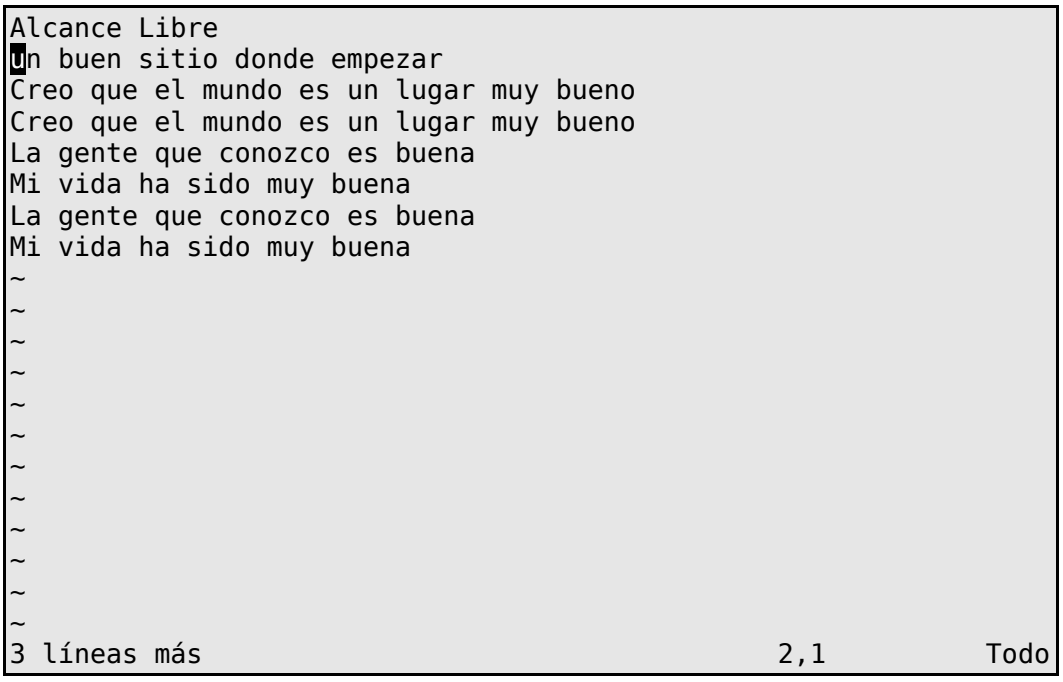
Vuelva a pulsar «dd» para cortar la línea «un buen sitio donde empezar» e inmediatamente pulse la tecla «p» para pegar la línea en el lugar correcto:



Coloque ahora el cursor sobre la letra «C» de la linea «Creo que el mundo es un lugar muy bueno» y pulse la tecla «3» seguido de «dd» y observe como son cortadas las tres siguientes lineas:

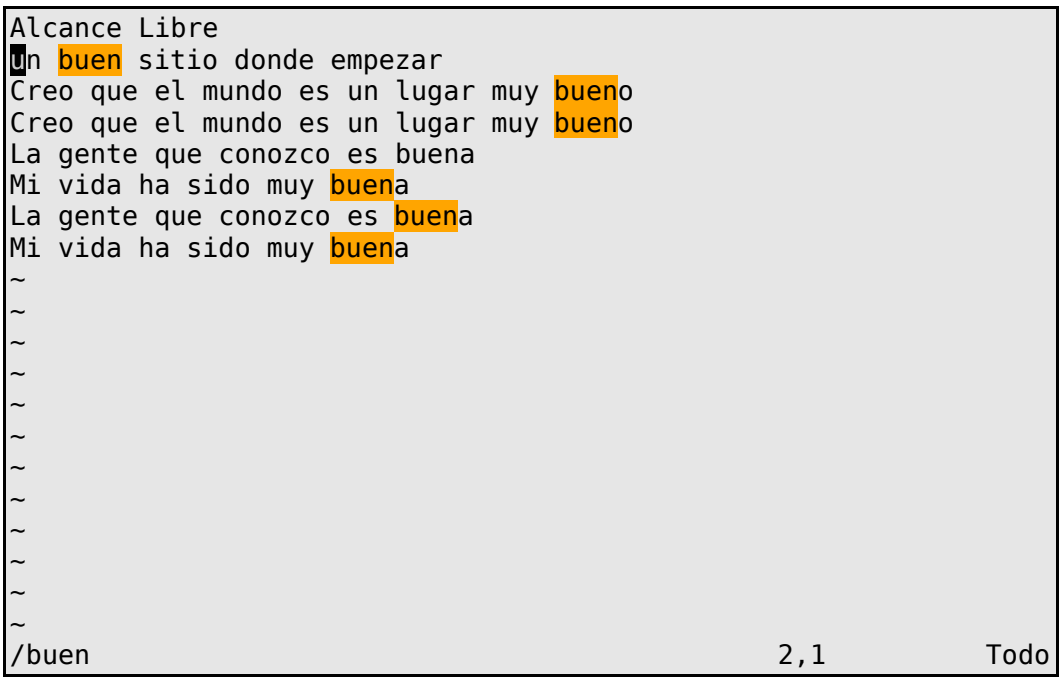


Pulse la tecla «p» una vez, observe el resultado. Vuelva a pulsar la tecla «p» y observe el resultado. Las dos acciones anteriores añadieron ahora 6 líneas restaurando las eliminadas anteriormente y agregando tres líneas más con el mismo contenido:

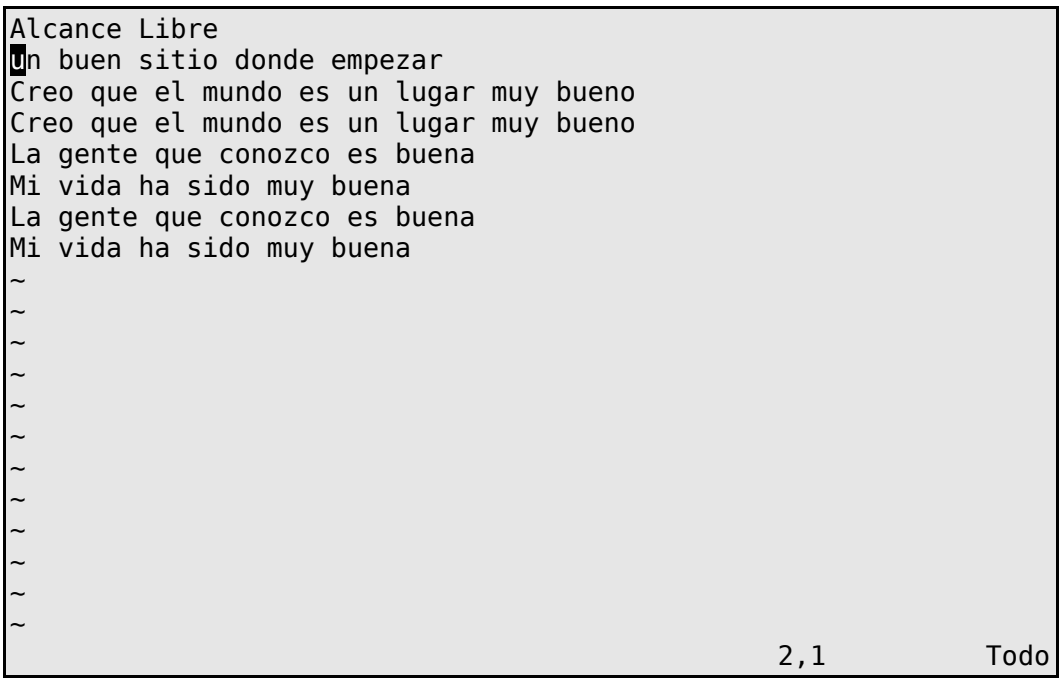


Pulse ahora la tecla **:** (dos puntos) seguido de la tecla «x» y la tecla <ENTER> a fin de salir guardando el fichero.

Abra nuevamente el fichero **adiosmundo.txt** con vi y pulse la combinación de teclas **:/buen**, de modo que se realice una búsqueda de la cadena de caracteres «buen» y además se resalten las coincidencias:



Para cancelar lo que se encuentra resaltado de los resultados, pulse la combinación de teclas **:nohl**:



Pulse **A** (combinación de las teclas SHIFT+a) mientras el cursor permanece en la segunda línea y observe que iniciará el modo **INSERTAR** colocando el cursor al final de la línea donde se encontraba:

```
Alcance Libre
un buen sitio donde empezar
Creo que el mundo es un lugar muy bueno
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
-- INSERTAR --                                  2,1           Todo
```

Pulse la tecla <ESC> y enseguida **o**. Notará que iniciará el modo **INSERTAR** abriendo una nueva línea:

```
Alcance Libre
un buen sitio donde empezar

Creo que el mundo es un lugar muy bueno
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
-- INSERTAR --                                  3,1           Todo
```

Pulse nuevamente la tecla <ESC> y en seguida la combinación **dG** (d, luego SHIFT+G). Notará que se elimina todo el contenido del texto desde la posición del cursor hasta el final del fichero:

```
Alcance Libre
un buen sitio donde empezar
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
7 líneas menos                                  2,1           Todo
```

Pulse la combinación **:u** y notará que el cambio se ha descartado, regresando las 7 líneas que habían sido eliminadas:

```
Alcance Libre
un buen sitio donde empezar
Creo que el mundo es un lugar muy bueno
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
~
7 líneas más                                    3,0-1         Todo
```

14.4. Otras combinaciones de teclas

Combinación	**Resultado**
i [o bien la tecla insert]	Inicia insertar texto **antes** del cursor
a	Inicia insertar texto **después** del cursor

Combinación	Resultado
I (i + SHIFT)	Inicia insertar texto al **inicio** de la línea donde se encuentra el cursor
A (a + SHIFT)	Inicia insertar texto al **final** de la línea donde se encuentra el cursor.
o	Abre una nueva línea e inicia insertar texto en la nueva línea.
x	Elimina el carácter que esté sobre el cursor.
dd	Elimina la línea actual donde se encuentre el cursor.
D	Elimina desde la posición actual del cursor hasta el final de la misma línea donde se encuentra el cursor.
dG	Elimina todo hasta el final del fichero.
:q	Aparece si no hubo cambios en el ficheros.
:q!	Aparece descartando los cambios en el fichero.
:w	Guarda el fichero sin salir.
:wq	Guarda el fichero y sale de vi.
:x	Lo mismo que :wq
:saveas /lo/que/sea	Guarda el fichero como otro fichero donde sea necesario.
:wq! ++enc=utf8	Codifica el fichero en UTF-8.
:u	Deshacer cambios
:red	Rehacer cambios.
:/cadena de caracteres	Búsqueda de cadenas de caracteres.
:nohl	Cancelar el resaltado de resultados de Búsqueda.

14.5. Más allá de las funciones básicas

Instale el paquete vim-enhanced:

```
yum -y install vim-enhanced
```

Utilice **vimtutor** y complete el **tutor interactivo oficial** de vi a fin de que conozca el resto de las funcionalidades más importantes.

15. Introducción a sed

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

15.1. Introducción.

15.1.1. Acerca de sed.

Sed es un editor de emisiones (**s**tream **ed**itor) utilizado para el procesamiento de texto en ficheros. Utiliza un lenguaje de programación para realizar transformaciones en una emisión de datos leyendo línea por línea de estos. Fue desarrollado entre 1973 y 1974 por Lee E. McMahon de Bell Labs. Está incluido en las instalaciones básicas de prácticamente todas las distribuciones de GNU/Linux.

15.2. Procedimientos.

A continuación se mostrarán ejemplos del uso de **sed**.

Utilice vi para crear el fichero usuario.txt:

```
vi usuario.txt
```

Ingrese el siguiente contenido y salga de vi:

```
Fulano Algo
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Si utiliza el mandato cat sobre el fichero, visualizará tal cual el contenido de usuario.txt como fue ingresado en vi.

```
cat usuario.txt
```

Si se quiere convertir a doble espacio la salida del fichero usuario.txt, utilice el siguiente mandato:

```
sed G usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo

Calle Mengana 123

Colonia Perengana

Ciudad de Zutano, C.P. 123456
```

Para guardar esta salida en el fichero usuario2.txt, utilice lo siguiente:

```
sed G usuario.txt > usuario2.txt
```

Si se quiere convertir a doble espacio la salida del fichero usuario.txt, utilice el siguiente mandato:

```
sed 'G;G' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo

Calle Mengana 123

Colonia Perengana

Ciudad de Zutano, C.P. 123456
```

Para guardar esta salida en el fichero usuario2.txt, utilice lo siguiente:

```
sed 'G;G' usuario.txt > usuario3.txt
```

El contenido de usuario3.txt tendrá triple espacio de separación. Si se desea convertir un fichero a doble espacio, pero que no haya más de una línea vacía entre cada lñíena con datos, se utiliza lo siguiente:

```
sed '/^$/d;G' usuario3.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo

Calle Mengana 123

Colonia Perengana

Ciudad de Zutano, C.P. 123456
```

Si se desea eliminar el doble espacio del fichero usuario2.txt, se utiliza lo siguiente:

```
sed 'n;d' usuario2.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo

Calle Mengana 123
```

```
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Si se quiere agregar una línea en blanco arriba de toda línea que contenga la expresión regular **enga**, se utiliza lo siguiente:

```
 sed '/enga/{x;p;x;}' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle M**enga**na 123
Colonia P**eren**gana
Ciudad de Zutano, C.P. 123456
```

Si se quiere agregar una línea en blanco debajo de toda línea que contenga la expresión regular **3**, se utiliza lo siguiente:

```
sed '/3/G' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 12**3**

Colonia Perengana
Ciudad de Zutano, C.P. 12**3**456
```

Si se quiere agregar una línea en blanco arriba y debajo de toda línea que contenga la expresión regular **3**, se utiliza lo siguiente:

```
sed '/3/{x;p;x;G;}' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 123

Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Para reemplazar texto se utiliza el modelo 's/texto/nuevo-texto/' donde texto puede ser también una expresión regular. En el siguiente ejemplo se reemplazarán las incidencias del número por el número 9:

```
sed 's/3/9/g' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 12**9**

Colonia Perengana
```

```
Ciudad de Zutano, C.P. 129456
```

En el siguiente ejemplo se reemplazan los espacios por tabuladores a todo lo largo de todas las líneas:

```
sed 's/\ /\t/g' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano  Algo
Calle   Mengana 123
Colonia Perengana
Ciudad  de Zutano,      C.P.    123456
```

En el siguiente ejemplo se reemplazan solo el primer espacio de cada línea por un tabulador:

```
sed 's/\ /\t/' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano  Algo
Calle   Mengana 123
Colonia Perengana
Ciudad  de Zutano, C.P. 123456
```

La siguiente línea añade 5 espacios al inicio de cada línea:

```
sed 's/^/     /' usuario.txt
```

La salida devolverá lo siguiente:

```
     Fulano Algo
     Calle Mengana 123
     Colonia Perengana
     Ciudad de Zutano, C.P. 123456
```

El siguiente mandato solo imprime la primera línea del fichero usuario.txt:

```
sed q usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
```

El siguiente mandato solo imprime las primeras dos líneas del fichero usuario.txt:

```
sed 2q usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Calle Mengana 123
```

El siguiente mandato solo muestra las últimas tres líneas del fichero usuario.txt:

```
sed -e :a -e '$q;N;4,$D;ba' usuario.txt
```

La salida devolverá lo siguiente:

```
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

El siguiente mandato solo mostrará las líneas que incluyen **3**:

```
sed '/3/!d' usuario.txt
```

La salida devolverá lo siguiente:

```
Calle Mengana 123
Ciudad de Zutano, C.P. 123456
```

El siguiente mandato solo mostrará las líneas que **no** incluyen **3**:

```
sed '/3/d' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
Colonia Perengana
```

El siguiente mandato pide mostrar la linea que está inmediatamente después de la expresión **Fulano**, pero no la línea en si que incluye **Fulano**:

```
sed -n '/Fulano/{n;p;}' usuario.txt
```

La salida devolverá lo siguiente:

```
Calle Mengana 123
```

El siguiente mandato pide mostrar la linea que está inmediatamente antes de la expresión **Calle**, pero no la línea en si que incluye **Calle**:

```
sed -n '/Calle/{g;1!p;};h' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo
```

15.3. Bibliografía.

- Eric Pement: http://student.northpark.edu/pemente/sed/sed1line.txt
- Wikipedia: http://en.wikipedia.org/wiki/Sed

16. Introducción a AWK

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

16.1. Introducción.

16.1.1. Acerca de AWK.

AWK, cuyo nombre deriva de la primera letra de los apellidos de sus autores Alfred **A**ho, Peter **W**einberger y Brian **K**ernighan, es un lenguaje de programación que fue diseñado con el objetivo de procesar datos basados sobre texto y una de las primeras herramientas en aparecer en Unix. Utiliza listas en un índice ordenado por cadenas clave (listas asociativas) y expresiones regulares. Es un lenguaje ampliamente utilizado para la programación de guiones ejecutables pues añade funcionalidad a las tuberías en los sistemas operativos tipo **POSIX**. Está incluido en las instalaciones básicas de prácticamente todas las distribuciones de GNU/Linux.

16.1.2. Estructura de los programas escritos en AWK.

El mandato **awk** utiliza un fichero o emisión de ordenes y un fichero o emisión de entrada. El primero indica como procesar al segundo. El fichero de entrada es por lo general texto con algún formato que puede ser un fichero o bien la salida de otro mandato.

La sintaxis general utilizada para el mandato **awk** sigue el siguiente patrón:

awk 'expresión-regular { orden }'

Cuando se utiliza el mandato awk, éste examina el fichero de entrada y ejecuta la orden cuando encuentra la expresión regular especificada.

El siguiente modelo ejecutaría la orden al inicio del programa y antes de que sean procesados los datos del fichero de entrada:

```
awk 'BEGIN { orden }'
```

El siguiente modelo ejecutaría la orden al final del programa y después de que sean procesados los datos del fichero de entrada:

```
awk 'BEGIN { orden }'
```

El siguiente modelo ejecutaría la orden por cada una de las líneas del fichero de entrada:

```
awk '{ orden }'
```

16.2. Procedimientos.

A continuación se mostrarán ejemplos del uso de AWK.

El siguiente mandato específica que al inicio se imprima en la salida la frase "Hola mundo" y terminar el procesamiento.

```
awk 'BEGIN { print "Hola mundo"; exit }'
```

Lo anterior deberá devolver una salida como la siguiente:

```
Hola mundo
```

Si se genera el fichero prueba.txt del siguiente modo:

```
echo -e "Columna1\tColumna2\tColumna3\tColumna4\n" > ejemplo.txt
```

Y se visualiza con el mandato cat:

```
cat ejemplo.txt
```

Devolverá el siguiente contenido:

```
Columna1        Columna2        Columna3        Columna4
```

Si se utiliza el mandato awk para que solo muestre la columna 1 y la columna 3 del siguiente modo:

```
awk '{ print $1, $3}' ejemplo.txt
```

La salida devolverá lo siguiente:

```
Columna1 Columna3
```

Si se utiliza el mandato awk para que solo muestre la columna 3 y la columna 1, en ese orden, del siguiente modo:

```
awk '{ print $3, $1}' ejemplo.txt
```

La salida devolverá lo siguiente:

```
Columna3 Columna1
```

Si se añaden datos al fichero ejemplo.txt del siguiente modo:

```
echo -e "Dato1\tDato2\tDato3\tDato4\n" >> ejemplo.txt
echo -e "Dato5\tDato6\tDato7\tDato8\n" >> ejemplo.txt
echo -e "Dato9\tDato10\tDato11\tDato4\12" >> ejemplo.txt
```

Y se visualiza con el mandato cat:

```
cat ejemplo.txt
```

Devolverá el siguiente contenido:

```
Columna1        Columna2        Columna3        Columna4
Dato1   Dato2   Dato3   Dato4
Dato5   Dato6   Dato7   Dato8
Dato9   Dato10  Dato11  Dato4
```

Si se utiliza nuevamente el mandato awk para que solo muestre la columna 1 y la columna 3 del siguiente modo:

```
awk '{ print $1, $3}' ejemplo.txt
```

La salida devolverá lo siguiente:

```
Columna1 Columna3
Dato1 Dato3
Dato5 Dato7
Dato9 Dato11
```

Si se utiliza el mandato awk del siguiente modo para que solo muestre solo la línea cuya columna contenga la expresión regular Dato5:

```
awk '/Dato5/ { print }' ejemplo.txt
```

La salida devolverá lo siguiente:

```
Dato5   Dato6   Dato7   Dato8
```

Si se utiliza el mandato awk del siguiente modo para que solo muestre solo la línea cuya columna contenga la expresión regular Dato5, y además solo las columnas 1 y 4:

```
awk '/Dato5/ { print $1, $4}' ejemplo.txt
```

La salida devolverá lo siguiente:

```
Dato5 Dato8
```

Si se utiliza el mandato awk del siguiente modo para que muestre solo las líneas con más de 35 caracteres en el fichero /etc/crontab:

```
awk 'length > 35' /etc/crontab
```

La salida devolverá lo siguiente:

```
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

Si se utiliza el mandato awk del siguiente modo para que muestre solo las líneas con menos de 35 caracteres en el fichero /etc/crontab:

```
awk 'length < 35' /etc/crontab
```

La salida devolverá lo siguiente:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/
# run-parts
```

Utiliza vi para crear el fichero usuario.txt:

```
vi usuario.txt
```

Ingrese el siguiente contenido:

```
Fulano Algo
Calle Mengana 123
Colonia Perengana
Ciudad de Zutano, C.P. 123456
```

Para que el mandato **awk** reconozca cada línea como un registro completo, en lugar de considerar cada palabra como una columna, se utiliza '**BEGIN { FS="\n" ; RS=""}**', donde el valor de **FS** (**F**ield **S**eparator o separador de campo) se establece como un retorno de carro y el valor de **RS** (**R**ecord **S**eparator o separador de registro) se establece como una línea vacía. Si utiliza el siguiente mandato donde se establecen los valores mencionados para FS y RS y se pide se impriman los valores de cada registro (cada línea) separados por una coma y un espacio:

```
awk 'BEGIN { FS="\n"; RS="" } { print $1 ", " $2 ", " $3 ", " $4 }' usuario.txt
```

La salida devolverá lo siguiente:

```
Fulano Algo, Calle Mengana 123, Colonia Perengana, Ciudad de Zutano, C.P. 123456
```

El mandato **awk** puede realizar conteo de líneas, palabras y caracteres. El el siguiente mandato se establece que el valor de **w** sea igual al número de campos (**N**ew **F**ield o **NF**), **c** sea igual la longitud de cada campo, y que se imprima el número de campos, el valor de **w** y el valor de **c**:

```
awk '{ w += NF; c += length} \
END { print \
"Campos: " NR , "\nPalabras: " w, "\nCaracteres: " c }' \
usuario.txt
```

La salida devolverá lo siguiente:

```
Campos: 4
Palabras: 12
Caracteres: 74
```

Genere el fichero numeros.txt con el siguiente contenido, donde las columnas serán separadas por un tabulador:

```
1 2 3 4
5 6 7 8
9 10 11 12
```

El mandato awk puede realizar operaciones matemáticas. el siguiente mandato establece que s es igual a la suma del valor de los campos de la primera columna del fichero numeros.txt, e imprime el valor de s:

```
awk '{ s += $1 } END { print s }' numeros.txt
```

La salida devolverá lo siguiente (resultado de la suma de 1+5+9):

```
15
```

Si se hace lo mismo, pero con los valores de la columna 2:

```
awk '{ s += $2 } END { print s }' numeros.txt
```

La salida devolverá lo siguiente (resultado de la suma de 2+6+10):

```
18
```

Para hacer conteo de frecuencia de palabras, Se establece que el valor para **FS** (**F**ield **S**eparator o separador de línea) sea igual a expresiones regulares que van desde la a a la z y desde la A a la Z, se establece que el valor de la variable i es igual a 1 y menor al número de campos.

```
awk 'BEGIN { FS="[^a-zA-Z]+"} \
{ for (i=1; i<=NF; i++) words[tolower($i)]++ } \
END { for (i in words) print i, words[i] }' /etc/crontab
```

La salida devolverá lo siguiente:

```
 7
bin 3
run 5
etc 4
```

```
sbin 3
bash 1
weekly 1
daily 1
cron 4
usr 2
path 1
shell 1
parts 5
home 1
mailto 1
monthly 1
hourly 1
root 6
```

17. Permisos del Sistema de Ficheros

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

17.1. Introducción

La asignación de permisos de acceso (de lectura, escritura y ejecución) pueden asignarse a través de modos, que son combinaciones de números de tres dígitos (usuario, grupo y resto del mundo) y el mandato **chmod**.

17.2. Notación simbólica

El esquema de notación simbólica se compone de 10 caracteres, donde el primer carácter indica el tipo de fichero:

Valor	Descripción
-	Denota un fichero regular.
d	Denota un directorio.
b	Denota un fichero especial de dispositivos de bloque.
c	Denota un fichero de carácter especial
l	Denota un enlace simbólico.
p	Denota una tubería nombrada (FIFO)
s	Denota un zócalo de dominio (socket)

Cada clase de permisos es representada por un conjunto de tres caracteres. El primer conjunto de caracteres representa la clase del usuario, el segundo conjunto de tres caracteres representa la clase del grupo y el tercer conjunto representa la clase de «otros» (resto del mundo). Cada uno de los tres caracteres representa permisos de lectura, escritura y ejecución, respectivamente y en ese orden.

Ejemplos:

Permisos	Descripción
drwxr-xr-x	Directorio con permiso 755.
crw-rw-r--	Fichero de carácter especial con permiso 664.
srwxrwxr-x	Zócalo con permiso 775.
prw-rw-r--	Tubería (FIFO) con permiso 664.

Permisos	Descripción
-rw-r--r--	Fichero regular con permiso 644.

17.3. Notación octal

La notación octal consiste de valores de tres a cuatro dígitos en base-8. Con la notación octal de tres dígitos cada número representa un componente diferente de permisos a establecer: clase de usuario, clase de grupo y clase de «otros» (resto del mundo), respectivamente. Cada uno de estos dígitos es la suma de sus bits que lo componen (en el sistema numeral binario). Como resultado, bits específicos se añaden a la suma conforme son representados por un numeral:

- El Bit de ejecución añade **1** a la suma.
- El bit de escritura añade **2** a la suma.
- El bit de lectura añade **4** a la suma.

Estos valores nunca producen combinaciones ambiguas y cada una representa un conjunto de permisos específicos. De modo tal puede considerarse la siguiente tabla:

Valor	Permiso	Decripción
0	-	Nada
1	x	Ejecución
2	w	Escritura
3	wx	Escritura y ejecución
4	r	Lectura
5	rx	Lectura y Ejecución
6	rw	Lectura y Escritura
7	rwx	Lectura, Escritura y Ejecución

Nota: 3 (wx) es el resultado de 1+2 (w+x). 5 (rx) es el resultado de 4+1 (r+x). 6 (rw) es el resultado de 4+2 (r+w). 7 (rwx) es el resultado de 4+3 (r+xw).

17.3.1. Permisos adicionales

Hay una forma de cuatro dígitos. Bajo este esquema el estándar de tres dígitos descrito arriba se convierte en los últimos tres dígitos del conjunto. El primer dígito representa permisos adicionales. En sistemas y sustento lógico donde no puede ser omitido este primer dígito del conjunto de cuatro, se establece cero como valor de éste.

El primer dígito del conjunto de cuatro es también la suma de sus bits que le componen:

1. El bit pegajoso (sticky bit) añade **1** al total de la suma.
2. El bit setgid añade **2** al total de la suma.
3. El bit setuid añade **4** al total de la suma.

Lo que hace el permiso SUID o bit setuid es que cuando se ha establecido la ejecución, el proceso resultante asumirá la identidad del usuario dado en la clase de usuario (propietario del elemento).

De la misma manera que el anterior, lo que hace el permiso SGID o bit setgid es que cuando se ha establecido la ejecución, el proceso resultante asumirá la identidad del grupo dado en la clase de grupo (propietario del elemento). Cuando setgid ha sido aplicado a un directorio, todos los nuevos ficheros creados debajo de este directorio heredarán el grupo propietario de este mismo directorio. Cuando no se ha establecido setgid, el comportamiento predefinido es asignar el grupo del usuario al crear nuevos elementos.

El bit pegajoso (sticky bit) significa que un usuario sólo podrá modificar y eliminar ficheros y directorios subordinados dentro de un directorio que le pertenezca. En ausencia del bit pegajoso (sticky bit) se aplican las reglas generales y el derecho de acceso de escritura por si solo permite al usuario crear, modificar y eliminar ficheros y directorios subordinados dentro de un directorio. Los directorios a los cuales se les ha establecido bit pegajoso restringen las modificaciones de los usuarios a sólo adjuntar contenido, manteniendo control total sobre sus propios ficheros y pueden crear nuevos ficheros; sin embargo, sólo pueden adjuntar o añadir contenido a los ficheros de otros usuarios. El bit pegajoso (sticky bit) es utilizado en directorios como **/tmp** y **/var/spool/mail**.

De modo tal puede considerarse la siguiente tabla:

Valor	Permiso	Descripción
1	`--- --- --`**`t`**	bit pegajoso
2	`--- --`**`s`**` ---`	bit setgid
3	`--- --`**`s`**` --`**`t`**	bit pegajoso + bit setgid
4	`--`**`s`**` --- ---`	bit setuid
5	`--`**`s`**` --- --`**`t`**	bit setuid + bit pegajoso
6	`--`**`s`**` --`**`s`**` ---`	bit setuid + bit setgid
7	`--`**`s`**` --`**`s`**` --`**`t`**	bit setuid + bit setgid + bit pegajoso

Cuando un fichero no tiene permisos de ejecución en alguna de las clases y le es asignado un permiso especial, éste se representa con una letra mayúscula.

Permiso	Clase	Ejecuta	No ejecuta
setuid	Usuario	s	S
setgid	Grupo	s	S
pegajoso (sticky)	Otros	t	T

17.4. Ejemplos

17.4.1. Ejemplos de permisos regulares

Permiso	Clase de Usuario	Clase de Grupo	Clase de Otros
0400	r--	---	---
0440	r--	r--	---

Permiso	Clase de Usuario	Clase de Grupo	Clase de Otros
0444	r--	r--	r--
0500	r-x	---	---
0550	r-x	r-x	---
0555	r-x	r-x	r-x
0644	rw-	r--	r--
0664	rw-	rw-	r--
0666	rw-	rw-	rw-
0700	rwx	---	---
0711	rwx	--x	--x
0707	rwx	---	rwx
0750	rwx	r-x	---
0755	rwx	r-x	r-x
0777	rwx	rwx	rwx

17.4.2. Ejemplos de permisos especiales

Permiso	Clase de Usuario	Clase de Grupo	Clase de Otros
1644	rw-	r--	r-**T**
2644	rw-	r-**S**	r--
3644	rw-	r-**S**	r-**T**
4644	rw**S**	r--	r--
5644	rw**S**	r--	r-**T**
6644	rw**S**	r-**S**	r--
7644	rw**S**	r-**S**	r-**T**
1777	rwx	rwx	rw**t**
2755	rwx	r-**s**	r-x
3755	rwx	r-**s**	r-**t**
4755	rw**s**	r-x	r-x
5755	rw**s**	r-x	r-**t**
6755	rw**s**	r-**s**	r-x
7755	rw**s**	r-**s**	r-**t**

17.5. Uso de chmod

```
chmod [opciones] modo fichero
```

Ejemplo:

```
mkdir -p ~/tmp/
touch ~/tmp/algo.txt
ls -l ~/tmp/algo.txt
chmod 755 ~/tmp/algo.txt
ls -l ~/tmp/algo.txt
```

Lo anterior debe arrojar una salida similar a la siguiente:

```
[fulano@localhost ~]$ mkdir -p ~/tmp/
[fulano@localhost ~]$ touch ~/tmp/algo.txt
[fulano@localhost ~]$ ls -l ~/tmp/algo.txt
-rw-rw-r-- 1 fulano fulano 0 mar 2 15:09 /home/fulano/tmp/algo.txt
[fulano@localhost ~]$ chmod 755 ~/tmp/algo.txt
[fulano@localhost ~]$ ls -l ~/tmp/algo.txt
-rwxr-xr-x 1 fulano fulano 0 mar 2 15:09 /home/fulano/tmp/algo.txt
[fulano@localhost ~]$
```

17.5.1. Opciones de chmod

Opción	**Descripción**
-R	Cambia permisos de forma descendente en un directorio dado. Es la única opción de los estándares POSIX
-c	Muestra que ficheros han cambiado recientemente en una ubicación dada
-f	No muestra errores de ficheros o directorios que no se hayan podido cambiar
-v	Descripción detallada de los mensajes generados por el proceso

17.5.2. El mandato chmod y los enlaces simbólicos

El mandato **chmod** jamás cambia los permisos de enlaces simbólicos; sin embargo no representa un problema en virtud de que jamás se utilizan los permisos de los enlaces simbólicos. Si se aplica el mandato **chmod** sobre un enlace simbólico, se cambiará el permiso del fichero o directorio hacia el cual apunta. Cuando se aplica **chmod** de forma descendente en un directorio, éste ignora los enlaces simbólicos que pudiera encontrar en el recorrido.

18. Cómo utilizar el mandato chattr.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

18.1. Introducción.

18.1.1. Acerca del mandato chattr.

El mandato **chattr** se utiliza para cambiar los atributos de los sistemas de ficheros **ext2** y **ext3**. Desde cierto punto de vista, es análogo al mandato **chmod**, pero con diferente sintaxis y opciones. Utilizado adecuadamente, dificulta las acciones en el sistema de ficheros por parte de un intruso que haya logrado suficientes privilegios en un sistema.

En la mayoría de los casos, cuando un intruso consigue suficientes privilegios en un sistema, lo primero que hará será eliminar los registros de sus actividades modificando estructuras de los ficheros de bitácoras del sistema y otros componentes. Utilizar el mandato **chattr** ciertamente no es obstáculo para un usuario experto, pero, afortunadamente, la gran mayoría de los intrusos potenciales no suelen ser expertos en GNU/Linux o Unix, dependiendo enormemente de diversos programas o guiones (los denominados *rootkits* y *zappers*) para eliminar aquello que permita descubrir sus actividades.

Utilizar el mandato **chattr**, incluido en el paquete **e2fsprogs**, que se instala de forma predeterminada en todas las distribuciones de GNU/Linux por, tratarse de un componente esencial, hace más difícil borrar o alterar bitácoras, ficheros de configuración y componentes del sistema. Theodore Ts'o es el desarrollador y quien se encarga de mantener **e2fsprogs**, mismo que se distribuye bajo los términos de la licencia **GNU/GPL**, e incluye otras herramientas como e2fsck, e2label, fsck.ext2, fsck.ext3, mkfs.ext2, mkfs.ext3, tune2fs y dumpe2fs, entre otras.

URL: http://e2fsprogs.sourceforge.net/

18.2. Opciones.

-R	Cambia recursivamente los atributos de directorios y sus contenidos. Los enlaces simbólicos que se encuentren, son ignorado
-V	Salida de **charttr** más descriptiva, mostrando además la versión del programa.
-v	Ver el número de versión del programa.

18.3. Operadores.

+	Hace que se añadan los atributos especificados a los atributos existentes de un fichero.
-	Hace que se eliminen los atributos especificados de los atributos existentes de un fichero
=	Hace que solamente haya los atributos especificados.

18.4. Atributos.

A	Establece que la fecha del último acceso (atime) no se modifica.
a	Establece que el fichero solo se puede abrir en modo de adjuntar para escritura.
c	Establece que el fichero es comprimido automáticamente en el disco por el núcleo del sistema operativo. Al realizar lectura de este fichero, se descomprimen los datos. La escritura de dicho fichero comprime los datos antes de almacenarlos en el disco.
D	Cuando se trata de un directorio, establece que los datos se escriben de forma sincrónica en el disco. Es decir, los datos se escriben inmediatamente en lugar de esperar la operación correspondiente del sistema operativo. Es equivalente a la opción **dirsync** del mandato **mount**, pero aplicada a un subconjunto de ficheros.
d	Establece que el fichero no sea candidato para respaldo al utilizar la herramienta **dump**.
i	Establece que el fichero será inmutable. Es decir, no puede ser eliminado, ni renombrado, no se pueden apuntar enlaces simbólicos, ni escribir datos en el fichero.
j	En los sistemas de ficheros ext3, cuando se montan con las opciones **data=ordered** o **data=writeback**, se establece que el fichero será escrito en el registro por diario (**Journal**). Si el sistema de ficheros se monta con la opción **data=journal** (opción predeterminada), todo el sistema de ficheros se escribe en el registro por diario y por lo tanto el atributo no tiene efecto.
s	Cuando un fichero tiene este atributo, los bloques utilizados en el disco duro son escritos con ceros, de modo que los datos no se puedan recuperar por medio alguno. Es la forma más segura de eliminar datos.
S	Cuando el fichero tiene este atributo, sus cambios son escritos de forma sincrónica en el disco duro. Es decir, los datos se escriben inmediatamente en lugar de esperar la operación correspondiente del sistema operativo. Es equivalente a la opción **sync** del mandato **mount**.

u	Cuando un fichero con este atributo es eliminado, sus contenidos son guardados permitiendo recuperar el fichero con herramientas para tal fin.

18.5. Utilización.

```
chattr [-RV] +-=[AacDdijsSu] [-v versión] ficheros
```

18.5.1. Ejemplos.

el siguiente mandato agrega el atributo inmutable al fichero algo.txt..

```
chattr +i algo.txt
```

El siguiente mandato elimina el atributo inmutable al fichero algo.txt.

```
chattr -i algo.txt
```

El siguiente mandato agrega el modo de solo adjuntar para escritura al fichero algo.txt.

```
chattr +a algo.txt
```

El siguiente mandato elimina el modo de solo adjuntar para escritura al fichero algo.txt.

```
chattr -a algo.txt
```

El siguiente mandato establece que el fichero algo.txt solo tendrá los atributos **a**, **A**, **s** y **S**.

```
chattr =aAsS algo.txt
```

El siguiente mandato lista los atributos del fichero algo.txt.

```
lsattr algo.txt
```

19. Creando depósitos yum

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

19.1. Introducción.

Yum es una herramienta sumamente útil para el manejo de paquetería RPM. Aprender a crear en el disco duro las bases de datos para los depósitos yum resulta práctico puesto que no habrá necesidad de recurrir hacia los depósitos localizados en servidores en Internet y consumir innecesariamente ancho de banda en el proceso.

19.2. Procedimientos

Primero se deben generar los directorios que alojarán los depósitos. Uno para la paquetería incluida en los discos de instalación y otro para las actualizaciones:

```
mkdir -p /var/ftp/pub/os
mkdir -p /var/ftp/pub/updates
```

Tome todos los discos de instalación y copie íntegramente su contenido hacia el interior del directorio localizado en la ruta /var/ftp/pub/os/ con el siguiente procedimiento:

```
mount /media/cdrom
cp -Rf /media/cdrom/* /var/ftp/pub/os/
eject
```

Del mismo modo, si dispone del CD correspondiente, copie (o bien descargue) todas las actualizaciones dentro del directorio localizado en la ruta /var/ftp/pub/updates/ con el siguiente procedimiento:

```
mount /media/cdrom
cp -Rf /media/cdrom/* /var/ftp/pub/updates/
eject
```

Una vez copiado todo al disco duro, hay que instalar el paquete createrepo, incluido en los discos de instalación de CentOS y White Box Enterprise Linux.

```
yum -y install createrepo
```

Una vez instalado, sólo basta ejecutar **createrepo** sobre cada directorio a fin de generar los depósitos yum:

```
createrepo /var/ftp/pub/os/
createrepo /var/ftp/pub/updates/
```

Se puede acceder localmente a los depósitos generados **utilizando las siguientes líneas** como contenido del fichero ***.repo** localizado dentro de **/etc/yum.repos.d/**, en lugar de las líneas que apuntan hacia servidores en Internet:

```
[base]
name=Enterprise Linux $releasever - $basearch - base
baseurl=file:///var/ftp/pub/os/
gpgcheck=1
enabled=1

[updates-released]
name=Enterprise Linux $releasever - $basearch - Updates Released
baseurl=file:///var/ftp/pub/updates/
gpgcheck=1
enabled=1
```

Si se desea acceder a estos mismo depósitos utilizando el servicio FTP, y **suponiendo** que el servidor utilizaría 192.168.1.1 como dirección IP, las máquinas cliente deben utilizar lo siguiente:

```
[base]
name=Enterprise Linux $releasever - $basearch - base
baseurl=ftp://192.168.1.1/pub/os/
gpgcheck=1
enabled=1

[updates-released]
name=Enterprise Linux $releasever - $basearch - Updates Released
baseurl=ftp://192.168.1.1/pub/updates/
gpgcheck=1
enabled=1
```

Antes de utilizar la opción **gpgcheck=1**, se deberán importar las llaves públicas GPG que están en el disco 1 de instalación del sistema.

```
mount /media/cdrom
rpm --import /media/cdrom/*KEY*
```

Si creó un depósito con el disco de extras de curso, la llave pública de Alcance Libre se encuentra en el directorio raíz del CD.

Si utiliza Red Hat™ Enterprise Linux 3, CentOS 3.0 o White Box Enterprise Linux 3, se utiliza **yum-arch** en lugar de createrepo, y **/mnt/cdrom** en lugar de /media/cdrom.

White Box Enterprise Linux 4 no incluye yum por defecto, por lo que hay que instalarlo manualmente desde los discos de instalación.

20. Uso de yum para instalar y desinstalar paquetería y actualizar sistema

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

20.1. Introducción

Actualizar el sistema aplicando los más recientes parches de seguridad y correctivos al sistema operativo no es tan difícil como muchos suponen, ni tampoco tiene que ser un infierno de dependencias entre paquetes RPM como algunos argumentan. La realidad de las cosas es que es mucho muy simple y sólo requiere de un buen ancho de banda, o bien, de muchísima paciencia. A continuación presentamos los procedimientos para utilizar yum y **realizar fácilmente** lo que algunos denominan como «*horrible, difícil y complicado*».

Los procedimientos son tan simples que realmente no hay muchas excusas para no aplicar los parches de seguridad y correctivos al sistema.

20.2. Procedimientos

20.2.1. Actualizar sistema

Actualización del sistema con todas las dependencias que sean necesarias:

```
yum update
```

20.2.2. Búsquedas

Realizar una búsqueda de algún paquete o término en la base de datos en alguno de los depósitos yum configurados en el sistema:

```
yum search cualquier-paquete
```

Ejemplo:

```
yum search httpd
```

20.2.3. Consulta de información

Consultar la información contenida en un paquete en particular:

```
yum info cualquier-paquete
```

Ejemplo:

```
yum info httpd
```

20.2.4. Instalación de paquetes

Instalación de paquetería con resolución automática de dependencias:

```
yum install cualquier-paquete
```

Ejemplo:

```
yum install httpd
```

20.2.5. Desinstalación de paquetes

Desinstalación de paquetes junto con todo aquello que dependa de los mismos:

```
yum remove cualquier-paquete
```

Ejemplo:

```
yum remove httpd
```

20.2.5.1. Algunos paquetes que se pueden desinstalar del sistema.

Los siguientes paquetes pueden ser desinstalados del sistema de manera segura junto con todo aquello que dependa de éstos:

1. pcmcia-cs (kernel-pcmcia-cs): requerido sólo en computadoras portátiles para el soporte de PCMCIA.
2. mdadm: requerido sólo para arreglos RAID.
3. autofs: servicio de auto-montado de unidades de disco.
4. ypserv: servidor NIS, utilizado principalmente como servidor de autenticación.
5. ypbind, yp-tools: herramientas necesarias para autenticar contra un servidor NIS (ypserv)
6. hwcrypto: bibliotecas y herramientas para interactuar con aceleradores criptográficos de sustento físico (hardware).
7. vnc-server: servidor VNC
8. irda-utils: herramientas y soporte para dispositivos infrarrojos.

Ejecute lo siguiente para desinstalar los paquetes anteriormente mencionados:

```
yum -y remove pcmcia-cs mdadm autofs ypserv ypbind yp-tools hwcrypto
vnc-server irda-utils
```

20.2.6. Listado de paquetes

Lo siguiente listará todos los paquetes disponibles en la base de datos yum y que pueden instalarse:

```
yum list available | less
```

Lo siguiente listará todos los paquetes instalados en el sistema:

```
yum list installed |less
```

Lo siguiente listará todos los paquetes instalados en el sistema y que pueden (y deben) actualizarse:

```
yum list updates | less
```

20.2.7. Limpieza del sistema

Yum proporciona como resultado de su uso cabeceras y paquetes RPM almacenados en el interior del directorio localizado en la ruta **/var/cache/yum/**. Particularmente los paquetes RPM que se han instalado pueden ocupar mucho espacio y, es por tal motivo, que conviene eliminarlos una vez que ya no tienen utilidad. Igualmente conviene hacer lo mismo con las cabeceras viejas de paquetes que ya no se encuentran en la base de datos. A fin de realizar la limpieza correspondiente, puede ejecutarse lo siguiente:

```
yum clean all
```

21. Cómo utilizar RPM

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

21.1. Introducción.

21.1.1. Acerca de RPM.

RPM Package Manager, anteriormente conocido como **R**ed Hat **P**ackage **M**anager y que es más conocido por su nombre abreviado **RPM**, es un sistema de gestión de paquetería para distribuciones de GNU/Linux y que está considerado en la Base Estándar para Linux (**L**inux **S**tandard **B**ase o **LSB**), que es un proyecto cuyo objetivo es desarrollar y promover estándares para mejorar la compatibilidad entre las distribuciones de GNU/Linux para permitir a las aplicaciones ser utilizadas en cualquier distribución.

RPM fue originalmente desarrollado por **Red Hat** para su distribución de GNU/Linux, y ha sido llevado hacia otra distribuciones de Linux y sistemas operativos.

RPM utiliza una base de datos que se almacena en **/var/lib/rpm**, la cual contiene toda la meta-información de todos los paquetes que son instalados en el sistema y que es utilizada para dar seguimiento a todos los componentes que son instalados. Esto permite instalar y desinstalar limpiamente todo tipo de aplicaciones, bibliotecas, herramientas y programas y gestionar sus dependencias exactas.

21.2. Procedimientos.

RPM viene instalado de modo predeterminado en **Red Hat Enterprise Linux**, **Fedora**, **CentOS**, **White Box Enterprise Linux**, **SuSE Linux**, **OpenSuSE**, **Mandriva** y distribuciones derivadas de estas.

21.2.1. Reconstrucción de la base de datos de RPM.

Hay ciertos escenarios en donde se puede corromper la base de datos de **RPM**. Ésta se puede reconstruir fácilmente utilizando el siguiente mandato:

```
rpm --rebuilddb
```

21.2.2. Consulta de paquetería instalada en el sistema.

Si se desea conocer si está instalado un paquete en particular, se utiliza el mandato **rpm** con la opción **-q**, que realiza una consulta (*query*) en la base de datos por un nombre de paquete en particular. En el siguiente mandato, donde como ejemplo se preguntará a **RPM** si está instalado el paquete **traceroute**:

```
rpm -q traceroute
```

Lo anterior debe devolver una salida similar a la siguiente:

```
traceroute-2.0.1-2.el5
```

Si se desea conocer que es lo que información incluye el paquete **traceroute**, se utiliza el mandato **rpm** con las opciones **-qi**, para hacer la consulta y solicitar información del paquete (*query info*). En el siguiente ejemplo se consulta al mandato **rpm** por la información del paquete **traceroute**:

```
rpm -qi traceroute
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Name        : traceroute                   Relocations: (not relocatable)
Version     : 2.0.1                             Vendor: CentOS
Release     : 2.el5                          Build Date: sáb 06 ene 2007 04:02:13 CST
Install Date: mié 30 abr 2008 11:46:09 CDT      Build Host: builder5.centos.org
Group       : Applications/Internet         Source RPM: traceroute-2.0.1-2.el5.src.rpm
Size        : 59726                            License: GPL
Signature   : DSA/SHA1, mar 03 abr 2007 19:28:12 CDT, Key ID a8a447dce8562897
URL         : http://dmitry.butskoy.name/traceroute
Summary     : Traces the route taken by packets over an IPv4/IPv6 network
Description :
The traceroute utility displays the route used by IP packets on their
way to a specified network (or Internet) host.  Traceroute displays
the IP number and host name (if possible) of the machines along the
route taken by the packets.  Traceroute is used as a network debugging
tool.  If you're having network connectivity problems, traceroute will
show you where the trouble is coming from along the route.
Install traceroute if you need a tool for diagnosing network connectivity
problems.
```

Puede consultarse qué componentes forman parte del paquete utilizando el mandato **rpm** con las opciones **-ql**, donde se realiza una consulta listando los componentes que lo integran (*query list*). Si se desea conocer que componentes instaló el paquete **traceroute**, utilice el siguiente mandato:

```
rpm -ql traceroute
```

Lo anterior debe devolver una salida similar a la siguiente:

```
/bin/traceroute
/bin/traceroute
/bin/traceroute6
/bin/tracert
/usr/share/doc/traceroute-2.0.1
/usr/share/doc/traceroute-2.0.1/COPYING
/usr/share/doc/traceroute-2.0.1/CREDITS
/usr/share/doc/traceroute-2.0.1/README
```

```
/usr/share/doc/traceroute-2.0.1/TODO
/usr/share/man/man8/traceroute.8.gz
```

Si se desea consultar a cual paquete pertenece un elemento instalado en el sistema, se utiliza el mandato **rpm** con las opciones **-qf**, que realizan una consulta por un fichero en el sistema de archivos (*query file*). En el siguiente ejemplo se consultará a la mandato rpm a que paquete pertenece el fichero **/etc/crontab**:

```
rpm -qf /etc/crontab
```

Lo anterior debe devolver una salida similar a la siguiente:

```
crontabs-1.10-8
```

Si desea consultar la lista completa de paquetes instalados en el sistema, utilice el siguiente mandato, donde **-qa** significa consultar todo (*query all*):

```
rpm -qa
```

Debido a que lo anterior devuelve una lista demasiado grande para poderla visualizar con comodidad, puede utilizarse **less** o **more** como subrutina:

```
rpm -qa |less
```

Si se quiere localizar un paquete o paquetes en particular, se puede utilizar el mandato **rpm** con las opciones **-qa** y utilizar **grep** como subrutina. En el siguiente ejemplo se hace una consulta donde se quiere conocer que paquetes están instalado en el sistema y que incluyan la cadena **php** en el nombre.

```
rpm -qa |grep php
```

Lo anterior pudiera devolver una salida similar a la siguiente:

```
php-5.1.6-15.el5
php-mbstring-5.1.6-15.el5
php-pear-1.4.9-4
php-ldap-5.1.6-15.el5
php-cli-5.1.6-15.el5
php-mysql-5.1.6-15.el5
php-odbc-5.1.6-15.el5
php-common-5.1.6-15.el5
php-pdo-5.1.6-15.el5
```

Si se quiere revisar en orden cronológico, de más nuevos a más antiguos, que paquetes están instalados, se puede agregar a **-qa** la opción **--last**, y **less** o **more** como subrutina para visualizar con comodidad la salida.

```
rpm -qa --last|less
```

Lo anterior devuelve una salida extensa dentro con **less** como visor. Pulse la teclas de **arriba** (↑) y **abajo** (↓) o **Av. Pág.** y **Reg. Pág.** para desplazarse en la lista. Pulse la tecla **q** para salir.

Si se quiere verificar si los componentes instalados por un paquete **RPM** han sido modificados o alterados o eliminados, se puede utilizar el mandato **rpm** con la opción **-V**, la cual realiza una verificación de la integridad de los componentes de acuerdo a las firmas digitales de cada componente (MD5SUM o suma MD5). En el siguiente ejemplo se verificara si el paquete **crontabs** ha sido alterado:

```
rpm -V crontabs
```

Si algún componente fue modificado, puede devolverse una salida similar a la siguiente, donde el fichero **/etc/crontab** fue modificado tras su instalación:

```
S.5....T c /etc/crontab
```

Si se desea realizar una verificación de todos los componentes del sistema, se puede utilizar el mandato rpm con las opciones **-Va**, que hace una consulta, especifica todos los paquetes, y solicita se verifique si hubo cambios (*query all Verify*).

```
rpm -Va
```

Lo anterior puede devolver una salida muy extensa, pero sin duda alguna mostrará todos los componentes que fueron modificados o alterados o eliminados tras la instalación del paquete al que pertenecen. Un ejemplo de una salida común sería:

```
.......T c /etc/pki/nssdb/cert8.db
.......T c /etc/pki/nssdb/key3.db
..5....T c /etc/pki/nssdb/secmod.db
S.5....T c /etc/crontab
.......T c /etc/inittab
S.5....T c /etc/rc.d/rc.local
S.5....T c /etc/mail/access
S.5....T c /etc/mail/local-host-names
S.5....T c /etc/mail/sendmail.cf
S.5....T c /etc/mail/sendmail.mc
```

21.2.3. Instalación de paquetes.

La mayoría de los distribuidores serios de equipamiento lógico en formato RPM siempre utilizan una firma digital PG/GnuPG para garantizar que éstos son confiables y como un método de evitar que paquetes alterados pasen por el usuario administrador del sistema y sistemas de gestión de paquetes como yum, up2date, Yast, Pup, etc., sin ser detectados. Las firmas digitales de los responsables de la distribución siempre incluyen firmas digitales en el disco de instalación o bien en alguna parte del sistema de archivos. En el caso de **CentOS** y **Red Hat Enterprise**, las firmas digitales están en /usr/share/doc/rpm-*/ o bien **/usr/share/rhn/**. Algunos distribuidores pueden tener estas firmas en algún servidor HTTP o FTP. Para importar una firma digital, se utiliza el mandato **rpm** con la opción **--import**. Para ejemplificar, realice el siguiente procedimiento:

```
rpm --import http://www.alcancelibre.org/al/AL-RPM-KEY
```

Lo anterior importa la firma digital de **Alcance Libre** y permitirá detectar si un paquete de Alcance Libre fue alterado o está corrupto o si fue dañado. Si se utiliza **yum** para gestionar la paquetería, éste de modo predeterminado impide instalar paquetes que si estos carecen de una firma digital que esté instalada en la base de datos de **RPM**.

Cuando se desee instalar un paquete con extensión ***.rpm**, siempre es conveniente revisar dicho paquete. Hay varias formas de verificar su contenido antes de proceder a instalado. Para fines demostrativos, ingrese hacia http://www.alcancelibre.org/al/webapps/ y descarge el paquete **tnef**.

Una vez descargado el paquete **tnef**, se puede verificar la información de dicho paquete utilizando el mandato **rpm** con las opciones **-qp**, para realizar la consulta especificando que se trata de un paquete **RPM** (*query package*), y la opción -i, para solicitar información.

```
rpm -qpi tnef-1.2.3.1-1.1.el5.al.i386.rpm
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Name        : tnef                         Relocations: /usr
Version     : 1.2.3.1                           Vendor: Alcance Libre, Inc.
Release     : 1.1.el5.al                    Build Date: mié 02 may 2007 14:06:59 CDT
Install Date: (not installed)               Build Host: localhost.localdomain
Group       : Mail/Encoders                 Source RPM: tnef-1.2.3.1-1.1.el5.al.src.rpm
Size        : 134695                           License: GPL
Signature   : DSA/SHA1, mié 02 may 2007 14:07:00 CDT, Key ID 91004df87c080b33
Packager    : Joel Barrios <http://joel-barrios.blogspot.com/>
URL         : http://tnef.sourceforge.net
Summary     : Decodes MS-TNEF attachments.
Description :
TNEF is a program for unpacking MIME attachments of type
"application/ms-tnef". This is a Microsoft only attachment.
Due to the proliferation of Microsoft Outlook and Exchange mail servers,
more and more mail is encapsulated into this format.
The TNEF program allows one to unpack the attachments which were
encapsulated into the TNEF attachment.  Thus alleviating the need to use
Microsoft Outlook to view the attachment.
```

Si se desea conocer que componentes va a instalar un paquete RPM en particular, se puede utilizar el mandato **rpm** con las opciones **-qpl**, para realizar la consulta, especificar que se trata de un paquete **RPM** y para solicitar la lista de componentes (*query package list*). En el siguiente ejemplo se realiza esta consulta contra el paquete **tnef-1.2.3.1-1.1.el5.al.i386.rpm**:

```
rpm -qpl tnef-1.2.3.1-1.1.el5.al.i386.rpm
```

Lo anterior debe devolver una salida similar a la siguiente:

```
/usr/bin/tnef
/usr/man/man1/tnef.1.gz
/usr/share/doc/tnef-1.2.3.1
/usr/share/doc/tnef-1.2.3.1/AUTHORS
/usr/share/doc/tnef-1.2.3.1/BUGS
/usr/share/doc/tnef-1.2.3.1/COPYING
/usr/share/doc/tnef-1.2.3.1/ChangeLog
/usr/share/doc/tnef-1.2.3.1/NEWS
/usr/share/doc/tnef-1.2.3.1/README
/usr/share/doc/tnef-1.2.3.1/TODO
```

Para verificar si las firmas digitales de un paquete **RPM** son las mismas y el paquete no ha sido alterado, se puede utilizar el mandato **rpm** con las opción **-K**, que solicita verificar firmas digitales de un paquete **RPM** (*Keys*):

```
rpm -K tnef-1.2.3.1-1.1.el5.al.i386.rpm
```

Si el paquete está integro, debe devolver una salida similar a la siguiente:

```
tnef-1.2.3.1-1.1.el5.al.i386.rpm: (sha1) dsa sha1 md5 gpg OK
```

Si el paquete RPM fue dañado, alterado o está corrupto, puede devolver una salida similar a la siguiente:

```
tnef-1.2.3.1-1.1.el5.al.i386.rpm: (sha1) dsa sha1 MD5 GPG NOT OK
```

Para instalar un paquete, se utiliza el mandato **rpm** con las opciones **-ivh**, que significa instalar, devolver una salida descriptiva y mostrar una barra de progreso (*install verbose hash*). Si el paquete no hace conflicto con otro y/o no sobreescribe componentes de otro paquete, se procederá a instalar el mismo. En el siguiente ejemplo se instalará el paquete **tnef-1.2.3.1-1.1.el5.al.i386.rpm**:

```
rpm -ivh tnef-1.2.3.1-1.1.el5.al.i386.rpm
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Preparing...                ########################################### [100%]
   1:tnef                   ########################################### [100%]
```

Si hubiera una versión de éste paquete instalada en el sistema, **rpm -ivh** no realizará la instalación y devolverá un mensaje respecto a que la está instalado dicho paquete. Repita el siguiente mandato:

```
rpm -ivh tnef-1.2.3.1-1.1.el5.al.i386.rpm
```

Al ya haber sido instalado el paquete **tnef**, el sistema deberá devolver una salida similar a la siguiente:

```
Preparing...                ########################################### [100%]
        package tnef-1.2.3.1-1.1.el5.al is already installed
```

Hay circunstancias y escenarios donde se requiere reinstalar de nuevo el paquete. Para lograr esto se agrega la opción **--force** para forzar la reinstalación de un paquete. En el siguiente ejemplo se solicita al mandato **rpm** forzar la reinstalación de el paquete tnef-1.2.3.1-1.1.el5.al.i386.rpm:

```
rpm -ivh --force tnef-1.2.3.1-1.1.el5.al.i386.rpm
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Preparing...                ########################################### [100%]
   1:tnef                   ########################################### [100%]
```

Para verificar las dependencias de un paquete descargado, se utiliza el mandato **rpm** con las opciones **-qp** y **--requires**, la cual consulta las dependencias del paquete. En el siguiente ejemplo, se ha descargado el paquete **joomla-1.0.15-2.9.el5.al.noarch.rpm** desde http://www.alcancelibre.org/al/webapps/, y se procede a consultar sus dependencias:

```
rpm -qp --requires joomla-1.0.15-2.9.el5.al.noarch.rpm
```

Lo anterior debe devolver una salida similar a la siguiente:

```
config(joomla) = 1.0.15-2.9.el5.al
httpd
php >= 5
php-mysql
php-xml
rpmlib(CompressedFileNames) <= 3.0.4-1
rpmlib(PayloadFilesHavePrefix) <= 4.0-1
```

Pueden hacerse consultas a la inversa de lo anterior, es decir, consultar al mandato **rpm** que paquete provee alguna dependencia en particular. En el siguiente ejemplo se solicitará al mandato **rpm** que paquete provee la dependencia **php**.

```
rpm -q --whatprovides php
```

Lo anterior debe devolver una salida similar a la siguiente:

```
php-5.1.6-15.el5
```

También puede consultarse qué requiere de un paquete o componente en particular. En el siguiente ejemplo se consulta al mandato **rpm** que paquetes requieren al paquete **httpd**.

```
rpm -q --whatrequires httpd
```

Lo anterior puede devolver una salida similar a la siguiente:

```
system-config-httpd-1.3.3.1-1.el5
squirrelmail-1.4.8-4.0.1.el5.centos.2
squirrelmail-1.4.8-4.0.1.el5.centos.2
gnome-user-share-0.10-6.el5
```

De ser necesario, se puede incluso hacer consultas respecto a ficheros (como bibliotecas compartidas) para conocer que paquetes dependen de éstos. En el siguiente ejemplo se consulta la mandato **rpm** que paquetes requieren a la biblioteca **libbz2.so.1**:

```
rpm -q --whatrequires libbz2.so.1
```

Lo anterior debe devolver una salida similar a la siguiente, y que consiste en una lista de paquetes **RPM** instalados en el sistema:

```
bzip2-libs-1.0.3-3
bzip2-1.0.3-3
python-2.4.3-19.el5
gnupg-1.4.5-13
elinks-0.11.1-5.1.0.1.el5
rpm-4.4.2-47.el5
rpm-libs-4.4.2-47.el5
rpm-python-4.4.2-47.el5
```

```
gnome-vfs2-2.16.2-4.el5
libgsf-1.14.1-6.1
php-cli-5.1.6-15.el5
php-5.1.6-15.el5
kdelibs-3.5.4-13.el5.centos
ImageMagick-6.2.8.0-4.el5_1.1
```

Para instalar o actualizar un paquete, se utiliza el mandato **rpm** con las opciones -Uvh, que significa instalar o actualizar, devolver una salida descriptiva y mostrar una barra de progreso (*update verbose hash*), y se procede a instalar y/o actualizar el mismo:

```
rpm -Uvh joomla-1.0.15-2.9.el5.al.noarch.rpm
```

Si falta alguna de las dependencias, el sistema devolverá una salida similar a la siguiente:

```
error: Failed dependencies:
        php-xml is needed by joomla-1.0.15-2.9.el5.al.noarch
```

Evidentemente se debe instalar el paquete **php-xm**l para poder instalar el paquete **joomla-1.0.15-2.9.el5.al.noarch.rpm**. Este puede estar incluido en el disco de instalación o bien estar incluido entre las actualizaciones del sistema.

Si el paquete php-xml hubiera estado instalado (**yum -y install php-xml**), la salida hubiera sido similar a la siguiente:

```
Preparing...                ########################################### [100%]
   1:joomla                 ########################################### [100%]
```

Antes de la aparición de **yum**, este era el *talón de Aquiles* de **RPM**. Actualmente estos problemas se pueden resolver utilizando **yum** en los sistemas que lo incluyen. La forma más práctica de instalar paquetería **RPM** resolviendo dependencias automáticamente es a través de **yum**. En el siguiente ejemplo se realiza el procedimiento de instalación del paquete **joomla-1.0.15-2.9.el5.al.noarch.rpm** utilizando **yum**:

```
yum -y localinstall joomla-1.0.15-2.9.el5.al.noarch.rpm
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Loading "fastestmirror" plugin
Loading "skip-broken" plugin
Loading "installonlyn" plugin
Setting up Local Package Process
Examining joomla-1.0.15-2.9.el5.al.noarch.rpm: joomla - 1.0.15-2.9.el5.al.noarch
Marking joomla-1.0.15-2.9.el5.al.noarch.rpm to be installed
Setting up repositories
Loading mirror speeds from cached hostfile
Reading repository metadata in from local files
Resolving Dependencies
--> Populating transaction set with selected packages. Please wait.
---> Package joomla.noarch 0:1.0.15-2.9.el5.al set to be updated
--> Running transaction check
--> Processing Dependency: php-xml for package: joomla
--> Restarting Dependency Resolution with new changes.
--> Populating transaction set with selected packages. Please wait.
```

```
---> Package php-xml.i386 0:5.1.6-15.el5 set to be updated
--> Running transaction check
Dependencies Resolved
================================================================================
 Package                 Arch       Version          Repository        Size
================================================================================
Installing:
 joomla                  noarch     1.0.15-2.9.el5.al  joomla-1.0.15-
2.9.el5.al.noarch.rpm  6.3 M
Installing for dependencies:
 php-xml                 i386       5.1.6-15.el5     base               93 k
Transaction Summary
================================================================================
Install      2 Package(s)
Update       0 Package(s)
Remove       0 Package(s)
Total download size: 6.4 M
Downloading Packages:
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: php-xml                      ######################### [1/2]
  Installing: joomla                       ######################### [2/2]
Installed: joomla.noarch 0:1.0.15-2.9.el5.al
Dependency Installed: php-xml.i386 0:5.1.6-15.el5
Complete!
```

Algunos paquetes incluyen guiones que ejecutan procesos que pueden ser requeridos previo o posterior a la instalación. Si no se desea que se ejecuten estos guiones, se añade a **rpm -ivh** o **rpm -Uvh** la opción **--noscripts**. En el siguiente ejemplo, se instalará el paquete **joomla-1.0.15-2.9.el5.al.noarch.rpm** sin la ejecución de los guiones que pudieran estar definidos en el paquete **RPM**:

```
rpm -Uvh --noscripts joomla-1.0.15-2.9.el5.al.noarch.rpm
```

21.2.3.1. Recuperación de permisos originales a partir de rpm.

En circunstancias en las cuales ser realizaron cambios en los permisos en el sistema de archivos, es posible volver a dejarlos de acuerdo a los especificados en el paquete **RPM** original utilizando el mandato **rpm** con la opción **--setperms** del siguiente modo:

```
rpm --setperms paquete
```

Vea el permiso de **/usr/bin/passwd** del siguiente modo:

```
ls -l /usr/bin/passwd
```

Lo anterior puede devolver una salida similar a la siguiente:

```
-rwsr-xr-x 1 root root 22984 ene  6  2007 /usr/bin/passwd
```

Cambie el permiso del siguiente modo:

```
chmod 700 /usr/bin/passwd
```

Vuelva a ver el permiso de **/usr/bin/passwd** del siguiente modo:

```
ls -l /usr/bin/passwd
```

Lo anterior debe devolver una salida similar a la siguiente:

```
-rwx------ 1 root root 22984 ene  6  2007 /usr/bin/passwd
```

El fichero **/usr/bin/passwd** pertence al paquete passwd, confirmelo del siguiente modo:

```
rpm -qf /usr/bin/passwd
```

Lo anterior debe devolver una salida similar a la siguiente:

```
passwd-0.73-1
```

Para recuperar de nuevo el permiso original de **/usr/bin/passwd**, utilice lo siguiente:

```
rpm --setperms passwd
```

Vuelva a ver el permiso de **/usr/bin/passwd** del siguiente modo:

```
ls -l /usr/bin/passwd
```

Lo anterior debe devolver una salida similar a la siguiente y que corresponde al permiso original del fichero **/usr/bin/passwd**:

```
-rwsr-xr-x 1 root root 22984 ene  6  2007 /usr/bin/passwd
```

21.2.4. Desinstalación de paquetes.

Para desinstalar paquetería, se utiliza el mandato **rpm** con la opción -e, que se utiliza para eliminar, seguida del nombre del paquete. En el siguiente ejemplo, se solicita al mandato **rpm** desinstalar los paquetes **joomla** y **php-xml**:

```
rpm -e joomla php-xml
```

Si no hay dependencias que lo impidan, el sistema solo devolverá el símbolo de sistema. Si el paquete o alguno de sus componentes fuera dependencia de otro u otros paquetes, el sistema informará que no es posible desinstalar y devolverá la lista de paquetes que lo requieren. En el siguiente ejemplo se tratará de desinstalar el paquete **crontabs**:

```
rpm -q crontabs
```

Como el paquete **crontabs** es requerido por **anacron**, el sistema devolverá una salida similar a la siguiente:

```
error: Failed dependencies:
        crontabs is needed by (installed) anacron-2.3-45.el5.centos.i386
```

Si se desea des instalar cualquier paquete sin importar que otros dependan de este, se puede utilizar agregar la opción **--nodeps**. Esto es contraindicado, y solo debe ser utilizado es situaciones muy particulares o escenarios donde así se requiere. Evite siempre desinstalar paquetes que sean dependencia de otros en el sistema a menos que vaya a reinstalar inmediatamente un paquete que los sustituya.

22. Cómo crear paquetería con rpmbuild

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

22.1. Introducción

Crear paquetería a través de rpmbuild no es tan complicado como algunos suponen. Aunque no se instala de modo predeterminado, rpmbuild es una herramienta que forma parte del paquete rpm-build y que se incluye en la mayoría de las distribuciones actuales que utilizan paquetería en formato RPM.

Este documento mostrará los procedimientos para:

- Generar una clave GnuPG para firmar digitalmente los paquetes creados.
- Configuración y creación de una jaula para rpmbuild.
- Creación de ficheros *.spec.
- Uso del mandato rpmbuild.

22.2. Instalación del sustento lógico necesario

Es indispensable contar con la paquetería de desarrollo mínima necesaria instalada en el sistema. Lamentablemente no hay recetas mágicas. Si se pretende crear paquetería a partir de códigos fuente es necesario estar familiarizado con las bibliotecas compartidas necesarias, cabeceras de desarrollo, compiladores y otras herramientas de desarrollo relacionadas o requeridas por un sustento lógico en particular. Un conjunto mínimo sería el siguiente:

- Gcc: compilador.
- glibc-devel: bibliotecas de desarrollo para C.
- automake: generador de ficheros Makefile.
- autoconf: herramienta para configuración de códigos fuente y ficheros Makefile.
- rpm-build y rpm-devel.
- gnupg
- Gpgme y seahorse: **herramientas incluidas en LPT Desktop** que se utilizarán en los procedimientos de este documento para generar la clave utilizada para firmar digitalmente los paquetes rpm resultantes.
- Si va a crear paquetería para GNOME, necesitará por lo menos lo siguiente, con todo lo que dependa de éste: glib2-devel, atk-devel, pango-devel, gtk2-devel, libbonoboui-devel, libgnomeui-devel, gnome-vfs2-devel, libwnck-devel, gnome-panel-devel, gnome-desktop-devel, nautilus-devel, gstreamer-devel y gstreamer-plugins-devel.
- Si va a crear paquetería para KDE, necesitará al menos lo siguiente, con todo lo que dependa de éste: qt-devel, arts-devel, kdelibs-devel, kdebase-devel, kdenetwork-devel, kdegraphics-devel y kdemultimedia-devel.

Si utiliza Cent OS, White Box Enterprise Linux o bien Red Hat™ Enterprise Linux, necesitará correr lo siguiente para instalar el mínimo de paquetería:

```
yum -y install gcc* automake* autoconf* rpm-build rpm-devel gnupg
```

Si desea generar paquetería para GNOME, necesitará **también** instalar el mínimo de paquetería de desarrollo de GNOME:

```
yum -y install glib2-devel atk-devel pango-devel gtk2-devel libbonoboui-devel libgnomeui-
devel gnome-vfs2-devel libwnck-devel gnome-panel-devel gnome-desktop-devel nautilus-devel
gstreamer-devel gstreamer-plugins-devel
```

Si va a generar paquetería para KDE, necesitará **también** instalar el mínimo de paquetería de desarrollo de KDE:

```
yum -y install qt-devel arts-devel kdelibs-devel kdebase-devel kdenetwork-devel
kdegraphics-devel kdemultimedia-devel
```

Si además tiene instalado LPT Desktop, puede instalar **también** el sustento lógico restante:

```
yum -y install seahorse gpgme
```

22.3. Procedimientos

22.3.1. Creación de la clave GnuPG

1. Desde una sesión gráfica, inicie seahorse y de clic en en botón de «Nuevo» en el panel de «Opciones de primera vez».

2. Lo anterior iniciará un asistente de creación de claves.

3. Elija el nivel de seguridad como «Seguridad extra alta».

4. Especifique su nombre completo, un breve comentario opcional y su cuenta de correo electrónico permanente que se relacionará exclusivamente con la nueva clave.

5. Especifique una frase de paso que sólo usted pueda recordar. Se recomienda utilizar espacios y signos de puntuación.

6. En la pantalla de «Fecha de caducidad», salvo que específicamente requiera lo contrario, especifique «Sin caducidad».

7. Tome nota de como aparece **exactamente** el nombre de la llave, incluyendo paréntesis, espacios y otros símbolos, ya que se utilizarán en el siguiente procedimiento.

22.3.2. Configuración y creación de una jaula para rpmbuild

Jamás utilice la cuenta de root sin importar la circunstancia, para crear o reconstruir paquetería en formato RPM. Esto puede resultar peligroso debido a que la configuración de algunos programas pueden tratar de instalar componentes en el sistema en lugar del directorio especificado para rpmbuild, lo cual dará como resultado diversas consecuencias de seguridad y de estabilidad para el sistema.

La jaula será creada de modo seguro dentro de una **cuenta de usuario normal sin privilegios**, a

fin de poder detectar e impedir que algunos procedimientos durante la creación de paquetes intenten instalar componentes no deseados en el sistema.

22.3.2.1. Componentes del fichero ~/.rpmmacros

Utilizando cualquier editor de texto, genere el fichero ~/.rpmmacros, en el cual se definirán valores para algunas variables utilizadas por rpmbuild:

- %debug_package: sirve para especificar si se anula o no la generación de paquetería de depuración. La paquetería de depuración solo es útil para los programadores a fin de localizar fallas en los programas empaquetados. Para la mayoría de los casos se especifica el valor %{nil} a fin de impedir que se genere paquetería de depuración.
- %_unpackaged_files_terminate_build: sirve para especificar si la construcción de un paquete se deberá interrumpir si hay componentes ignorados por el fichero *.spec. 0 deshabilita, 1 habilita. ¿Qué valor se recomienda?; la respuesta es obvia: no es deseable un paquete al cual le faltan componentes, así que se especificará 1.
- %_signature: se utilizará gpg para firmar los paquetes resultantes.
- %_gpg_path: ruta del directorio .gpg a utilizar. Estará localizado dentro de la carpeta de inicio del usuario utilizado.
- %_gpg_name: identidad a utilizar para firmar los paquetes resultantes. El formato utilizado es el mismo como aparece el nombre de su clave GnuPG en seahorse: Su Nombre (Breve comentario) <su cuenta de correo electrónico>.
- %_gpgbin: ruta del binario gpg, normalmente en /usr/bin/gpg.
- %_topdir: ruta donde se localiza la jaula para rpmbuild.
- %_tmppath: directorio de elementos temporales que será utilizado para simular instalaciones.
- %packager: su nombre completo y dirección de correo electrónico o bien el URL de su sitio de red.
- %distribution: nombre del producto o bien para especificar para que distribución de GNU/Linux se utilizará la paquetería.
- %vendor: nombre de su empresa u organización.
- %desktop_vendor: variable opcional (y no oficial) para definir el nombre de la empresa en el nombre algunos ficheros, principalmente entradas de menú. Especifique el nombre corto de su empresa **sin espacios**.

A continuación un ejemplo del contenido del fichero ~/.rpmmacros, utilizando valores ficticios:

```
%debug_package %{nil}
%_unpackaged_files_terminate_build 1
%_signature gpg
%_gpg_path %(echo "$HOME")/.gnupg
%_gpg_name Fulano de Perengano (Una empresa ficticia) <fulano@algún-dominio.com>
%_gpgbin /usr/bin/gpg
%_topdir %(echo "$HOME")/rpmbuild
%_tmppath %(echo "$HOME")/rpmbuild/TMP
%packager Fulano de Perengano <su cuenta de correo o bien http://su-sitio-de-red.com>
%distribution nombre de su producto aquí
%vendor su nombre o nombre de su empresa aquí
%desktop_vendor nombre-de-su-empresa-sin-espacios
```

22.3.2.2. Creación de la estructura de la jaula para rpmbuild

Desde una terminal, genere la estructura de directorios necesaria utilizando lo siguiente:

```
mkdir -p ~/rpmbuild/{BUILD,RPMS,SOURCES,SRPMS,SPECS,TMP}
mkdir -p ~/rpmbuild/RPMS/{athlon,i386,i586,i686,noarch}
```

22.3.3. Creación de los ficheros*.spec

Los ficheros *.spec contienen la información que utilizará rpmbuild para construir un paquete. Del contenido de éstos dependerá que sea posible descomprimir, configurar, compilar, instalar virtualmente y empaquetar un sustento lógico en particular a partir de un código fuente.

Name:

Se refiere nombre del paquete. No puede llevar espacios. Regularmente es el mismo nombre utilizado para el paquete del código fuente.

Version:

Se refiere al número de versión del paquete

Release:

Número de lanzamiento o entrega

URL:

URL original del sitio de red del sustento lógico que se va a empaquetar.

Summary:

Resumen o descripción corta del paquete.

License:

Licencia o licencias utilizadas por el paquete.

Group:

Grupo o categoría de sustento lógico al cual pertenece el paquete. Lista de grupos válidos:

Amusements/Games
Amusements/Graphics
Applications/Archiving
Applications/Communications
Applications/Databases
Applications/Editors
Applications/Emulators
Applications/Engineering
Applications/File
Applications/Internet
Applications/Multimedia
Applications/Productivity
Applications/Publishing
Applications/System
Applications/Text
Development/Debuggers
Development/Languages
Development/Libraries
Development/System
Development/Tools
Documentation
System Environment/Base
System Environment/Daemons
System Environment/Kernel
System Environment/Libraries
System Environment/Shells
User Interface/Desktops
User Interface/X
User Interface/X Hardware Support

Buildroot:

Ruta donde se realizará la instalación virtual, es decir: `%{_tmppath}/%{name}-%{version}-root`

Source:

Se puede especificar solamente el nombre del paquete utilizado para el código fuente, aunque por norma se sugiere especificar el URL exacto hacia el código fuente.

BuildRequires:

Lista separada por comas o espacios de componentes o paquetes requeridos para poder construir el sustento lógico involucrado.

BuildPreReq:

Lista de componentes o paquetes que deben estar previamente instalados en el sistema antes de iniciar la compilación del sustento lógico involucrado.

Requires:

Lista de paquetes de los cuales depende el sustento lógico empaquetado para poder funcionar.

PreReq:

Lista de componentes o paquetes que deben estar previamente instalados en el sistema antes de iniciar la instalación de el sustento lógico involucrado.

%description

Descripción detallada acerca del paquete

%prep

Procedimientos, si los hubiere, requeridos antes de desempaquetar el código fuente. Regularmente no los hay.

%setup

Procedimientos, si los hubiere, requeridos al desempaquetar o después de desempaquetar el código fuente. Regularmente aquí es donde se aplican parches y otros correctivos.

%build

Procedimientos necesarios para poder compilar desde el código fuente de un sustento lógico en particular. Por lo general basta con un `%configure` y `%__make`, pero se recomienda leer a detalle el instructivo de instalación de cada programa en particular a fin de asegurar los procedimientos correctos para compilar el sustento lógico.

%install

Procedimiento de instalación requerido para un paquete en particular. Se recomienda limpiar cualquier instalación previa utilizando `%__rm -fr %{buildroot}`. La instalación será virtual y se realizará dentro de ~/rpmbuild/TMP/ que es establecido por la variable %{buildroot}. Por lo general es suficiente `%__make DESTDIR=%{buildroot} install`, ; sin embargo algunos programas pudieran requerir instalación individual de algunos o todos sus componentes.

%clean

Procedimientos para limpiar aquello que ya no se necesita después de haber creado exitosamente el paquete RPM. Específicamente se refiere a la instalación virtual que se realizó dentro de ~/rpmbuild/TMP/. Para la mayoría de los casos es suficiente utilizar `%__rm -fr %{buildroot}`..

%preun

Procedimientos que se deben correr justo antes de proceder a instalar un paquete. Se utiliza principalmente con paquetes que necesitan crear cuentas de sistema u otros preparativos.

%post

Procedimientos que se deben correr justo después de proceder a instalar un paquete. Ejemplos: Cuando los paquetes incluyen bibliotecas compartidas, se ejecuta ldconfig. Si un paquete incluye un esquema para GConf, se debe correr lo necesario para registrar el esquema.

%postun

Procedimientos que se deben correr justo después de proceder a desinstalar un paquete. Se utiliza principalmente con paquetes que necesitan correr tareas administrativas, como detener y/o dar de baja un servicio.

%files

Lista de todos los componentes de el sustento lógico empaquetado en sus rutas definitivas.

%changelog

Bitácora de cambios del fichero *.spec. Requiere un formato especial:

* [Dia de la semana en abreviado y en inglés] [Mes abreviado en inglés] día año Nombre empaquetador <correo electrónico o URL de sitio de red>
- Algunos cambios
- Más cambios
- Otros cambios

Ejemplo:
* Sun Sep 25 2005 Fulano de Perengano <http://mi-sitio-güeb.algo/>
- Fichero *.spec inicial.
- Se añadieron cosas
- Se puso un guión para algo

22.3.3.1. Ejemplo de fichero *.spec.

```
Name: algo
Version: 0.1
Release: 1
URL: http://sitio-de-red-del-sustento-lógico-a-utilizar/
Summary: Paquete imaginario que hace algo.
License: GPL
Group: Applications/File

Buildroot: %{_tmppath}/%{name}-%{version}-root
Source: http://un-sitio-güeb.algo/algo-0.1.tar.bz2
BuildRequires: gtk2-devel
BuildPreReq: /usr/bin/desktop-file-install
Requires: gtk2
PreReq: /usr/bin/update-desktop-database

%description
Programa imaginario escrito en un lenguaje abstracto e inexistente que hace
cosas imaginarias e imposibles sólo para fines demostrativos.

%prep
%setup -q

%build
%configure
%__make

%install
%__make DESTDIR=%{buildroot} install

%clean
%__rm -fr %{buildroot}

%preun

%post
/sbin/ldconfig
```

```
%postun

%files
defattr(-,root,root)
/usr/bin/algo
/usr/lib/libalgo.so.0
/usr/share/applications/algo.desktop

%changelog
* Sun Sep 25 2005 Fulano de Perengano <http://mi-sitio-güeb.algo/>
- Se añadieron cosas
- Se puso un guión para algo

* Sat Sep 24 2005 Fulano de Perengano <http://mi-sitio-güeb.algo/>
- Fichero *.spec inicial.
```

22.3.4. Uso del mandato rpmbuild

Lista y descripción de opciones principales:

`--sign`
: Especifica que se debe firmar un paquete con clave digital predeterminada.

`--clean`
: Solicita a rpmbuild corra los procesos especificados en la sección %clean para dejar limpio el directorio de temporales utilizado para realizar instalaciones virtuales.

`--target=[arquitectura]`
: Se utiliza para indicar a rpmbuild para que arquitectura será construido el paquete. De modo predefinido rpmbuild crea los paquetes para la arquitectura predeterminada del sistema. Puede especificarse i386, i585, i686, noarch, athlon, etc., de acuerdo a lo que sea requerido.

`-ba`
: Solicita a rpmbuild corra todos los procedimientos necesarios para generar un paquete RPM binario y el paquete RPM fuente (*.src.rpm) a partir de un fichero *.spec.

`-bb`
: Solicita a rpmbuild corra todos los procedimientos necesarios para generar solamente un paquete RPM binario a partir de un fichero *.spec.

`-bp`
: Solicita a rpmbuild corra todos los procedimientos necesarios en la sección %prep y aplicación de parches en %setup. Se utiliza principalmente para verificar y depurar estos procedimientos antes de comenzar la compilación e instalación.

`-bc`
: Solicita a rpmbuild corra todos los procedimientos necesarios en la sección %prep, aplicación de parches en %setup y compilación en %build. No realiza instalación virtual ni crea paquetes RPM. Se utiliza principalmente para verificar y depurar estos procedimientos.

`-bi`
: Solicita a rpmbuild corra todos los procedimientos necesarios en la sección %prep, aplicación de parches en %setup, compilación en %build e instalación virtual en %install. No crea paquetes RPM. Se utiliza principalmente para verificar y depurar estos procedimientos.

`--short-circuit`
: Se utiliza en combinación con -bc y bi. Solicita a rpmbuild saltar todos los pasos previos y correr únicamente la compilación, en el caso de ser combinado con -bc, o bien saltar todos los

pasos previos y correr únicamente los procedimientos para realizar la instalación virtual, en el caso de ser combinado con -bi. Se utiliza principalmente para verificar y depurar estos procedimientos.

`--rmspec`
: Solicita a rpmbuild elimine el fichero *.spec después de crear exitosamente los paquetes RPM correspondientes. Se utiliza para mantener limpia la jaula de rpmbuild.

`--rmsource`
: Solicita a rpmbuild elimine todo lo que corresponda a las fuentes, es decir, códigos fuentes, parches y otros elementos, después de crear exitosamente los paquetes RPM correspondientes. Se utiliza para mantener limpia la jaula de rpmbuild.

`--rebuild`
: Solicita a rpmbuild reconstruya un paquete a partir de un *.src.rpm.

22.3.4.1. Ejemplos de uso del mandato rpmbuild

Construir sólo un paquete RPM, **sin generar *.src.rpm**, a partir de un fichero *.spec:

```
rpmbuild -bb algo.spec
```

Construir sólo un paquete RPM junto con el correspondiente *.src.rpm a partir de un fichero *.spec:

```
rpmbuild -ba --clean --sign --rmspec --rmsource algo.spec
```

Construir solo un paquete RPM sin *.src.rpm a partir de un fichero *.spec, con firma digital, limpieza de directorio de instalaciones virtuales y eliminación de *.spec y fuentes tras terminar exitosamente:

```
rpmbuild -bb *.spec
```

Construir sólo un paquete RPM y el correspondiente *.src.rpm a partir de un fichero *.spec, con firma digital, limpieza de directorio de instalaciones virtuales y eliminación de *.spec y fuentes tras terminar exitosamente:

```
rpmbuild -ba --clean --sign --rmspec --rmsource *.spec
```

Reconstruir sólo un paquete RPM a partir de un *.src.rpm:

```
rpmbuild --rebuild cualquier-paquete.src.rpm
```

Reconstruir sólo un paquete RPM a partir de un *.src.rpm, con firma digital, limpieza de directorio de instalaciones virtuales y eliminación de *.spec y fuentes tras terminar exitosamente:

```
rpmbuild --rebuild --clean --sign --rmspec --rmsource cualquier-paquete.src.rpm
```

22.4. Ejercicios

22.4.1. Paquete RPM binario y el paquete *.src.rpm correspondiente creando el fichero *.spec necesario

1. Acceda hacia http://www.nano-editor.org y descargue el código fuente de **la más reciente versión estable** del editor de texto Nano.

2. Coloque el *.tar.gz del código fuente dentro del directorio ~/rpmbuild/SOURCES/

```
mv nano-1.2.5.tar.gz ~/rpmbuild/SOURCES/
```

3. Cambie hacia el directorio ~/rpmbuild/SPECS/

```
cd ~/rpmbuild/SPECS/
```

4. Con cualquier editor de texto simple, genere el fichero ~/rpmbuild/SPECS/nano.spec con el siguiente contenido **(al terminar, por favor verifique la sintaxis, línea por línea)**:

```
Name: nano
Version: 1.2.5
Release: 1
URL: http://www.nano-editor.org/
Summary: Un pequeño editor de texto.
License: GPL
Group: Applications/Editors

Buildroot: %{_tmppath}/%{name}-%{version}-root
Source: http://www.nano-editor.org/dist/v1.2/nano-1.2.5.tar.gz

BuildRequires: ncurses-devel, glibc-devel, gcc
Requires: ncurses

%description
GNU nano es un pequeño y fácil de utilizar editor de texto.

%prep
%setup -q

%build
%configure
%__make

%install
%__make DESTDIR=%{buildroot} install

%clean
%__rm -fr %{buildroot}

%files
%defattr(-,root,root)
%doc AUTHORS BUGS COPYING ChangeLog INSTALL NEWS README THANKS TODO
%doc nanorc.sample
/usr/bin/nano
/usr/share/info/nano.info.gz
/usr/share/man/man1/nano.1.gz
/usr/share/man/man5/nanorc.5.gz
/usr/share/locale/*/LC_MESSAGES/nano.mo

%changelog
* Sun Sep 25 2005 Fulano de Perengano <http://mi-sitio-güeb.algo/>
- Fichero *.spec inicial.
```

5. Para poder construir nano, necesitará tener instalados los paquetes ncurses-devel (cabeceras

de desarrollo para ncurses), glibc-devel (cabeceras de desarrollo para C) y gcc (compilador de GNU.org). De ser necesario, proceda a instalar éstos:

```
yum -y install ncurses-devel glibc-devel gcc
```

6. Utilice lo siguiente para generar los paquetes binario y fuente correspondientes:

```
rpmbuild -ba nano.cpec
```

7. Suponiendo que utiliza una computadora con microprocesador compatible con Intel; al concluir el proceso, encontrará el paquete binario RPM dentro del directorio `~/rpmbuild/RPMS/i386/` y el paquete *.src.rpm dentro del directorio `~/rpmbuild/SRPMS/`.

22.4.2. Paquete RPM binario y el paquete *.src.rpm correspondiente realizando limpieza de directorio, firma digital

1. Utilizará el mismo fichero *.spec del ejercicio pasado.

2. Utilice lo siguiente para generar los paquetes correspondientes, ingresando la clave de acceso para GnuPG cuando le sea requerida:

```
rpmbuild -ba --clean --sign nano.cpec
```

3. Suponiendo que utiliza una computadora con microprocesador compatible con Intel; al terminar el proceso, encontrará el paquete binario RPM dentro del directorio `~/rpmbuild/RPMS/i386/` y el paquete *.src.rpm dentro del directorio `~/rpmbuild/SRPMS/`.

23. Cómo asignar cuotas de disco

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

23.1. Introducción

La utilización de cuotas de disco permite a los administradores de sistemas realizar la gestión eficiente del espacio compartido en disco por múltiples usuarios. Las cuotas restringen la capacidad de los usuarios para acceder hacia los recursos de sistema, tales como bloques (asignación de unidades) e inodos (entradas del sistema de ficheros). Cuando una cuota es excedida se aplica una política determinada por el administrador. Las cuotas se administran por sistema de archivos individuales y son únicas para usuarios o grupos.

23.2. Procedimientos

I. Debe iniciarse el sistema en nivel de corrida 1 (mono usuario), ya que **se requiere no haya procesos activos** utilizando contenido de la partición a la cual se le aplicará la cuota de disco.

II. Obviamente, durante la instalación, debió asignarse una partición dedicada para, por mencionar un ejemplo, los directorios `/var` y `/home`.

III. Con la finalidad de añadir el soporte para cuotas en las particiones anteriormente mencionadas, se debe añadir en el fichero **/etc/fstab** los parámetros **usrquota** y **grpquota** a las líneas que definen la configuración de las particiones /var y /home:

```
LABEL=/var      /var    ext3    defaults,usrquota,grpquota      1 2
LABEL=/home     /home   ext3    defaults,usrquota,grpquota      1 2
```

IV. Debe remontar las particiones para que surtan efecto los cambios:

```
mount -o remount /var
mount -o remount /home
```

V. Se deben crear los ficheros aquota.user, aquota.group, quota.user y quota.group, los cuales se utilizarán en adelante para almacenar la información y estado de las cuotas en cada partición.

```
cd /var
touch aquota.user aquota.group quota.user quota.group
cd /home
touch aquota.user aquota.group quota.user quota.group
```

VI. Ejecutar:

```
quotacheck -avug
```

La primera vez que se ejecuta el mandato anterior es normal que marque advertencias refiriéndose a posibles ficheros truncados, que en realidad no eran otra cosa sino ficheros de texto simple vacíos a los cuales se les acaba de convertir a formato binario. Si se ejecuta de nuevo **quotacheck - avug**, no deberá mostrar advertencia alguna.

VII. Para activar las cuotas de disco recién configuradas, solo bastará ejecutar:

```
quotaon /var
quotaon /home
```

VIII. Vaya al nivel de corrida 3 a fin de aplicar cuota de disco a algunos usuarios.

```
init 3
```

23.2.1. Edquota

Es importante conocer que significa cada columna mostrada por edquota.

Blocks: Bloques. Corresponde a la cantidad de bloques de 1 Kb que está utilizando el usuario.

Inodes: Inodos. Corresponde al número de ficheros que está utilizando el usuario. Un **inodo** (también conocido como Index Node) es un apuntador hacia sectores específicos de disco duro en los cuales se encuentra la información de un fichero. Contiene además la información acerca de permisos de acceso así como los usuarios y grupos a los cuales pertenece el fichero.

Soft: Límite de gracia. Límite de bloques de 1 KB que el usuario puede utilizar y que puede rebasar hasta que sea excedido el periodo de gracia (de modo predeterminado son 7 días).

Hard: Límite absoluto. Límite que no puede ser rebasado por el usuario bajo circunstancia alguna.

Asignar cuotas de disco a cualquier usuario o grupo. Solamente hará falta utilizar **edquota** citando el nombre del usuario al cual se le quiere aplicar:

```
edquota fulano
```

Lo anterior deberá mostrar algo como lo siguiente a través de **vi** u otro editor de texto simple:

```
Disk quotas for user fulano (uid 501):
Filesystem    blocks     soft     hard   inodes     soft     hard
/dev/hda7          0        0        0        0        0        0
/dev/hda5         24        0        0       10        0        0
```

23.2.1.1. Cuota absoluta

Suponiendo que se quiere asignar una cuota de disco de 6 MB para el usuario «fulano» en en `/dev/hda7` y `/dev/hda5`, se utilizaría lo siguiente:

```
Disk quotas for user fulano (uid 501):
Filesystem   blocks     soft     hard   inodes     soft     hard
/dev/hda7         0        0     6144        0        0        0
/dev/hda5        24        0     6144       10        0        0
```

El usuario siempre podrá rebasar una **cuota de gracia** pero **nunca** una **cuota absoluta**.

23.2.1.2. Cuota de gracia

El sistema tiene de modo predeterminado un **periodo de gracia** de 7 días que se puede modificar con el mandato **edquota -t**, donde se puede establecer un nuevo periodo de gracia por días, horas, minutos o segundos.

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
Filesystem   Block grace period     Inode grace period
/dev/hdb7                 7days                  7days
/dev/hdb5                 7days                  7days
```

La **cuota de gracia** establece los límites de bloques o **inodos** que un usuario tiene en una partición. Cuando el usuario excede el límite establecido por la cuota de gracia, el sistema advierte al mismo que se ha excedido la cuota del disco; sin embargo permite al usuario continuar escribiendo hasta que trascurre el tiempo establecido por el periodo de gracia, tras el cual al usuario se le impide continuar escribiendo sobre la partición. Suponiendo que quiere asignar una cuota de gracia de 6 MB en `/dev/hda7` y `/dev/hda5`, la cual podrá ser excedida hasta por 7 días, entonces se utilizaría lo siguiente:

```
Disk quotas for user fulano (uid 501):
Filesystem   blocks     soft     hard   inodes     soft     hard
/dev/hda7         0     6144        0        0        0        0
/dev/hda5        24     6144        0       10        0        0
```

23.2.1.3. Aplicando cuotas masivamente

Si se quiere que todo aplique para los usuarios existentes a partir de UID 510, por ejemplo, si se que tiene al usuario «pepito» como molde **(note por favor el acento grave en el mandato justo antes de awk, no es una comilla ni apostrofe)**:

```
edquota -p pepito `awk -F: '$3 > 510 {print $1}' /etc/passwd`
```

23.3. Comprobaciones

Utilice el mandato edquota con el usuario «fulano».

```
edquota fulano
```

Asigne al usuario «fulano» una cuota de disco de 50 MB en todas las particiones con cuota de disco habilitada:

```
Disk quotas for user fulano (uid 501):
Filesystem    blocks     soft     hard   inodes     soft     hard
/dev/hda7          0        0    51200        0        0        0
/dev/hda5         24        0    51200       10        0        0
```

Desde otra terminal acceda hacia el sistema como el usuario fulano y ejecute el mandato **quota** y observe con detenimiento la salida:

```
Disk quotas for user fulano (uid 501):
Filesystem  blocks    quota   limit   grace   files   quota   limit
grace
/dev/hda7        0        0   51200               1       0       0
/dev/hda5       24        0   51200              10       0       0
```

Realice una **copia** del directorio **/usr/lib** como el directorio subordinado **~/prueba-cuotas** dentro de su directorio de inicio:

```
cp -r /usr/lib ~/prueba-cuotas
```

Notará que llegará un momento en el que el sistema indicará que ya no es posible continuar copiando contenido dentro de **~/prueba-cuotas** debido a que se ha agotado el espacio en la partición.

Utilice de nuevo el mandato **quota** y observe con detenimiento la salida, en donde aparecerá un asterisco justo junto a la cantidad en la columna de bloques, la cual indica que se ha excedido la cuota del disco:

```
Disk quotas for user fulano (uid 501):
Filesystem  blocks    quota   limit   grace   files   quota   limit
grace
/dev/hda7        0        0   51200               1       0       0
/dev/hda5    51200*       0   51200            7439       0       0
```

Para poder volver a escribir sobre la partición, es necesario liberar espacio. Elimine por completo el directorio **~/prueba-cuotas** y vuelva a utilizar el mandato quota:

```
rm -fr ~/prueba-cuotas
quota
```

24. Introducción a TCP/IP

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

24.1. Introducción

TCP/IP fue desarrollado y presentado por el Departamento de Defensa de EE.UU. en 1972 y fue aplicado en **ARPANET** (**A**dvanced **R**esearch **P**rojects **A**gency **N**etwork), que era la red de área extensa del Departamento de Defensa como medio de comunicación para los diferentes organismos de EE.UU. La transición hacia TCP/IP en **ARPANET** se concretó en 1983.

Se conoce como **familia de protocolos de Internet** al conjunto de protocolos de red que son implementados por la pila de protocolos sobre los cuales se fundamenta Internet y que permiten la transmisión de datos entre las redes de computadoras.

Los dos protocolos más importantes, y que fueron también los primeros en definirse y también los más utilizados, son **TCP** (Protocolo de Control de Transmisión o **T**ransmission **C**ontrol **P**rotocol) e **IP** (Protocolo de Internet o **I**nternet **P**rotocol), de ahí que se denomine también como **Conjunto de Protocolos TCP/IP**. Los tipos de protocolos existentes superan los cien, ente los cuales podemos mencionar como los más conocidos a HTTP, FTP, SMTP, POP, ARP, etc.

TCP/IP es la plataforma que sostiene Internet y que permite la comunicación entre diferentes sistemas operativos en diferentes computadoras, ya sea sobre redes de área local (LAN) o redes de área extensa (WAN).

24.2. Niveles de pila

En la actualidad continúa la discusión respecto a si el modelo TCP/IP de cinco niveles encaja dentro del modelo OSI (Interconexión de Sistemas Abiertos u **O**pen**S**ystems **I**nterconnection) de siete niveles.

Modelo	Niveles
TCP/IP	5 Aplicación 4 Transporte 3 Red 2 Enlace 1 Físico.
OSI	7 Aplicación 6 Presentación 5 Sesión 4 Transporte 3 Red 2 Enlace de datos

Modelo	Niveles
	1 Físico

24.2.1. Modelo TCP/IP

Utiliza encapsulamiento para proveer la abstracción de protocolos y servicios hacia diferentes capas en la pila. La pila consiste de cinco niveles:

Nivel	Nombre	Descripción
5	**Aplicación**	Se compone de diversos protocolos de servicios como: • **DNS** (Domain Name System) • **TLS/SSL** (**T**ransport **L**ayer **S**ecurity) • **TFTP** (**T**rivial **F**ile **T**ransfer **P**rotocol) • **FTP** (**F**ile **T**ransfer **P**rotocol) • **HTTP** (**H**yper **T**ext **T**ransfer **P**rotocol) • **IMAP** (**I**nternet **M**esssage **A**ccess **P**rotocol) • **IRC** (**I**nternet **R**elay **C**hat) • **NNTP** (**N**etwork **N**ews **T**ransfer **P**rotocol) • **POP3** (**P**ost **O**ffice **P**rotocol) • **SIP** (**S**ession **I**niciation **P**rotocol) • **SMTP** (**S**imple **M**ail **T**ransfer **P**rotocol) • **SNMP** (**S**imple **N**etwork **M**anagement **P**rotcol) • **SSH** (**S**ecure **Sh**ell) • **TELNET** • **BitTorrent** • **RTP** (**R**eal-time **T**ransport **P**rotocol) • **rlogin** • **ENRP** (**E**ndpoint **H**andlespace **R**edundancy **P**rotocol) Los protocolos de encaminamiento como **BGP** (**B**order **G**ateway **P**rotocol) y **RIP** (**R**outing **I**nformation **P**rotocol) que utilizan transporte por TCP y UDP respectivamente pueden ser considerados como parte de este nivel.

Nivel	Nombre	Descripción
4	**Transporte**	Se compone de diversos protocolos de servicios como: • **TCP** (**T**ransmision **C**ontrol **P**rotocol) • **UDP** (**U**ser **D**atagram **P**rotocol), • **DCCP** (**D**atagram **C**ongestion **C**ontrol **P**rotocol) • **SCTP** (**S**tream **C**ontrol **T**ransmision **P**rotococol) • **IL** (**I**nternet **L**ink Protocol, similar a TCP pero más simple) • **RUDP** (**R**eliable **U**ser **D**atagram **P**rotocol), etc. Los protocolos como **OSPF** (**O**pen **S**hortest **P**ath **F**irst), que corren sobre IP, pueden ser también considerados como parte de esta capa. **ICMP** (**I**nternet **C**ontrol **M**essage **P**rotocol) e **IGMP** (**I**nternet **G**roup **M**anagement **P**rotocol) que también utilizan IP, pueden ser considerados parte del Nivel de Red.
3	**Red**	Se compone de diversos protocolos de servicios como **IP** (incluyendo **IPv4** e **IPv6**). Protocolos como **ARP** (**A**ddress **R**esolution **P**rotocol) y **RARP** (**R**everse **A**ddress **R**esolution **P**rotocol) que operan por debajo de IP, pero arriba del Nivel de enlace, de modo que pertenecen a un punto intermedio entre el Nivel de Red y el Nivel de Enlace.
2	**Enlace**	Compuesto de protocolos como: • **Ethernet** • **Wi-Fi** • **Token ring** • **PPP** (Point-to-Point **P**rotocol) • **SLIP** (**S**erial **L**ine **I**nternet **P**rotocol) • **FDDI** (Fiber Distributed **D**ata **I**nterface) • **ATM** (**A**synchronous **T**ransfer **P**rotocol) • **Frame Relay** • **SMDS** (Switched **M**ulti-megabit **D**ata **S**ervices)
1	**Físico**	Medio físico.

Los niveles más cercanos altos son los más cercanos al usuario, mientras que los que están más hacia abajo se encuentran más cercanos a la transmisión física de los datos. Salvo por evidentes razones en el primer y último niveles, cada nivel tiene un nivel superior y un nivel inferior que, respectivamente, o bien utilizan un servicio del nivel o proveen un servicio. Un método de abstracción para entender esto es mirar los niveles como proveedores o consumidores de servicios. Ejemplo: TCP en el nivel de transporte requiere un protocolo del nivel de Red, como sería IPv4, el

cual a su vez requiere de un protocolo del nivel de enlace, siendo TCP un proveedor de servicio para los protocolos del nivel de aplicación.

24.2.1.1. Nivel de aplicación

Es el nivel que utilizan los programas de red más comunes a fin de comunicarse a través de una red. La comunicación que se presenta en este nivel es especifica de las aplicaciones y los datos transportados desde el programa que están en el formato utilizado por la aplicación y van encapsulados en un protocolo del **Nivel de Transporte**. Siendo que el modelo TCP/IP no tiene niveles intermedios, el nivel de Aplicación debe incluir cualquier protocolo que actúe del mismo modo que los protocolos del **Nivel de Presentación** y **Nivel de Sesión** del **Modelo OSI**. Los protocolos del Nivel de Transporte más comúnmente utilizados son TCP y UDP, mismos que requieren un puerto disponible y específico para el servicio para los servidores y puertos efímeros. Aunque los encaminadores (routers) e interruptores (switches) no utilizan este nivel, las aplicaciones que controlan el ancho de banda si lo utilizan.

24.2.1.2. Nivel de Transporte

Este nivel principalmente provee lo necesario para conectar aplicaciones entre si a través de puertos. Mientras que IP (Internet Protocol),del Nivel de Red, provee solamente la mejor forma de entrega, el nivel de transporte es el primer nivel que se encarga de la fiabilidad. De entre todos los protocolos de este nivel, tanto TCP como UDP son utilizados para transportar un gran número de aplicaciones de alto nivel. Las aplicaciones en cualquier nivel se distinguen a través de los puertos TCP o UDP que utilicen.

TCP.

El mejor ejemplo de este nivel es TCP, que es un protocolo orientado hacia conexión que resuelve numerosos problemas de fiabilidad para proveer una transmisión de bytes fiable, ya que se encarga de que los datos lleguen en orden, tenga un mínimo de correcciones de errores, se descarten datos duplicados, se vuelvan a enviar los paquetes perdidos o descartados e incluya control de congestión de tráfico.

La conexiones a través de TCP tienen tres fases:

I. Establecimiento de la conexión

Antes de que el cliente intente conectarse con el servidor, éste último debe primero ligarse hacia el puerto para abrirlo para las conexiones, es decir, una **apertura pasiva**. Una vez establecida, el cliente puede iniciar la **apertura activa**. Se requiere de un saludo de tres etapas:

1. La apertura activa se realiza enviando un paquete SYN (sincroniza) hacia el servidor.
2. En respuesta, el servidor responde con un paquete SYN-ACK (conformación de sincronización).
3. Finalmente el cliente envía un paquete ACK (confirmación) de regreso hacia el servidor.

En este punto tanto cliente como servidor han recibido una conformación de la conexión.

II. Transferencia de datos

Hay tres funciones clave que diferencian a TCP de UDP:

1. Transferencia de datos libre de errores.
2. Transferencia de datos ordenada.
3. Retransmisión de paquetes perdidos.
4. Descartado de paquetes duplicados.
5. Ajuste en la congestión de la transmisión de datos.

III. **Terminación de la conexión**.

Esta etapa utiliza un saludo de tres vías, con cada extremo de la conexión terminando independientemente. Cuando uno de los extremos desea detener su parte de la conexión, envía un paquete FIN, que la otra parte confirma con un paquete ACK. Por tanto, una interrupción de la conexión requiere un par de paquetes FIN y ACK desde cada lado de la conexión TCP.

Una conexión puede quedar abierta a medias cuando uno de los extremos ha terminado la conexión desde su lado pero el otro extremo no. El extremo que terminó la conexión ya no puede enviar datos en la conexión, pero el el otro extremo sí.

El método más común es un saludo de tres etapas donde un anfitrión A envía un paquete FIN y el anfitrión B responde con un paquete FIN y un ACK (en el mismo paso) y el anfitrión A responde con un paquete ACK.

TCP realiza las siguientes etapas en su zócalo:

1. LISTEN
2. SYN-SENT
3. SYN-RECEIVED
4. ESTABLISHED
5. FIN-WAIT-1
6. FIN-WAIT-2
7. CLOSE-WAIT
8. CLOSING
9. LAST-ACK
10. TIME-WAIT
11. CLOSED

LISTEN representa la conexión en espera de peticiones desde cualquier puerto TCP remoto. **SYN-SENT** representa la espera del TCP remoto para enviar de regreso el paquete TCP estableciendo banderas **SYN** y **ACK**. **SYN-RECIVED** representa la espera para el TCP remoto para enviar de regreso la confirmación después de haber enviado de regreso otra confirmación de conexión al TCP remoto (establecido por el servidor TCP). **ESTABLISHED** representa que el puerto está listo para recibir/enviar datos desde/hacia el TCP remoto (lo hacen tanto clientes como servidores TCP). **TIME-WAIT** representa el tiempo de espera necesario para asegurar que el TCP remoto ha recibido la confirmación de su solicitud de terminación de la conexión.

UDP.

UDP, a veces referido sarcásticamente como *Unreliable* Datagram Protocol (Protcolo no fiable de datagrama), es un protocolo de datagrama sin corrección; no provee las garantía de fiabilidad y ordenamiento de TCP a los protocolos del **Nivel de Aplicación** y los datagramas pueden llegar en desorden o perderse sin notificación. Como consecuencia de lo anterior es que UDP es un protocolo más rápido y eficiente para tareas ligeras o sensibles al tiempo una interfaz muy simple entre el **Nivel de Red** y **Nivel de Aplicación**. Si se requiere algún tipo de

fiabilidad para los datos transmitidos, ésta debe ser implementada en los niveles superiores de la pila.

Al igual que IP, y a diferencia de TCP, es un protocolo de mejor esfuerzo o no-fiable. El único problema de fiabilidad que resuelve es la corrección de errores en la cabecera y datos transmitidos a través de un campo de 16 bits para **suma de verificación** (checksum), una forma de control de redundancia con la finalidad de proteger la integridad de datos verificando que no hayan sido corrompidos.

La estructura de paquetes UDP consiste de 4 campos.

- **Puerto de origen**. Encargado de identificar el puerto que envía y que se asume será el puerto hacia donde se envía la respuesta si se necesita. Este campo es opcional: si no se utiliza, el valor del campo debe ser 0.
- **Puerto de destino**. Identifica el puerto de destino. Es obligatorio.
- **Longitud**. Un campo de 16 bits que especifica la longitud del datagrama completo: cabecera y datos. La longitud mínima es de 8 bytes ya que es la longitud misma de la cabecera.
- **Suma de verificación**. Un campo de 16 bits que se utiliza para verificar errores en cabecera y datos.

Las aplicaciones más comunes que hacen uso de este tipo de protocolo son DNS, aplicaciones de transmisión de medios, voz sobre IP (VoIP), TFTP y juegos en línea.

SCTP.

SCTP es un **mecanismo de transporte fiable** orientado hacia conexión. Está orientado también hacia transmisión de datos pero no está orientado hacia bytes como TCP. Provee múltiples transmisiones distribuidos sobre una misma conexión. Puede además representar una conexión con múltiples direcciones IP de modo que si una IP falla, la conexión no se interrumpe. Se desarrolló inicialmente para aplicaciones de telefonía pero se puede utilizar en otras aplicaciones.

DCCP.

DCCP se encuentra en fase de desarrollo y bajo la tutela de la IETF (Internet Engineering Task Force) que pretende proveer la semántica de control de flujo de TCP y el modelo de servicio de datagrama de UDP a la vista del usuario.

RTP.

RTP es un protocolo de datagrama que fue diseñado para datos en tiempo real como la transmisión de audio y vídeo. Es un nivel de sesión que utiliza el formato de paquetes de UDP como base. Sin embargo se considera que este protocolo pudiera acomodar debajo del nivel de transporte del modelo TCP/IP.

24.2.1.3. Nivel de Red

Este nivel resuelve el problema de capturar los datos a través de una red única. **IP** (**I**nternet **P**rotocol) realiza la tarea básica de capturar los paquetes de datos desde una fuente hacia un destino. IP puede transportar datos para una gran cantidad de protocolos del nivel superior (Nivel de Transporte). Otro ejemplo de protocolo de este nivel es X.25, que es un conjunto de protocolos para redes WAN utilizando líneas telefónicas o sistema ISDN.

24.2.1.4. Nivel de Enlace

Este nivel no es realmente parte del **Conjunto de Protocolos TCP/IP**, sino que es el método utilizado para pasar paquetes desde el Nivel de Red sobre dos diferentes anfitriones. Este proceso puede ser controlado a través del sustento lógico utilizado como controlador del dispositivo para una tarjeta de red así como también sobre la **Programación en firme** (Firmware) o circuitos integrados auxiliares (chipsets). Estos procesos realizarán funciones de enlace de datos tales como añadir una cabecera de paquete para preparar la transmisión, y entonces transmitir el todo a través de un medio físico.

Este nivel es donde los paquetes son interceptados y enviados hacia una Red Privada Virtual (VPN). Cuando esto se lleva a acabo, los datos del Nivel de Enlace se consideran como los datos de la aplicación y procede descendiendo por la pila del modelo TCP/IP para realizar la verdadera transmisión. En el extremo receptor, los datos suben por la pila del modelo TCP/IP dos veces, una para la VPN y otra para el encaminamiento (routing).

24.2.1.5. Nivel Físico

Al igual que el Nivel de Enlace, no es realmente parte del **Conjunto de Protocolos TCP/IP**. Contempla todas las características físicas de la comunicación como la naturaleza del medio, detalles de conectores, código de canales y modulación, potencias de señal, longitudes de onda, sincronización y tiempo de vida así como distancias máximas.

24.2.2. Modelo OSI

El **Conjunto de Protocolos TCP/IP** (y su correspondiente pila) han sido utilizados antes de que se estableciera el modelo OSI (Interconexión de Sistemas Abiertos u **O**pen **S**ystems **I**nterconnection) y desde entonces el modelo TCP/IP ha sido comparado con el modelo OSI tanto en libros como en instituciones educativas. Ambas se relacionan pero no son equiparables. El modelo OSI utiliza siete niveles, mientras que el modelo TCP/IP utiliza cinco. Los dos niveles que hacen la diferencia en el Modelo OSI son el **Nivel de Presentación** y el **Nivel de Sesión**, mismos que podrían ser equivalentes al **Nivel de Aplicación** del modelo TCP/IP.

Del mismo modo que la pila del modelo TCP/IP, el modelo OSI no es lo suficientemente diverso en los niveles inferiores para abarcar las verdaderas capacidades del **Conjunto de Protocolos TCP/IP**. Un claro ejemplo es que falta un nivel intermedio para acomodar entre el **Nivel de Red** y el **Nivel de Transporte** para poder determinar donde corresponden los protocolos ICMP e IGMP, y otro nivel intermedio entre el **Nivel de Red** y el **Nivel de Transporte** para determinar donde corresponden los protocolos ARP y RARP.

Nivel	Nombre	Descripción
7	**Aplicación**	HTTP, SMTP, SNMP, FTP, Telnet, SIP, SSH, NFS, RTSP, **XMPP** (E**x**tensible **M**essaging and **P**resence **P**rotocol), Whois, ENRP Telnet.
6	**Presentación**	**XDR** (E**x**ternal **D**ata **R**epresentation), **ASN.1** (**A**bstract **S**yntax **N**otation 1), **SMB** (**S**erver **M**essage **B**lock),**AFP** (**A**pple **F**iling **P**rotocol), **NCP** (**N**etWare **C**ore **P**rotocol)
5	**Sesión**	**ASAP** (**A**ggregate **S**erver **A**ccess **P**rotocol), TLS, SSH, ISO 8327 / CCITT X.225, **RPC** (**R**emote **P**rocedure **C**all), **NetBIOS**, **ASP** (**A**ppletalk **S**ession **P**rotocol), Winsock, BSD sockets
4	**Transporte**	TCP, UDP, RTP, SCTP, SPX, ATP, IL
2	**Enlace de datos**	Ethernet, Token ring, HDLC, Frame relay, ISDN, ATM, 802.11 WiFi, FDDI, PPP

Nivel	Nombre	Descripción
1	**Físico**	Define todas las especificaciones físicas y eléctricas de los dispositivos, como son disposición de pines, voltajes, especificaciones de cableado, concentradores, repetidores, adaptadores de red, etc. **Cable**, **Radio**, f**ibra óptica**, **Red por palomas**.

Los niveles 7 al 4 se clasifican como niveles de anfitrión, mientras que los **niveles inferiores** del 1 al 3 se clasifican como **niveles de medios**.

25. Introducción a IP versión 4

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

25.1. Introducción.

IPv4 es la versión 4 del Protocolo de Internet (**IP** o **I**nernet **P**rotocol) y constituye la primera versión de IP que es implementada de forma extensiva. **IPv4** es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet. Fue descrito inicial mente en el RFC 791 elaborado por la Fuerza de Trabajo en Ingeniería de Internet (**IETF** o **I**nternet **E**ngineering **T**ask **F**orce) en Septiembre de 1981, documento que dejó obsoleto al RFC 760 de Enero de 1980.

IPv4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones (switches) de paquetes (por ejemplo a través de Ethernet). Tiene las siguientes características:

- Es un protocolo de un servicio de datagramas no fiable (también referido como de *mejor esfuerzo*).
- No proporciona garantía en la entrega de datos.
- No proporciona ni garantías sobre la corrección de los datos.
- Puede resultar en paquetes duplicado o en desorden.

Todos los problemas mencionados se resuelven en el nivel superior en el modelo TCP/IP, por ejemplo, a través de **TCP** o **UDP**.

El propósito principal de **IP** es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra.

25.2. Direcciones.

IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a 4,294,967,295 direcciones únicas. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, **Multidifusión** (Multicast), etc. Debido a esto se reduce el número de direcciones IP que realmente se pueden utilizar, es esto mismo lo que ha impulsado la creación de **IPv6** (actualmente en desarrollo) como reemplazo eventual dentro de algunos años para **IPv4**.

25.2.1. Representación de las direcciones.

Cuando se escribe una dirección **IPv4** en cadenas, la notación más común es la **decimal con puntos**. Hay otras notaciones basadas sobre los valores de los octetos de la dirección IP.

Utilizando como ejemplo: www.alcancelibre.org que tiene como dirección IP 201.161.1.226 en la notación decimal con puntos:

Notación	Valor	Conversión desde decimal con puntos
Decimal con puntos	201.161.1.226	-
Hexadecimal con puntos	0xC9.0xA1.0x01.0xE2	Cada octeto de la dirección es convertido individualmente a hexadecimal.
Octal con puntos	0311.0241.0001.0342	Cada octeto es convertido individualmente a octal.
Binario con puntos	11001001.10100001.00000001.11100010	Cada octeto es convertido individualmente a binario
Hexadecimal	0xC9A101E2	Concatenación de los octetos de hexadecimal con puntos.
Decimal	3382772194	La forma hexadecimal convertida a decimal.
Octal	31150200742	La forma hexadecimal convertida a octal.
Binario	11001001101000010000000111100010	La forma hexadecimal convertida a binario.

Teóricamente, todos estos formatos mencionados deberían ser reconocidos por los navegadores (sin combinar). Además, en las formas con puntos, cada octeto puede ser representado en combinación de diferentes bases. Ejemplo: 201.0241.0x01.226.

25.3. Asignación

Desde 1993 rige el esquema **CIDR** (**C**lassless **I**nter-**D**omain **R**outing o Encaminamiento Inter-Dominios sin Clases) cuya principal ventaja es permitir la subdivisión de redes y permite las entidades sub-asignar direcciones IP, como haría un ISP con un cliente.

El principio fundamental del encaminamiento (routing) es que la dirección codifica información acerca de localización de un dispositivo dentro de una red. Esto implica que una dirección asignada a una parte de una red no funcionará en otra parte de la red. Existe una estructura jerárquica que se encarga de la asignación de direcciones de Internet alrededor del mundo. Esta estructura fue creada para el **CIDR**, y hasta 1998 fue supervisada por la **IANA** (**I**nternet **A**ssigned **N**umbers **A**uthority o Agencia de Asignación de Números Internet) y sus **RIR** (**R**egional **I**nternet **R**egistries o Registros Regionales de Internet). Desde el 18 de Septiembre de 1998 la supervisión está a cargo de la **ICANN** (**I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers o Corporación de Internet para los Nombres y Números Asignados). Cada **RIR** mantiene una base de datos **WHOIS** disponible al publico y que permite hacer búsquedas que proveen información acerca de las asignaciones de direcciones IP. La información obtenida a partir de estas búsquedas juega un papel central en numerosas herramientas las cuales se utilizan para localizar direcciones IP geográficamente.

25.3.1. Bloques reservados.

Bloques de direcciones reservadas

Bloque de direcciones CIDR	Descripción	Referencia
0.0.0.0/8	Red actual (solo válido como dirección	RFC 1700

Bloque de direcciones CIDR	Descripción	Referencia
	de origen)	
10.0.0.0/8	**Red Privada**	RFC 1918
14.0.0.0/8	Red de datos públicos	RFC 1700
39.0.0.0/8	Reservado	RFC 1797
127.0.0.0/8	Anfitrión local (localhost)	RFC 1700
128.0.0.0/16	Reservado	
169.254.0.0/16	**Red Privada** (Zeroconf)	RFC 3927
172.16.0.0/12	**Red Privada**	RFC 1918
191.255.0.0/16		
192.0.0.0/24		
192.0.2.0/24	Red de pruebas	RFC 3330
192.88.99.0/24	Retransmisión desde **IPv6** hacia **IPv4**	RFC 3068
192.168.0.0/16	**Red Privada**	RFC 1918
198.18.0.0/15	Pruebas de desempeño de red	RFC 2544
223.255.255.0/24	Reservado	RFC 3330
224.0.0.0/4	Multidifusión (Multicast, antes red Clase D)	RFC 3171
240.0.0.0/4	Reservado (Antes red Clase E)	RFC 1700
255.255.255.255	Difusiones (Broadcast)	

25.3.1.1. Redes privadas.

De los más de **cuatro mil millones** de direcciones permitidas por **IPv4**, tres rangos están especialmente reservados para utilizarse solamente en redes privadas. Estos rangos no tienen encaminamiento fuera de una red privada y las máquinas dentro de estas redes privadas no pueden comunicarse directamente con las redes públicas. Pueden, sin embargo, comunicarse hacia redes públicas a través de la Traducción de Direcciones de Red o **NAT** (**N**etwork **A**ddress **T**ranslation).

Bloques reservados para redes privadas

Nombre	Rango de direcciones IP	Numero de direcciones IP	Tipo de clase	Bloque CIDR mayor
Bloque de 24bits	10.0.0.0 – 10.255.255.255	16,777,215	Única clase A	10.0.0.0/8
Bloque de 20bits	172.16.0.0 – 172.31.255.255	1,048,576	16 clases B contiguas	172.16.0.0/12
Bloque de 16bits	192.168.0.0 – 192.168.255.255	65,535	256 clases C contiguas	192.168.0.0/16

25.3.1.2. Anfitrión local (Localhost)

Además de las redes privadas, el rango 127.0.0.0 – 127.255.255.255, o 127.0.0.0/8 en la notación

CIDR, está reservado para la comunicación del anfitrión local (localhost). Ninguna dirección de este rango deberá aparecer en una red, sea pública o privada, y cualquier paquete enviado hacia cualquier dirección de este rango deberá regresar como un paquete entrante hacia la misma máquina.

25.4. Referencia de sub-redes de IP versión 4.

Algunos segmentos del espacio de direcciones de IP, disponibles para la versión 4, se especifican y asignan a través de documentos **RFC** (**R**equest **F**or **C**omments, o Solicitud De Comentarios), que son conjuntos de notas técnicas y de organización que se elaboran desde 1969 donde se describen los estándares o recomendaciones de Internet, antes ARPANET. Ejemplos de esto son los usos del Retorno del sistema (loopback, RFC 1643), las redes privadas (RFC 1918) y Zeroconf (RFC 3927) que no están bajo el control de los **RIR** (**R**egional **I**nternet **R**egistries o Registros Regionales de Internet).

La máscara de sub-red es utilizada para separar los bits de un identificados de una red a partir de los bits del identificados del anfitrión. Se escribe utilizando el mismo tipo de notación para escribir direcciones IP.

CIDR	Máscara de sub-red	Anfitriones	Nombre de la clase	Uso típico
/8	255.0.0.0	16777216	Clase A	Bloque más grande definido por la IANA
/9	255.128.0.0	8388608		
/10	255.192.0.0	4194304		
/11	255.224.0.0	2097152		
/12	255.240.0.0	1048576		
/13	255.248.0.0	524288		
/14	255.252.0.0	262144		
/15	255.254.0.0	131072		
/16	255.255.0.0	65536	Clase B	
/17	255.255.128.0	32768		ISP / negocios grandes
/18	255.255.192.0	16384		ISP / negocios grandes
/19	255.255.224.0	8192		ISP / negocios grandes
/20	255.255.240.0	4096		ISP pequeños / negocios grandes
/21	255.255.248.0	2048		ISP pequeños / negocios grandes
/22	255.255.252.0	1024		
/23	255.255.254.0	512		
/24	255.255.255.0	256	Clase C	LAN grande
/25	255.255.255.128	128		LAN grande
/26	255.255.255.192	64		LAN pequeña
/27	255.255.255.224	32		LAN pequeña

CIDR	Máscara de sub-red	Anfitriones	Nombre de la clase	Uso típico
/28	255.255.255.240	16		LAN pequeña
/29	255.255.255.248	8		
/30	255.255.255.252	4		Redes de unión (enlaces punto a punto)
/31	255.255.255.254	2		Red no utilizable, sugerida para enlaces punto a punto (RFC 3021)
/32	255.255.255.255	1		Ruta del anfitrión

25.5. Referencias.

- http://www.ietf.org/rfc/rfc760.txt
- http://www.ietf.org/rfc/rfc791.txt
- http://www.ietf.org/rfc/rfc1643.txt
- http://www.ietf.org/rfc/rfc1700.txt
- http://www.ietf.org/rfc/rfc1797.txt
- http://www.ietf.org/rfc/rfc1918.txt
- http://www.ietf.org/rfc/rfc2544.txt
- http://www.ietf.org/rfc/rfc3021.txt
- http://www.ietf.org/rfc/rfc3068.txt
- http://www.ietf.org/rfc/rfc3171.txt
- http://www.ietf.org/rfc/rfc3330.txt
- http://www.ietf.org/rfc/rfc3927.txt

26. Cómo configurar correctamente los parámetros de red

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

26.1. Introducción

Configurar los parámetros de red en una estación de trabajo GNU/Linux o un servidor no es realmente complicado. Solamente requerirá de algunos conocimientos básicos sobre redes y cualquier editor de texto simple.

26.2. Procedimientos

26.2.1. Detección y configuración del sustento físico (hardware)

La detección del sustento físico (hardware) es realizada o bien por el programa de instalación, o bien a través de *kudzu*, un servicio que inicia con el sistema y que se encarga de detectar y configurar los dispositivos de sustento físico (hardware) instalados. En términos generales, no hace falta configurar parámetro alguno, mientras los dispositivos de red sean compatibles y exista un controlador para la versión del núcleo (kernel) ejecutado.

Si acaso no fuese detectado el dispositivo de red debido a la ausencia de *kudzu*, es posible configurar todo manualmente. La marca de la tarjeta de red es lo que menos interesa; lo que es importante es que se determine con exactitud qué circuito integrado auxiliar (chipset) utiliza la tarjeta de red. Esto puede determinarse examinando físicamente la tarjeta de red o bien examinando a detalle la salida en pantalla que se obtiene al ejecutar el siguiente mandato:

```
lspci | grep Ethernet
```

Lo anterior devuelve una salida similar a las siguiente (en el caso de una tarjeta 3Com 905 C):

```
Ethernet controller: 3Com Corporation 3c905C-TX [Fast Etherlink] (rev
120).
```

Debe modificarse con un editor de textos el fichero **/etc/modules.conf** (núcleos de la serie 2.4) o **/etc/modprobe.conf** (núcleos de la serie 2.6) y debe verificarse que el módulo de su tarjeta de red realmente esté especificado correctamente. Ejemplo:

```
alias eth0 3c59x
```

Si se realizó alguna edición de este fichero, deberá ejecutarse el siguiente mandato, a fin de actualizar dependencias:

```
depmod -a
```

Si utiliza un núcleo de la serie 2.4.x o 2.6, la lista de módulos existentes en el sistema que se pueden utilizar para distintos circuitos integrados auxiliares (chipset) de distintos modelos de tarjetas de red, se puede obtener listando el contenido del directorio **/lib/modules/[versión del núcleo]/kernel/drivers/net/**. Ejemplo:

```
ls /lib/modules/2.6.9-22/kernel/drivers/net/
```

26.2.2. Asignación de parámetros de red

26.2.2.1. Nombre del anfitrión (HOSTNAME)

Debe modificarse con un editor de textos el fichero **/etc/hosts**, y debe verificarse que esté diferenciado el eco o retorno del sistema del nombre del sistema, el cual deberá estar asociado a una de las direcciones IP, específicamente la que esté asociada a dicho nombre en el servidor de nombres de dominio o DNS si se cuenta con uno en la red local. Ejemplo:

```
127.0.0.1  localhost.localdomain  localhost
192.168.1.50  nombre.dominio  nombre
```

Se debe establecer un nombre para el sistema. Éste deberá ser un nombre de dominio completamente resuelto por un servidor de nombre de dominio (DNS) o bien, en el caso de sistemas sin conexión a red o sistemas caseros, sea resuelto localmente en **/etc/hosts**. De tal modo, el **nombre del anfitrión** (*hostname*) del sistema se definirá dentro del fichero **/etc/sysconfig/network** del siguiente modo:

```
NETWORKING=yes
HOSTNAME=nombre.dominio
```

26.2.2.2. Dirección IP, máscara de subred y puerta de enlace

Debe modificarse con cualquier editor de textos y verificar que sus parámetros de red sean los correctos, el fichero localizado en la ruta **/etc/sysconfig/network-scripts/ifcfg-eth0**. Ejemplo:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.50
NETMASK=255.255.255.0
GATEWAY=192.168.1.254
```

Los parámetros anteriores son proporcionados por el administrador de la red local en donde se localice la máquina que está siendo configurada, o bien definidos de acuerdo a una planificación predefinida. El administrador de la red deberá proporcionar una dirección IP disponible (IPADDR) y una máscara de la sub-red (NETMASK).

26.2.2.3. Servidores de nombres

Debe modificarse con un editor de textos **/etc/resolv.conf** y deben establecerse en éste los servidores de resolución de nombres de dominio (DNS). Ejemplo:

```
nameserver 192.168.1.254
nameserver 192.168.1.1
```

26.2.3. Agregar encaminamientos (rutas) adicionales

Si se requiere establecer encaminamientos adicionales para obtener conectividad con otras redes, se pueden generar ficheros para cada interfaz que sea necesario, en donde se establecen los valores para puerta de enlace, red a la que se quiere acceder y la máscara de subred correspondiente. Los ficheros se deben generar dentro del directorio **/etc/sysconfig/network-scripts/** como *route-[interfaz]* y deben llevar el siguiente formato:

```
GATEWAY0=xxx.xxx.xxx.xxx
ADDRESS0=xxx.xxx.xxx.xxx
NETMASK0=xxx.xxx.xxx.xxx
```

Por citar un ejemplo, imaginemos que nos encontramos dentro de la red 192.168.1.0 y se requiere establecer conectividad con las redes 192.168.2.0 y 192.168.3.0, con máscaras 255.255.255.0, a través de las puertas de enlace o enrutadores o encaminadores con dirección IP 192.168.2.1 y 192.168.3.1, correspondientemente para cada red citada, a través de la primera interfaz Ethernet del sistema (eth0). La configuración de **/etc/sysconfig/network-scripts/route-eth0** sería la siguiente:

```
GATEWAY0=192.168.2.1
ADDRESS0=192.168.2.0
NETMASK0=255.255.255.0
GATEWAY1=192.168.3.1
ADDRESS1=192.168.3.0
NETMASK1=255.255.255.0
```

26.2.4. Función de reenvío de paquetes para IP versión 4

Si se tiene planeado implementar un NAT o DNAT, se debe habilitar el reenvío de paquetes para IP versión 4. Esto se realiza en el fichero **/etc/sysctl.conf** cambiando **net.ipv4.ip_forward = 0** por **net.ipv4.ip_forward = 1**:

```
net.ipv4.ip_forward = 1
```

26.2.5. Comprobaciones

Después de haber configurado todos los parámetros de red deseados, sólo deberá ser reiniciado el servicio de red, ejecutando lo siguiente:

```
service network restart
```

Basta solamente comprobar si hay realmente conectividad. Puede ejecutarse el mandato **ping** hacia cualquier dirección de la red local para tal fin.

```
ping 192.168.1.254
```

Las interfaces y la información de las mismas se puede examinar utilizando:

```
/sbin/ifconfig
```

Las encaminamientos se pueden comprobar ejecutado:

```
/sbin/route -n
```

Para comprobar si hay resolución de nombres, se puede realizar una consulta hacia los DNS definidos para el sistema utilizando:

```
host algún.dominio
```

26.2.6. Alta de direcciones IP virtuales

El alta de direcciones IP es verdaderamente simple. Basta definir solamente la dirección IP, la máscara de subred y el nombre del dispositivo. El fichero se genera igualmente con el nombre del dispositivo con el prefijo **ifcfg-**. Ejemplo del contenido del fichero **/etc/sysconfig/network-scripts/ifcfg-eth0:0** que corresponde al primer dispositivo virtual del primer dispositivo ethernet:

```
DEVICE=eth0:0
IPADDR=192.168.2.254
NETMASK=255.255.255.0
```

La comprobación, al ejecutar el mandato**ifconfig**, deberá regresar algo como lo siguiente

```
eth0      Link encap:Ethernet  HWaddr 00:01:02:03:04:05
          inet addr:192.168.1.254  Bcast:192.168.1.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:264830 errors:0 dropped:0 overruns:0 frame:0
          TX packets:255396 errors:0 dropped:0 overruns:0 carrier:0
          collisions:348 txqueuelen:1000
          RX bytes:42375618 (40.4 MiB)  TX bytes:20306080 (19.3 MiB)
          Interrupt:11 Base address:0xd000

eth0:0    Link encap:Ethernet  HWaddr 00:01:02:03:04:05
          inet addr:192.168.2.254  Bcast:192.168.2.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:11 Base address:0xd000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2590 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2590 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3327899 (3.1 MiB)  TX bytes:3327899 (3.1 MiB)
```

26.2.7. La función Zeroconf

De modo predeterminado, y a fin de permitir la comunicación entre dos diferentes sistemas a través de un cable RJ45 cruzado (*crossover*), el sistema tiene habilitado **Zeroconf**, también conocido como

Zero Configuration Networking o **Automatic Private IP Addressing** (APIPA). Es un conjunto de técnicas que automáticamente crean una dirección IP utilizable sin configuración de servidores de especiales. Permite a usuarios sin conocimientos de redes conectar computadoras, impresoras en red y otros artículos entre si. Sin Zeroconf los usuarios sin conocimientos tendrían que configurar servidores especiales como DHCP y DNS para poder establecer conectividad entre dos equipos.

Estando habilitado Zeroconf se mostrará un registro en la tabla de encaminamientos para la red 169.254.0.0 al ejecutar **route -n**, devolviendo una salida similar a la siguiente:

```
192.168.1.0     0.0.0.0         255.255.255.0   U       0       0
0  eth0
169.254.0.0     0.0.0.0         255.255.0.0     U       0       0
0  eth0
127.0.0.0       0.0.0.0         255.0.0.0       U       0       0
0  lo
0.0.0.0         192.168.1.1     0.0.0.0         UG      0       0
0  eth0
```

Si se desea desactivar Zeroconf, sólo bastará añadir en el fichero **/etc/sysconfig/network** el parámetro **NOZEROCONF** con el valor **yes**:

```
NETWORKING=yes
HOSTNAME=nombre.dominio
NOZEROCONF=yes
```

Al terminar, solamente hay que reiniciar el servicio de red para que surtan efecto los cambios y comprobar de nuevo con **route -n** que la ruta para **Zeroconf** ha desaparecido:

```
192.168.1.0     0.0.0.0         255.255.255.0   U       0       0
0  eth0
127.0.0.0       0.0.0.0         255.0.0.0       U       0       0
0  lo
0.0.0.0         192.168.1.1     0.0.0.0         UG      0       0
0  eth0
```

Una vez hecho lo anterior, existen dos servicios en el sistema en CentOS, White Box y Red Hat™ Enterprise Linux 4 que se pueden desactivar, puesto que sirven para establecer la comunicación a través de Zeroconf, éstos son mDNSResponder y nifd. Desactivar estos dos servicios ahorrará tiempo en el arranque y se consumirán **menos recursos de sistema**.

```
chkconfig nifd off
chkconfig mDNSResponder off
service nifd stop
service mDNSResponder stop
```

Para más detalles acerca de **Zeroconf**, puede consultarla información disponible en:

- http://www.zeroconf.org/
- http://en.wikipedia.org/wiki/Zeroconf

26.2.8. Deshabilitar IPv6

IPv6 o Protocolo de Internet versión 6 (Internet Protocol Version 6) es un estándar, del nivel de red del modelo TCP, orientada hacia datos, utilizada por dispositivos electrónicos para transmitir datos a través de una *Inter-red* (Internetworking), creado por Steve Deering y Craig Mudge mientras trabajaban para el Centro de Investigaciones de Palo Alto de Xerox, o **Xerox Palo Alto Research Center** (Xerox PARC).

Sucediendo a IPv4, es la segunda versión de Protocolo de Internet en ser formalmente adoptada para uso general. IPv6 tiene como objetivo solucionar el problema concerniente al límite de direcciones IP que se pueden asignar a través de IPv4, las cuales tendrán mucha demanda en un futuro no muy lejano cuando se incremente el número de teléfonos móviles y otros dispositivos de comunicación que ofrezcan acceso hacia Internet.

IPv4 «sólo» incluye soporte para 4,294 mil millones ($4{,}294 \times 10^9$) de direcciones IP, lo cual es adecuado para asignar una dirección IP a cada persona del planeta. IPv6 incluye soporte para 340 undecillones (340×10^{38}) de direcciones IP. Se espera que IPv4 siga siendo útil hasta alrededor del año 2025, lo cual dará tiempo para corregir errores y problemas en IPv6.

Mientras no se implemente de modo formal IPv6, éste cargará un controlador en el sistema que hará que algunas aplicaciones manifiesten un acceso lento hacia Internet o problemas de conectividad. Si no se va a utilizar IPv6 lo más conveniente es desactivarlo del sistema. Edite el fichero **/etc/modprobe.conf** y añada lo siguiente:

```
alias ipv6 off
alias net-pf-10 off
```

Al terminar ejecute:

```
/sbin/depmod -a
```

Reinicie el sistema a fin de que se efectúen los cambios.

26.3. Ejercicios

26.3.1. Encaminamientos estáticos

Este ejercicio considera lo siguiente:

1. Se tiene dos equipos de cómputo con GNU/Linux instalado en ambos.

2. **pc1.dominio** tiene una dirección IP 192.168.0.101 con máscara de subred 255.255.255.0 en el dispositivo eth0. Una dirección IP 10.0.0.101 con máscara de subred 255.0.0.0 en el dispositivo eth1.

3. **pc2.dominio** tiene una dirección IP 192.168.0.102 (o cualquiera otra en el mismo segmento) con máscara de subred 255.255.255.0 en el dispositivo eth0. No tiene otros dispositivos de red activos.

Visualice desde **pc2.dominio** los registros de la tabla de encaminamiento.

```
route -n
```

Obtendrá una salida similar a la siguiente:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0
eth0
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0
eth0
```

Intente ejecutar **ping** hacia la dirección recién añadida en **pc1.dominio**.

```
ping -c 3 10.0.0.101
```

El resultado esperado es que **ping** devuelva que hay 100% de pérdida de paquetes.

```
PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data.

--- 10.0.0.101 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

Proceda a añadir el encaminamiento que corresponde especificando la red, mascará de subred y puerta de enlace necesarios para llegar hacia 10.0.0.101.

```
route add \
-net 10.0.0.0 \
netmask 255.0.0.0 \
gw 192.168.0.101 \
eth0
```

Visualice de nuevo los registros de la tabla de encaminamiento.

```
route -n
```

Obtendrá una salida similar a la siguiente:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0
eth0
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0
eth0
10.0.0.0        192.168.0.1     255.0.0.0       UG    0      0        0
eth0
```

Intente ejecutar **ping** hacia la dirección recién añadida en **pc1.dominio**.

```
ping -c 3 10.0.0.101
```

El resultado esperado es que **ping** responda al ping, obteniéndose una salida similar a la siguiente:

```
PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data.
64 bytes from 10.0.0.101: icmp_seq=0 ttl=64 time=0.453 ms
64 bytes from 10.0.0.101: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 10.0.0.101: icmp_seq=2 ttl=64 time=0.347 ms

--- 10.0.0.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.347/0.389/0.453/0.048 ms, pipe 2
```

Reinicie el servicio de red, visualice de nuevo los registros de la tabla de encaminamiento y compruebe que ya no hay respuesta al hacer **ping** hacia 10.0.0.101 debido a que el registro en la tabla de encaminamiento fue eliminado al reiniciar el servicio de red.

```
service network restart
route -n
ping -c 3 10.0.0.101
```

Para hacer permanente el registro en la tabla de encaminamiento utilice un editor de texto del fichero **/etc/sysconfig/network-scripts/route-eth0** y ponga el siguiente contenido:

```
ADDRESS0=10.0.0.0
NETMASK0=255.0.0.0
GATEWAY0=192.168.0.101
```

Al terminar reinicie el servicio de red.

```
service network restart
```

Visualice nuevamente los registros de la tabla de encaminamiento.

```
route -n
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0
eth0
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0
eth0
10.0.0.0        192.168.0.1     255.0.0.0       UG    0      0        0
eth0
```

Intente ejecutar **ping** hacia la dirección recién añadida en **pc1.dominio**.

```
ping -c 3 10.0.0.101
```

Reinicie el servicio de red, visualice de nuevo los registros de la tabla de encaminamiento y compruebe que hay respuesta al hacer ping hacia 10.0.0.101.

```
service network restart
route -n
ping -c3 10.0.0.101
```

26.3.2. Direcciones IP virtuales

Este ejercicio considera lo siguiente:

1. Se tiene dos (o más) equipos de computo con GNU/Linux instalado en éstos.

2. **pc1.dominio** tiene una dirección IP 192.168**.0.**101 con máscara de subred 255.255.255.0 en el dispositivo eth0. No tiene otros dispositivos de red activos.

3. **pc2.dominio** tiene una dirección IP 192.168**.0.**102 con máscara de subred 255.255.255.0 en el dispositivo eth0. No tiene otros dispositivos de red activos.

Visualice las interfaces de red activas en el sistema.

```
ifconfig
```

Lo anterior debe devolver una salida similar a la siguiente, donde se mostrará que sólo están activas la interfaz **eth0** y la correspondiente al retorno del sistema (loopback):

```
eth0      Link encap:Ethernet  HWaddr 00:01:02:03:04:05
          inet addr:192.168.0.101  Bcast:192.168.0.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24784 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23366 errors:0 dropped:0 overruns:0 carrier:0
          collisions:112 txqueuelen:1000
          RX bytes:15323317 (14.6 MiB)  TX bytes:5794288 (5.5 MiB)
          Interrupt:11 Base address:0xd000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1337 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1337 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:125102 (122.1 KiB)  TX bytes:125102 (122.1 KiB)
```

Utilice **ping** para comprobar si acaso hay alguna respuesta desde la interfaz virtual **eth0:0**.

```
ping -c3 192.168.1.101
```

Lo anterior debe devolver una salida similar a la siguiente:

```
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.

--- 192.168.1.101 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

Configure, a través de **ifconfig,** los parámetros de la interfaz virtual **eth0:0**. Si la sintaxis fue correcta, el sistema no deberá devolver mensaje alguno.

```
ifconfig eth0:0 192.168.1.101 netmask 255.0.0.0
```

Utilice **ping** para comprobar que haya respuesta desde la interfaz virtual **eth0:0**.

```
ping -c3 192.168.1.101
```

Lo anterior debe devolver una salida similar a la siguiente:

```
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=0 ttl=64 time=0.453 ms
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.347 ms

--- 192.168.1.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.347/0.389/0.453/0.048 ms, pipe 2
```

Visualice las interfaces de red activas en el sistema.

```
ifconfig
```

Lo anterior debe devolver una salida similar a la siguiente, donde se mostrará que está activa la interfaz **eth0:0** junto con la interfaz **eth0** y la correspondiente al retorno del sistema (loopback):

```
eth0      Link encap:Ethernet  HWaddr 00:01:02:03:04:05
          inet addr:192.168.0.101  Bcast:192.168.0.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24784 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23366 errors:0 dropped:0 overruns:0 carrier:0
          collisions:112 txqueuelen:1000
          RX bytes:15323317 (14.6 MiB)  TX bytes:5794288 (5.5 MiB)
          Interrupt:11 Base address:0xd000

eth0:0    Link encap:Ethernet  HWaddr 00:01:02:03:04:05
          inet addr:192.168.1.101  Bcast:192.168.1.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:11 Base address:0xd000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1337 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1337 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:125102 (122.1 KiB)  TX bytes:125102 (122.1 KiB)
```

Reinicie el servicio de red.

```
service network restart
```

Utilice **ping** para comprobar si aún hay respuesta desde la interfaz virtual **eth0:0**.

```
ping -c3 192.168.1.101
```

Lo anterior debe devolver una salida similar a la siguiente:

```
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.

--- 192.168.1.101 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

Visualice las interfaces de red activas en el sistema.

```
ifconfig
```

Lo anterior debe devolver una salida similar a la siguiente, donde se mostrará que ya no está activa la interfaz **eth0:0**, y sólo se muestran activas la interfaz **eth0** y la correspondiente al retorno del sistema (loopback):

```
eth0      Link encap:Ethernet  HWaddr 00:01:02:03:04:05
          inet addr:192.168.0.101  Bcast:192.168.0.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24784 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23366 errors:0 dropped:0 overruns:0 carrier:0
          collisions:112 txqueuelen:1000
          RX bytes:15323317 (14.6 MiB)  TX bytes:5794288 (5.5 MiB)
          Interrupt:11 Base address:0xd000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1337 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1337 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:125102 (122.1 KiB)  TX bytes:125102 (122.1 KiB)
```

Para hacer permanente la interfaz de red virtual en **eth0:0** utilice un editor de texto el fichero **/etc/sysconfig/network-scripts/ifcfg-eth0:0** y ponga el siguiente contenido **(¡Respete mayúsculas y minúsculas!)**:

```
DEVICE=eth0:0
IPADDR=192.168.1.101
NETMASK=255.255.255.0
```

Reinicie el servicio de red.

```
service network restart
```

Visualice las interfaces de red activas en el sistema.

```
ifconfig
```

Lo anterior debe devolver una salida similar a la siguiente, donde nuevamente se mostrará que está activa la interfaz **eth0:0** junto con la interfaz **eth0** y la correspondiente al retorno del sistema (loopback):

```
eth0      Link encap:Ethernet  HWaddr 00:01:02:03:04:05
          inet addr:192.168.0.101  Bcast:192.168.0.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24784 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23366 errors:0 dropped:0 overruns:0 carrier:0
          collisions:112 txqueuelen:1000
          RX bytes:15323317 (14.6 MiB)  TX bytes:5794288 (5.5 MiB)
          Interrupt:11 Base address:0xd000

eth0:0    Link encap:Ethernet  HWaddr 00:01:02:03:04:05
          inet addr:192.168.1.101  Bcast:192.168.1.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:11 Base address:0xd000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1337 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1337 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:125102 (122.1 KiB)  TX bytes:125102 (122.1 KiB)
```

Utilice **ping** para comprobar que haya respuesta desde la interfaz virtual **eth0:0**.

```
ping -c3 192.168.1.101
```

Lo anterior debe devolver una salida similar a la siguiente:

```
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=0 ttl=64 time=0.453 ms
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.347 ms

--- 192.168.1.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.347/0.389/0.453/0.048 ms, pipe 2
```

La interfaz **eth0:0** estará activa la siguiente vez que inicie el sistema operativo con la dirección IP y máscara de subred asignados.

27. Cómo utilizar Netcat (nc)

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

27.1. Introducción.

27.1.1. Acerca de Netcat.

Netcat, o **nc** que es la forma en que se utiliza en el intérprete de mandatos, es una herramienta utilizada para supervisar y escribir sobre conexiones tanto por **TCP** como por **UDP**. Puede abrir conexiones **TCP**, enviar paquetes **UDP**, escuchar sobre puertos arbitrarios tanto **TCP** como **UDP**, supervisión de puertos y más, tanto para **IPv4** como **IPv6**. Es una de las herramientas de diagnóstico y seguridad más populares y también una de las mejor calificadas por la comunidad.

27.2. Procedimientos.

27.2.1. Conexiones simples.

Para iniciar una conexión hacia algún puerto en algún sistema, se utiliza el mandato **nc** seguido de una dirección **IP** y un puerto al cual conectarse. En el siguiente ejemplo se realizará una conexión hacia el puerto 25 (**SMTP**) de **127.0.0.1**:

```
nc 127.0.0.1 25
```

Si hay un servidor de correo funcionado, lo anterior puede devolver una salida similar a la siguiente:

```
220 localhost.localdomain ESMTP ; Wed, 28 May 2008 10:24:52 -0500
quit
221 2.0.0 localhost.localdomain closing connection
```

27.2.2. Revisión de puertos.

Para revisar los puertos abiertos, se utiliza **nc** con la opción , **-z** para solicitar se trate de escuchar por puertos abiertos, y un puerto o rango de puertos. En el siguiente ejemplo, se pide al mandato **nc** revisar la presencia de puertos abiertos **TCP** (modo predeterminado) entre el rango del puerto 21 al

25.

```
nc -vz 127.0.0.1 21-25
```

Lo anterior puede devolver una salida como la siguiente, si se encontrasen abiertos los puertos 21, 22 y 25.

```
Connection to 127.0.0.1 21 port [tcp/ftp] succeeded!
Connection to 127.0.0.1 22 port [tcp/ssh] succeeded!
Connection to 127.0.0.1 25 port [tcp/smtp] succeeded!
```

Opcionalmente se pueden revisar si están abiertos los puertos abiertos por UDP añadiendo la opción -u. En el siguiente ejemplo se solicita al mandato **nc** revisar que puertos **UDP** abiertos que se encuentran entre el rango del puerto 21 al 80.

```
nc -zu 127.0.0.1 21-80
```

Lo anterior puede devolver una salida como la siguiente si se encuentran abiertos los puertos **UDP** 53, 67 y 68:

```
Connection to 127.0.0.1 53 port [udp/domain] succeeded!
Connection to 127.0.0.1 67 port [udp/bootps] succeeded!
Connection to 127.0.0.1 68 port [udp/bootpc] succeeded!
```

Si se quiere obtener una salida más descriptiva, solo es necesario especificar **nc -vz** y la dirección **IP** si se quiere revisar puertos **TCP** abiertos, o bien **nc -vzu** para puertos **UDP** abiertos, donde **-v** define se devuelva una salida **más descriptiva**. En el siguiente ejemplo se pide al mandato **nc** revisar los puertos **TCP** abiertos entre el puerto 20 al 25.

nc -vz 127.0.0.1

La salida de lo anterior devolverá, a diferencia de utilizar solo -z, que puertos están cerrados.

```
nc: connect to 127.0.0.1 port 20 (tcp) failed: Connection refused
Connection to 127.0.0.1 21 port [tcp/ftp] succeeded!
Connection to 127.0.0.1 22 port [tcp/ssh] succeeded!
nc: connect to 127.0.0.1 port 23 (tcp) failed: Connection refused
nc: connect to 127.0.0.1 port 24 (tcp) failed: Connection refused
Connection to 127.0.0.1 25 port [tcp/smtp] succeeded!
```

27.2.3. Creando un modelo cliente servidor.

Es relativamente simple crear un modelo cliente/servidor. Desde una terminal que será utilizada para iniciar un modelo de servidor, se utiliza el mandato **nc** con la opción **-l** (listen o escuchar) seguida de un puerto que esté desocupado. Esto hará que nc se comporte como servidor escuchando peticiones en un puerto arbitrario. En el siguiente ejemplo se hará que mandato **nc** funcione como servidor escuchando peticiones en el puerto **22222**.

```
nc -l 22222
```

Para establecer la conexión como cliente, desde otra terminal se inicia el mandato nc especificando a continuación una IP local para el sistema y el numero de puerto al que se quiera conectar. En el

siguiente ejemplo se realiza la conexión al puerto **22222** de **127.0.0.1**

```
nc 127.0.0.1 22222
```

Todo lo que se escriba desde la terminal como cliente podrá ser visto en la terminal como servidor.

27.2.4. Transferencia de datos.

Tomando el ejemplo anterior, es posible realizar transferencia de datos desde una terminal como cliente hacia una terminal como servidor. La única diferencia es que en el servidor se cambia las salida estándar de la terminal hacia un fichero del siguiente modo:

```
nc -l 22222 > algo.out
```

En el cliente se realiza algo similar. En lugar de ingresar datos desde la conexión. se hace a partir de un fichero con contenido de la siguiente forma:

```
nc 127.0.0.1 22222 < algo.in
```

En el ejemplo descrito se realiza la transferencia de datos del fichero **algo.in**, desde el proceso como cliente, hacia el fichero **algo.out**, en el proceso como servidor.

28. Como utilizar Netstat.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

28.1. Introducción.

28.1.1. Acerca de Netstat

Netstat es una herramienta utilizada para supervisar las conexiones de red, tablas de encaminamiento, estadísticas de interfaces y asignaturas de multidifusión. Se utiliza principalmente para encontrar problemas en una red y para medir el tráfico de red como una forma de calcular el desempeño de ésta.

28.2. Procedimientos.

Para visualizar todas las conexiones activas en el sistema, tanto TCP como UDP, se utiliza la opción -a.

```
netstat -a
```

Debido a que la cantidad de datos puede ser mucha para ser visualizada con comodidad en la pantalla del monitor, se puede utilizar el mandato less como subrutina.

```
netstat -a | less
```

A continuación se muestra un ejemplo de la salida:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:netbios-ssn               *:*                         LISTEN
tcp        0      0 *:submission                *:*                         LISTEN
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:x11                       *:*                         LISTEN
tcp        0      0 *:5904                      *:*                         LISTEN
tcp        0      0 *:webcache                  *:*                         LISTEN
udp        0      0 *:filenet-tms               *:*
udp        0      0 *:filenet-nch               *:*
udp        0      0 *:filenet-rmi               *:*
udp        0      0 *:filenet-pa                *:*
```

```
udp        0      0 192.168.122.1:netbios-ns    *:*
udp        0      0 servidor00.c:netbios-ns     *:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     17530  @/tmp/fam-root-
unix  2      [ ACC ]     STREAM     LISTENING     7944   /dev/gpmctl
unix  2      [ ACC ]     STREAM     LISTENING     6991   /var/run/audit_events
unix  2      [ ACC ]     STREAM     LISTENING     7409   /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     7506   /var/run/pcscd.comm
unix  2      [ ACC ]     STREAM     LISTENING     7647   /var/run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     7737   /var/run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     16795  @/tmp/dbus-4Uato6eJUH
```

Para mostrar solo las conexiones activas por TCP, se utiliza:

```
netstat -t
```

Para mostrar solo las conexiones activas por UDP, se utiliza:

```
netstat -u
```

Para mostrar las estadísticas de uso para todos los tipos de conexiones, se utiliza:

```
netstat -s
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Ip:x  2      [ ]         DGRAM                    8015
    8005 total packets received                   7929
    2 with invalid addressesAM                    7896
    0 forwarded]         DGRAM                    7866
    0 incoming packets discarded                  7505
    7928 incoming packets delivered CONNECTED     7412
    7905 requests sent outTREAM     CONNECTED     7411
Icmp: 3      [ ]         STREAM     CONNECTED     7349
    19 ICMP messages receivedAM     CONNECTED     7348
    0 input ICMP message failed.                  7199
    ICMP input histogram:DGRAM                    7071
        destination unreachable: 18               6947
        echo requests: 1 DGRAM                    6917
    19 ICMP messages sentSTREAM     CONNECTED     6845
    0 ICMP messages failedTREAM     CONNECTED     6844
    ICMP output histogram:a | less
        destination unreachable: 18
        echo replies: 1
Tcp:
    114 active connections openings
    2 passive connection openings
    0 failed connection attempts
    12 connection resets received
    0 connections established
    7622 segments received
    7533 segments send out
    68 segments retransmited
    0 bad segments received.
    17 resets sent
```

```
Udp:
    287 packets received
    0 packets to unknown port received.
    0 packet receive errors
    279 packets sent
TcpExt:
    7 TCP sockets finished time wait in fast timer
    135 delayed acks sent
    Quick ack mode was activated 26 times
    61 packets directly queued to recvmsg prequeue.
    18364064 packets directly received from backlog
    3912320 packets directly received from prequeue
    2081 packets header predicted
    1525 packets header predicted and directly queued to user
    475 acknowledgments not containing data received
    1311 predicted acknowledgments
    1 times recovered from packet loss due to SACK data
    1 congestion windows fully recovered
    4 congestion windows partially recovered using Hoe heuristic
    13 congestion windows recovered after partial ack
    0 TCP data loss events
    4 timeouts after SACK recovery
    1 fast retransmits
    47 other TCP timeouts
    22 DSACKs sent for old packets
    1 DSACKs received
    9 connections reset due to early user close
```

Para mostrar solamente las estadísticas originadas por conexiones TCP, se utiliza:

```
netstat -s -t
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Tcp:
    114 active connections openings
    2 passive connection openings
    0 failed connection attempts
    12 connection resets received
    0 connections established
    7622 segments received
    7533 segments send out
    68 segments retransmited
    0 bad segments received.
    17 resets sent
TcpExt:
    7 TCP sockets finished time wait in fast timer
    135 delayed acks sent
    Quick ack mode was activated 26 times
    61 packets directly queued to recvmsg prequeue.
    18364064 packets directly received from backlog
    3912320 packets directly received from prequeue
    2081 packets header predicted
    1525 packets header predicted and directly queued to user
    475 acknowledgments not containing data received
```

```
    1311 predicted acknowledgments
    1 times recovered from packet loss due to SACK data
    1 congestion windows fully recovered
    4 congestion windows partially recovered using Hoe heuristic
    13 congestion windows recovered after partial ack
    0 TCP data loss events
    4 timeouts after SACK recovery
    1 fast retransmits
    47 other TCP timeouts
    22 DSACKs sent for old packets
    1 DSACKs received
    9 connections reset due to early user close
```

Para mostrar solamente las estadísticas originadas por conexiones TCP, se utiliza:

```
netstat -s -u
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Udp:
    287 packets received
    0 packets to unknown port received.
    0 packet receive errors
    279 packets sent
```

Para mostrar la tabla de encaminamientos, se utiliza:

```
netstat -r
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.0.0     *               255.255.255.0   U         0 0          0 eth0
192.168.122.0   *               255.255.255.0   U         0 0          0 virbr0
169.254.0.0     *               255.255.0.0     U         0 0          0 eth0
default         192.168.0.254   0.0.0.0         UG        0 0          0 eth0
```

Para mostrar las asignaciones grupos de multidifusión, se utiliza:

```
netstat -g
```

Lo anterior puede devolver una salida similar a la siguiente:

```
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      ALL-SYSTEMS.MCAST.NET
virbr0          1      224.0.0.251
virbr0          1      ALL-SYSTEMS.MCAST.NET
eth0            1      224.0.0.251
eth0            1      ALL-SYSTEMS.MCAST.NET
lo              1      ff02::1
```

```
peth0            1      ff02::1
virbr0           1      ff02::1:ff00:0
virbr0           1      ff02::1
vif0.0           1      ff02::1
eth0             1      ff02::1:ff56:18b9
eth0             1      ff02::1
xenbr0           1      ff02::1
vif1.0           1      ff02::1
```

Para mostrar la tabla de interfaces activas en el sistema, se utiliza:

```
netstat -i
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500   0     2397      0      0      0     2079      0      0      0 BMRU
lo        16436   0     5780      0      0      0     5780      0      0      0 LRU
peth0      1500   0     3294      0      0      0     2584      0      0      0 BORU
vif0.0     1500   0     2079      0      0      0     2397      0      0      0 BORU
vif1.0     1500   0       45      0      0      0      384      0      0      0 BORU
virbr0     1500   0        0      0      0      0       72      0      0      0 BMRU
xenbr0     1500   0      216      0      0      0        0      0      0      0 BORU
```

29. Cómo utilizar ARP.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

29.1. Introducción

29.1.1. Acerca de ARP.

ARP significa **A**ddress **R**esolution **P**rotocol, o protocolo de resolución de direcciones. **ARP** se utiliza para **supervisar y modificar** la tabla de asignaciones de direcciones **IP** y direcciones **MAC** (**M**edia **A**ccess **C**ontrol). **ARP** utiliza un cache que consiste en una tabla que almacena las asignaciones entre nivel de enlace de datos y las direcciones IP del nivel de red. El nivel de enlace de datos se encarga de gestionar las direcciones **MAC** y el nivel de red de las direcciones **IP**. **ARP** asocia direcciones **IP** a las direcciones **MAC**, justo a la inversa del protocolo **RARP** que asigna direcciones **MAC** a las direcciones **IP**. Para reducir el número de peticiones **ARP**, cada sistema operativo que implementa el protocolo **ARP** mantiene una cache en la **memoria RAM** de todas las recientes asignaciones.

29.2. Procedimientos.

Visualizar el cache **ARP** actual.

```
arp -a
```

Debe devolver algo similar a lo siguiente, en el caso de tratarse de un solo sistema:

```
m254.alcancelibre.org (192.168.1.254) at 00:14:95:97:27:E9 [ether] on eth0
```

Cuando se trata de un servidor intermediario (proxy), la tabla puede verse de este modo:

```
m051.redlocal.net (10.1.1.51) at 00:13:20:D0:09:1E [ether] on eth1
m046.redlocal.net (10.1.1.46) at 00:0F:1F:B1:71:14 [ether] on eth1
m073.redlocal.net (10.1.1.73) at 00:11:25:F6:93:F1 [ether] on eth1
m070.redlocal.net (10.1.1.70) at 00:11:25:F6:A2:52 [ether] on eth1
m040.redlocal.net (10.1.1.40) at 00:0D:60:6E:27:34 [ether] on eth1
```

```
m036.redlocal.net (10.1.1.36) at 00:0D:60:6E:25:FB [ether] on eth1
m011.redlocal.net (10.1.1.11) at 00:11:2F:C7:D0:D7 [ether] on eth1
```

El mandato **arp** acepta varias opciones más. Si se desea visualizar la información en estilo Linux, se utiliza el parámetro -e. ejemplo:

```
arp -e
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
m051.redlocal.net        ether   00:13:20:D0:09:1E   C                     eth1
m046.redlocal.net        ether   00:0F:1F:B1:71:14   C                     eth1
m073.redlocal.net        ether   00:11:25:F6:A2:52   C                     eth1
m070.redlocal.net        ether   00:11:25:F6:95:8E   C                     eth1
m040.redlocal.net        ether   00:0D:60:6E:26:6F   C                     eth1
m036.redlocal.net        ether   00:11:25:F6:5F:81   C                     eth1
```

Si se desea observar lo anterior en formato numérico, se utiliza el parámetro -n. ejemplo:

```
arp -n
```

Lo anterior debe devolver algo similar a lo siguiente:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
10.1.1.46                ether   00:0F:1F:B1:71:14   C                     eth1
10.1.1.70                ether   00:11:25:F6:A2:52   C                     eth1
10.1.1.73                ether   00:11:25:F6:93:F1   C                     eth1
10.1.1.40                ether   00:0D:60:6E:27:34   C                     eth1
10.1.1.34                ether   00:0D:60:6E:26:6F   C                     eth1
```

Si se desea especificar una interfaz en particular, se utiliza el parámetro -i seguido del nombre de la interfaz. Ejemplo:

```
arp -i eth0
```

Lo anterior debe regresar algo similar a lo siguiente, en el caso de tratarse de un solo sistema:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
m254.alcancelibre.org    ether   00:14:95:97:27:E9   C                     eth0
```

Si se desea añadir un registro manualmente, se puede hacer utilizando el parámetro -s seguido del nombre de un anfitrión y la dirección MAC correspondiente. Ejemplo:

```
arp -s m200.redlocal.net 00:08:A1:84:18:AD
```

Si se quiere eliminar un registro de la tabla, solo se utiliza el parámetro **-d** seguido del nombre del anfitrión a eliminar. Ejemplo:

```
arp -d m200.redlocal.net
```

Para limpiar todo el cache, se puede utilizar un bucle como el siguiente:

```
for i in `arp -n | awk '{print $1}' | grep -v Address`
do
arp -d $i
done
```

En el guión anterior se pide crear la variable *i* a partir de **arp** con la opción **-n** para devolver las direcciones numéricas, mostrando a través de **awk** solo la primera columna de la tabla generada, y eliminando la cadena de caracteres **Address**. Esto genera una lista de direcciones IP que se asignan como valores de la variable *i* en el bucle, donde se elimina cada una de estas direcciones IP utilizando **arp -d**.

El objeto de limpiar el cache de **ARP** es permitir corregir los registros de la tabla en ciertos escenarios donde, por ejemplo, un servidor o estación de trabajo fue encendido con una dirección **IP** que ya está uso.

30. Introducción a IPTABLES

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

30.1. Introducción.

30.1.1. Acerca de Iptables y Netfilter.

Netfilter es un conjunto de *ganchos* (**Hooks**, es decir, técnicas de programación que se emplean para crear cadenas de procedimientos como manejador) dentro del núcleo de GNU/Linux y que son utilizados para interceptar y manipular paquetes de red. El componente mejor conocido es el cortafuegos, el cual realiza procesos de filtración de paquetes. Los *ganchos* son también utilizados por un componente que se encarga del **NAT** (acrónimo de **N**etwork **A**ddress **T**ranslation o Traducción de dirección de red). Estos componentes son cargados como módulos del núcleo.

Iptables es el nombre de la herramienta de espacio de usuario (**User Space**, es decir, área de memoria donde todas las aplicaciones, en modo de usuario, pueden ser intercambiadas hacia memoria virtual cuando sea necesario) a través de la cual los administradores crean reglas para cada filtrado de paquetes y módulos de **NAT**. **Iptables** es la herramienta estándar de todas las distribuciones modernas de GNU/Linux.

URL: http://www.netfilter.org/

30.2. Equipamiento lógico necesario.

30.2.1. Instalación a través de yum.

Si utiliza **CentOS 4** y **5**, **Red Hat Enterprise Linux 5** o **White Box Enterprise Linux 4** y **5**, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install iptables
```

30.2.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date –i iptables
```

30.3. Procedimientos.

30.3.1. Cadenas.

Las cadenas pueden ser para tráfico entrante (INPUT), tráfico saliente (OUTPUT) o tráfico reenviado (**FORWARD**).

30.3.2. Reglas de destino.

Las reglas de destino pueden ser aceptar conexiones (**ACCEPT**), descartar conexiones (**DROP**), rechazar conexiones (**REJECT**), encaminamiento posterior (**POSTROUTING**), encaminamiento previo (**PREROUTING**), **SNAT**, **NAT**, entre otras.

30.3.3. Políticas por defecto.

Establecen cual es la acción a tomar por defecto ante cualquier tipo de conexión. La opeción -P cambia una política para una cadena. En el siguiente ejemplo se descartan (**DROP**) todas las conexiones que ingresen (INPUT), todas las conexiones que se reenvíen (**FORWARD**) y todas las conexiones que salgan (OUTPUT), es decir, se descarta todo el tráfico que entre desde una red pública y el que trate de salir desde la red local.

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```

30.3.4. Limpieza de reglas específicas.

A fin de poder crear nuevas reglas, se deben borrar las existentes, para el tráfico entrante, tráfico reenviado y tráfico saliente así como el NAT.

```
iptables -F INPUT
iptables -F FORWARD
iptables -F OUTPUT
iptables -F -t nat
```

30.3.5. Reglas específicas.

Las opciones más comunes son:

- -A añade una cadena, la opción -i define una interfaz de tráfico entrante
- -o define una interfaz para trafico saliente
- -j establece una regla de destino del tráfico, que puede ser **ACCEPT**, **DROP** o **REJECT**. La
- -m define que se aplica la regla si hay una coincidencia específica
- --state define una lista separada por comas de distinto tipos de estados de las conexiones (INVALID, ESTABLISHED, NEW, RELATED).
- --to-source define que IP reportar al tráfico externo
- -s define trafico de origen
- -d define tráfico de destino
- --source-port define el puerto desde el que se origina la conexión

- --destination-port define el puerto hacia el que se dirige la conexión
- -t tabla a utilizar, pueden ser nat, filter, mangle o raw.

Ejemplos de reglas.

Reenvío de paquetes desde una interfaz de red local (eth1) hacia una interfaz de red pública (eth0):

```
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

Aceptar reenviar los paquetes que son parte de conexiones existentes (ESTABLISHED) o relacionadas de tráfico entrante desde la interfaz eth1 para tráfico saliente por la interfaz eth0:

```
iptables -A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Permitir paquetes en el propio muro cortafuegos para tráfico saliente a través de la interfaz eth0 que son parte de conexiones existentes o relacionadas:

```
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Permitir (**ACCEPT**) todo el tráfico entrante (INPUT) desde (**-s**) cualquier dirección (0/0) la red local (eth1) y desde el retorno del sistema (lo) hacia (**-d**) cualquier destino (0/0):

```
iptables -A INPUT -i eth1 -s 0/0 -d 0/0 -j ACCEPT
iptables -A INPUT -i lo -s 0/0 -d 0/0 -j ACCEPT
```

Hacer (-j) SNAT para el tráfico saliente (**-o**) a tráves de la interfaz eth0 proveniente desde (**-s**) la red local (**192.168.0.0/24**) utilizando (--to-source) la dirección IP **w.x.y.z**.

```
iptables -A POSTROUTING -t nat -s 192.168.0.0/24 -o eth0 -j SNAT --to-source x.y.z.c
```

Descartar (**DROP**) todo el tráfico entrante (**-i**) desde la interfaz eth0 que trate de utilizar la dirección IP pública del servidor (**w.x.y.z**), alguna dirección IP de la red local (**192.168.0.0/24**) o la dirección IP del retorno del sistema (127.0.01)

```
iptables -A INPUT -i eth0 -s w.x.y.x/32 -j DROP
iptables -A INPUT -i eth0 -s 192.168.0.0/24 -j DROP
iptables -A INPUT -i eth0 -s 127.0.0.0/8 -j DROP
```

Aceptar (**ACCEPT**) todos los paquetes SYN (--syn) del protocolo TCP (-p tcp) para los puertos (**--destination-port**) de los protocolos SMTP (25), HTTP(80), HTTPS (443) y SSH (22):

```
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 25 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 80 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 443 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 22 --syn -j ACCEPT
```

Aceptar (**ACCEPT**) todos los paquetes SYN (--syn) del protocolo TCP (-tcp) para los puertos (**--destination-port**) del protocolos SMTP (25) en el servidor (**w.x.y.z**/32), desde (**-s**) cualquier lugar (0/0) hacia (**-d**) cualquier lugar (0/0).

```
iptables -A INPUT -p tcp -s 0/0 -d w.x.y.z/32 --destination-port 25 --syn -j ACCEPT
```

Aceptar (**ACCEPT**) todos los paquetes SYN (--syn) del protocolo TCP (-p tcp) para los puertos (**--destination-port**) de los protocolos POP3 (110), POP3S (995), IMAP (143) y IMAPS (993):

```
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 110 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 995 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 143 --syn -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 0/0 --destination-port 993 --syn -j ACCEPT
```

Aceptar (**ACCEPT**) el tráfico entrante (**-i**) proveniente desde la interfaz eth1 cuando las conexiones se establezcan desde el puerto (--sport) 67 por protocolos (**-p**) TCP y UDP.

```
iptables -A INPUT -i eth1 -p tcp --sport 68 --dport 67 -j ACCEPT
iptables -A INPUT -i eth1 -p udp --sport 68 --dport 67 -j ACCEPT
```

Aceptar (**ACCEPT**) conexiones de tráfico entrante (INPUT) por protocolo (**-p**) UDP cuando se establezcan desde (**-s**) el servidor DNS 200.33.145.217 desde el puerto (**--source-port**) 53 hacia (**-d**) cualquier destino (0/0):

```
iptables -A INPUT -p udp -s 200.33.146.217/32 --source-port 53 -d 0/0 -j ACCEPT
```

30.3.5.1. Cerrar accesos.

Descartar (**DROP**) el tráfico entrante (INPUT) para el protocolo (**-p**) TCP hacia los puerto (**--destination-port**) de SSH (22) y Telnet (23):

```
iptables -A INPUT -p tcp --destination-port 22 -j DROP
iptables -A INPUT -p tcp --destination-port 23 -j DROP
```

Descartar (**DROP**) todo tipo de conexiones de tráfico entrante (INPUT) desde (**-s**) la dirección IP a.b.c.d:

```
iptables -A INPUT -s a.b.c.d -j DROP
```

Rechazar (**REJECT**) conexiones hacia (OUTPUT) la dirección IP a.b.c.d desde la red local:

```
iptables -A OUTPUT -d a.b.c.d -s 192.168.0.0/24 -j REJECT
```

30.3.6. Eliminar reglas.

En general se utiliza la misma regla, pero en lugar de utilizar -A (append), se utiliza -D (delete).

Elininar la regla que descarta (**DROP**) todo tipo de conexiones de tráfico entrante (INPUT) desde (**-s**) la dirección IP a.b.c.d:

```
iptables -D INPUT -s a.b.c.d -j DROP
```

30.3.7. Mostrar la lista de cadenas y reglas.

Una vez cargadas todas las cadenas y reglas de **iptables** es posible visualizar éstas utilizando el mandato **iptables** con las opciones **-n**, para ver las listas en formato numérico, y -**L**, para solicitar la lista de éstas cadenas.

```
iptables -nL
```

Cuando no hay reglas ni cadenas cargadas, la salida **debe** devolver lo siguiente:

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Cuando hay cadenas presentes, la salida, suponiendo que se utilizarón los ejemplos de este documento, debe devolver algo similar a lo siguiente:

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
DROP       all  --  192.168.1.64         0.0.0.0/0
DROP       all  --  172.16.0.0/24        0.0.0.0/0
DROP       all  --  127.0.0.0/8          0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:25 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            192.168.1.64        tcp dpt:25 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:110 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:995 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:143 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:993 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:68 dpt:67
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:68 dpt:67
ACCEPT     udp  --  200.33.146.217       0.0.0.0/0           udp spt:53

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@m064 ~]# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
DROP       all  --  192.168.1.64         0.0.0.0/0
DROP       all  --  172.16.0.0/24        0.0.0.0/0
DROP       all  --  127.0.0.0/8          0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:25 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            192.168.1.64        tcp dpt:25 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:110 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:995 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:143 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:993 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:68 dpt:67
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:68 dpt:67
ACCEPT     udp  --  200.33.146.217       0.0.0.0/0           udp spt:53
```

```
Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

30.3.8. Iniciar, detener y reiniciar el servicio iptables.

Si está de acuerdo con las reglas generadas de **iptables**, utilice el siguiente mandato para guardar éstas:

```
service iptables save
```

Las reglas quedarán almacenadas en el fichero **/etc/sysconfig/iptables**.

Para ejecutar por primera vez el servicio **iptables**, utilice:

```
service iptables start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service iptables restart
```

Para detener el servicio **iptables** y borrar todas las reglas utilice:

```
service iptables stop
```

30.3.9. Agregar el servicio iptables al arranque del sistema.

Para hacer que el servicio de **iptables** esté activo con el siguiente inicio del sistema, en todos los niveles de corrida (2, 3, 4, y 5), se utiliza lo siguiente:

```
chkconfig iptables on
```

30.4. Bibliografía.

- Wikipedia: http://en.wikipedia.org/wiki/Iptables
- Dennis G. Allard y Don Cohen http://oceanpark.com/notes/firewall_example.html

31. Cómo configurar un servidor DHCP en una LAN

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

31.1. Introducción.

31.1.1. Acerca del protoclo DHCP.

DHCP (acrónimo de **D**ynamic Host **C**onfiguration **P**rotocol que se traduce Protocolo de configuración dinámica de servidores) es un protocolo que permite a dispositivos individuales en una red de direcciones IP obtener su propia información de configuración de red (dirección IP; máscara de sub-red, puerta de enlace, etc.) a partir de un servidor DHCP. Su propósito principal es hacer más fáciles de administrar las redes grandes. **DHCP** existe desde 1993 como protocolo estándar y se describe a detalle en el RFC 2131.

Sin la ayuda de un servidor **DHCP**, tendrían que configurarse de forma manual cada dirección IP de cada anfitrión que pertenezca a una Red de Área Local. Si un anfitrión se traslada hacia otra ubicación donde existe otra Red de Área Local, se tendrá que configurar otra dirección IP diferente para poder unirse a esta nueva Red de Área Local. Un servidor **DHCP** entonces supervisa y distribuye las direcciones IP de una Red de Área Local asignando una dirección IP a cada anfitrión que se una a la Red de Área Local. Cuando, por mencionar un ejemplo, una computadora portátil se configura para utilizar **DHCP**, a ésta le será asignada una dirección IP y otros parámetros de red necesarios para unirse a cada Red de Área Local donde se localice.

Existen tres métodos de asignación en el protocolo **DHCP**:

- **Asignación manual**: La asignación utiliza una tabla con direcciones **MAC** (acrónimo de **M**edia **A**ccess **C**ontrol **A**ddress, que se traduce como dirección de Control de Acceso al Medio). Sólo los anfitriones con una dirección **MAC** definida en dicha tabla recibirá el IP asignada en la misma tabla. Ésto se hace a través de los parámetros **hardware ethernet** y **fixed-address**.
- **Asignación automática**: Una dirección de IP disponible dentro de un rango determinado se asigna permanentemente al anfitrión que la requiera.
- **Asignación dinámica**: Se determina arbitrariamente un rango de direcciones IP y cada anfitrión conectado a la red está configurada para solicitar su dirección IP al servidor cuando se inicia el dispositivo de red, **utilizando un intervalo de tiempo controlable** (parámetros **default-lease-time** y **max-lease-time**) de modo que las direcciones IP no son permanentes y se reutilizan de forma dinámica.

URL: http://www.ietf.org/rfc/rfc2131.txt y http://www.ietf.org/rfc/rfc2132.txt

31.1.2. Acerca de dhcp por Internet Software Consortium, Inc.

Fundado en 1994, Internet Software Consortium, Inc., distribuye un conjunto de herramientas para el protocolo **DHCP**, las cuales consisten en:

- **Servidor DHCP**
- **Cliente DHCP**
- **Agente de retransmisión.**

Dichas herramientas utilizan un **API** (**A**pplication **P**rogramming **I**nterface o Interfaz de Programación de Aplicaciones) modular diseñado para ser lo suficientemente general para ser utilizado con facilidad en los sistemas operativos que cumplen el estándar **POSIX** (**P**ortable **O**perating **S**ystem **I**nterface for UNI**X** o interfaz portable de sistema operativo para Unix) y no-POSIX, como Windows.

URL: http://isc.org/products/DHCP/

31.2. Equipamiento lógico necesario.

31.2.1. Instalación a través de yum.

Si utiliza **CentOS 4** o **White Box Enterprise Linux 4**, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install dhcp
```

31.2.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date -i dhcp
```

31.3. Procedimientos.

31.3.1. Fichero de configuración /etc/dhcpd.conf.

Considerando **como ejemplo** que se tiene una red local con las siguientes características:

- Número de red 192.168.0.0
- Máscara de sub-red: 255.255.255.0
- Puerta de enlace: 192.168.0.1
- Servidor de nombres: 192.168.0.1, 148.240.241.42 y 148.240.241.10
- Servidor Wins: 192.168.0.1
- Servidores de tiempo (**NTP**): 0.pool.ntp.org, 1.pool.ntp.org y 2.pool.ntp.org
- Rango de direcciones IP a asignar de modo dinámico: 192.168.0.11-192.168.0.199
- Dos direcciones IP se asignarán como fijas (192.168.0.253 y 192.168.0.254) para las tarjetas de red con direcciones **MAC** (**M**edia **A**ccess **C**ontrol o Control de

Acceso de Medios) 00:50:BF:27:1C:1C y 00:01:03:DC:67:23.

NOTA: Es indispensable **conocer y entender perfectamente** todo lo anterior para poder continuar con este documento.

Puede utilizar el siguiente contenido de ejemplo **para adaptar y crear desde cero** un nuevo fichero **/etc/dhcpd.conf** que se ajuste a una red y conjunto de sistemas en particular.

```
ddns-update-style interim;
ignore client-updates;
shared-network miredlocal {
        subnet 192.168.0.0 netmask 255.255.255.0 {
        option routers 192.168.0.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.0.255;
        option domain-name "redlocal.net";
        option domain-name-servers 192.168.0.1, 148.240.241.42, 148.240.241.10;
        option netbios-name-servers 192.168.0.1;
        option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org;
        range 192.168.0.11 192.168.0.199;
        default-lease-time 21600;
        max-lease-time 43200;
        }
        host m253 {
                option host-name "m253.redlocal.net";
                hardware ethernet 00:50:BF:27:1C:1C;
                fixed-address 192.168.0.253;
                }
        host m254 {
                option host-name "m254.redlocal.net";
                hardware ethernet 00:01:03:DC:67:23;
                fixed-address 192.168.0.254;
                }
}
```

31.3.2. Fichero de configuración /etc/sysconfig/dhcpd.

Una buena medida de seguridad es hacer que el servicio **dhcpd** solo funcione a través de la interfaz de red utilizada por la LAN, esto en el caso de tener múltiples dispositivos de red. Edite el fichero **/etc/sysconfig/dhcpd** y agregue como argumento del parámetro **DHCPDARGS** el valor **eth0**, **eth1**, **eth2**, etc., o lo que corresponda. Ejemplo, considerando que **eth0** es la interfaz correspondiente a la LAN:

```
# Command line options here
DHCPDARGS=eth0
```

31.3.3. Iniciar, detener y reiniciar el servicio dhcpd.

Para iniciar por primera vez el servicio **dhcpd**, utilice:

```
/sbin/service dhcpd start
```

Para hacer que los cambios hechos a la configuración del servicio **dhcpd** surtan efecto, utilice:

```
/sbin/service dhcpd restart
```

Para detener el servicio **dhcpd**, utilice:

```
/sbin/service dhcpd stop
```

31.3.4. Agregar el servicio dhcpd al arranque del sistema.

Para hacer que el servicio de **dhcpd** esté activo con el siguiente inicio del sistema, en todos los niveles de corrida (2, 3, 4, y 5), se utiliza lo siguiente:

```
/sbin/chkconfig dhcpd on
```

31.4. Comprobaciones desde cliente DHCP.

Hecho lo anterior solo falta con configurar como interfaces DHCP las estaciones de trabajo que sean necesarias sin importar que sistema operativo utilicen.

Después de configurado e iniciado el servicio, desde una terminal como root **en otro sistema** que será utilizado como cliente, considerando que se tiene una interfaz de red denominada **eth0**, utilice los siguientes mandatos para desactivar la interfaz **eth0** y asignar una nueva dirección **IP** a través del servidor **dhcp**.

```
/sbin/ifdown eth0
/sbin/dhclient eth0
```

Lo anterior deberá devolver el mensaje *«Determinando la información IP para eth0...»* y el símbolo de sistema. Para corroborar, utilice el mandato **ifconfig** para visualizar los dispositivos de red activos en el sistema.

La configuración del dispositivo de red, considerando **como ejemplo** la interfaz eth0 con direción **MAC** 00:01:03:DC:67:23, solicitando los datos para los servidores **DNS**, correspondiente al fichero **/etc/sysconfig/network-scripts/ifcfg-eth0**, sería con el siguiente contenido:

```
DEVICE=eth0
ONBOOT=yes
USERCTL=yes
BOOTPROTO=dhcp
PEERDNS=yes
HWADDR=00:01:03:DC:67:23
TYPE=Ethernet
```

31.5. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir los puerto 67 y 68 por UDP (**BOOTPS** y **BOOTPC**, respectivamente).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** en un sistema con una zona (**net**), correspondería a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      udp     67,68
```

```
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** en un sistema con dos zonas (**net** y **loc**), donde solo se va a permitir el acceso al servicio **dhcpd** desde la red local, correspondería a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  loc     fw      udp     67,68
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

32. Cómo configurar vsftpd (Very Secure FTP Daemon)

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

32.1. Introducción.

32.1.1. Acerca del protocolo FTP.

FTP (**F**ile **T**ransfer **P**rotocol) o Protocolo de Transferencia de Archivos (o ficheros informáticos) es uno de los protocolos estándar más utilizados en Internet siendo el más idóneo para la transferencia de grandes bloques de datos a través de redes que soporten TCP/IP. El servicio utiliza los puertos 20 y 21, exclusivamente sobre TCP. El puerto 20 es utilizado para el flujo de datos entre cliente y servidor. El puerto 21 es utilizando para el envío de órdenes del cliente hacia el servidor. Prácticamente todos los sistemas operativos y plataformas incluyen soporte para FTP, lo que permite que cualquier computadora conectada a una red basada sobre TCP/IP pueda hacer uso de este servicio a través de un cliente FTP.

URL: http://tools.ietf.org/html/rfc959

32.1.2. Acerca de vsftpd.

Vsftpd (**V**ery **S**ecure **FTP** **D**aemon) es un equipamiento lógico utilizado para implementar servidores de archivos a través del protocolo **FTP**. Se distingue principalmente porque sus valores predeterminados son muy seguros y por su sencillez en la configuración, comparado con otras alternativas como ProFTPD y Wu-ftpd. Actualmente se presume que vsftpd es quizá el servidor **FTP** más seguro del mundo.

URL: http://vsftpd.beasts.org/

32.2. Equipamiento lógico necesario.

32.2.1. Instalación a través de yum.

Si utiliza **CentOS 4** o **White Box Enterprise Linux 4**, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install vsftpd
```

32.2.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o

actualizar el equipamiento lógico necesario:

```
up2date –i vsftpd
```

32.3. Ficheros de configuración.

/etc/vsftpd.user_list	Lista que definirá usuarios a enjaular o no a enjaular, dependiendo de la configuración.
/etc/vsftpd/vsftpd.conf	Fichero de configuración.

32.4. Procedimientos.

Utilice un editor de texto y modifique el fichero **/etc/vsftpd/vsftpd.conf**. A continuación analizaremos los parámetros a modificar o añadir, según serequiera para necesidades particulares.

32.4.1. Parámetro anonymous_enable.

Se utiliza para definir si se permitirán los accesos anónimos al servidor. Establezca como valor **YES** o **NO** de acuerdo a lo que se requiera.

```
anonymous_enable=YES
```

32.4.2. Parámetro local_enable.

Es particularmente interesante si se combina con la función de jaula (**chroot**). Establece si se van a permitir los accesos autenticados de los usuarios locales del sistema. Establezca como valor **YES** o **NO** de acuerdo a lo que se requiera.

```
local_enable=YES
```

32.4.3. Parámetro write_enable.

Establece si se permite el mandato **write** (escritura) en el servidor. Establezca como valor **YES** o **NO** de acuerdo a lo que se requiera.

```
write_enable=YES
```

32.4.4. Parámetro anon_upload_enable

Específica si los usuarios anónimos tendrán permitido subir contenido al servidor. Por lo general no es una función deseada, por lo que se acostubra desactivar ésta.

```
anon_upload_enable=NO
```

32.4.5. Parámetro anon_mkdir_write_enable

Específica si los usuarios anónimos tendrán permitido crear directorios en el servidor. Al igual que la nterior, por lo general no es una función deseada, por lo que se acostubra desactivar ésta.

```
anon_mkdir_write_enable=NO
```

32.4.6. Parámetro ftpd_banner.

Este parámetro sirve para establecer el banderín de bienvenida que será mostrado cada vez que un usuario acceda al servidor. Puede establecerse cualquier frase breve que considere conveniente.

```
ftpd_banner=Bienvenido al servidor FTP de nuestra empresa.
```

32.4.7. Estableciendo jaulas para los usuarios: parámetros chroot_local_user y chroot_list_file.

De modo predeterminado los usuarios del sistema que se autentiquen tendrán acceso a otros directorios del sistema fuera de su directorio personal. Si se desea recluir a los usuarios a solo poder utilizar su propio directorio personal, puede hacerse fácilmente con el parámetro **chroot_local_user** que habilitará la función de **chroot()** y los parámetros chroot_list_enable y chroot_list_file para establecer el fichero con la lista de usuarios que quedarán excluidos de la función **chroot()**.

```
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/vsftpd.chroot_list
```

Con lo anterior, cada vez que un usuario local se autentique en el servidor FTP, solo tendrá acceso a su propio directorio personal y lo que este contenga. **No olvide crear el fichero /etc/vsftpd/vsftpd.chroot_list, ya que de otro modo no arrancará el servicio vsftpd**.

```
touch /etc/vsftpd/vsftpd.chroot_list
```

32.4.8. Control del ancho de banda.

32.4.8.1. Parámetro anon_max_rate.

Se utiliza para limitar la tasa de transferencia en bytes por segundo para los usuarios anónimos, algo sumamente útil en servidores FTP de acceso público. En el siguiente ejemplo se limita la tasa de transferencia a 5 Kb por segundo para los usuarios anónimos:

```
anon_max_rate=5120
```

32.4.8.2. Parámetro local_max_rate.

Hace lo mismo que **anon_max_rate**, pero aplica para usuarios locales del servidor. En el siguiente ejemplo se limita la tasa de transferencia a 5 Kb por segundo para los usuarios locales:

```
local_max_rate=5120
```

32.4.8.3. Parámetro max_clients.

Establece el número máximo de clientes que podrán acceder simultáneamente hacia el servidor FTP. En el siguiente ejemplo se limitará el acceso a 5 clientes simultáneos.

```
max_clients=5
```

32.4.8.4. Parámetro max_per_ip.

Establece el número máximo de conexiones que se pueden realizar desde una misma dirección IP. Tome en cuenta que algunas redes acceden a través de un servidor intermediario (Proxy) o puerta de enlace y debido a esto podrían quedar bloqueados innecesariamente algunos accesos. en el siguiente ejemplo se limita el número de conexiones por IP simultáneas a 5.

```
max_per_ip=5
```

32.4.9. Iniciar, detener y reiniciar el servicio vsftpd.

A diferencia de otros servicios FTP como **Wu-ftpd**, el servicio **vsftpd** no requiere configurarse para trabajar sobre demanda, aunque tiene dicha capacidad. Por lo tanto no depende de servicio **xinetd**. La versión incluida en distribuciones como CentOS 4, Red Hat™ Enterprise Linux 4 y White Box Enterprise Linux 4 puede iniciar, detenerse o reiniciar a través de un guión similar a los del resto del sistema.

Para iniciar por primera vez el servicio, utilice:

```
service vsftpd start
```

Para hacer que los cambios hechos a la configuración surtan efecto, utilice:

```
service vsftpd restart
```

Para detener el servicio, utilice:

```
service vsftpd stop
```

32.4.10. Agregar el servicio al arranque del sistema.

Para hacer que el servicio de **vsftpd** esté activo con el siguiente inicio del sistema, en todos los niveles de corrida (2, 3, 4, y 5), se utiliza lo siguiente:

```
chkconfig vsftpd on
```

32.5. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir los puerto 20 y 21 por TCP (**FTP-DATA** y **FTP**, respectivamente).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     20,21
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

32.6. Ejercicio VSFTPD

Acceder como **root** al servidor correspondiente al equipo de trabajo y detener el servicio **vsftpd**.

```
service vsftpd stop
```

Se **eliminará** el paquete **vsftpd** del sistema y se eliminará todo resto de la configuración anterior para poder instalarlo nuevamente y poder comenzar con una nueva configuración.

```
yum -y remove vsftpd
rm -fr /etc/vsftpd
```

Se procede a instalar de nuevo el paquete **vsftpd**.

```
yum -y install vsftpd
```

Se edita el fichero de configuración utilizando **vim**. Este fichero tiene contenido, por lo que si aparece en blanco o como fichero nuevo, se debe salir del editor y verificar que esté correcta la ruta definida en el intérprete de mandatos.

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

Utilizando el documento titulado Cómo configurar vsftpd (Very Secure FTP Daemon)., configurar los siguientes parámetros donde además deberá explicar en un **reporte por escrito** en papel qué es lo que hace cada uno de estos parámetros con los valores que serán asignados en el ejercicio:

```
anonymous_enable=YES
local_enable=YES
write_enable=YES
anon_upload_enable=NO
anon_mkdir_write_enable=NO
ftpd_banner=Bienvenido al servidor FTP de nuestra institución.
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/vsftpd.chroot_list
anon_max_rate=25600
local_max_rate=51200
max_clients=4
max_per_ip=4
```

Es importante crear el fichero definido en el parámetro **chroot_list_file**. Si este faltase, el servicio de FTP no funcionará correctamente. Debe crearse con el mandato **touch** del siguiente modo:

```
touch /etc/vsftpd/vsftpd.chroot_list
```

Iniciar el servicio recién configurado.

```
service vsftpd start
```

Añadir el servicio **vsftpd** al arranque del sistema.

```
chkconfig vsftpd on
```

Crear la cuenta de usuario **pruebasftp**, asignando **/sbin/nologin** como intérprete de mandatos,asignando **/var/www/pruebasftp** como directorio de inicio, asignar apache como el grupo predeterminado para el usuario, y el criptograma **1Fvs3oU5c$4ff89riowPb1EmJ7O.QtD0** (que corresponde a 123qwe) como clave de acceso. Nota: al asignar la clave de acceso con este método, los signos $ siempre se escriben como secuencia de escape utilizando \, ya que de otra forma el sistema los interpretaría como variables de entorno.

```
useradd -s /sbin/nologin -m -d /var/www/pruebasftp -g apache --password
"\$1\$Fvs3oU5c\$4ff89riowPb1EmJ7O.QtD0" pruebasftp
```

NOTA: El mandato anterior es una sola línea en el intérprete de mandatos.

Se podrá apreciar la actividad de del servidor FTP recién configurado consultando el contenido del fichero **/var/log/xferlog**. Utilice el mandato **tail** con la opción **-f** para supervisar lo que ocurrirá al realizar una transferencia a través del servidor FTP.

```
tail -f /var/log/xferlog
```

Accediendo desde otro equipo hacia **127.0.0.1** con el usuario **pruebasftp** y la clave de acceso **123qwe**, realizar una transferencia accediendo con el mandato **ftp** y subiendo cualquier fichero con el mandato **mput** del **intérprete ftp**.

```
ftp 127.0.0.1

Connected to 127.0.0.1 (127.0.0.1).
220 (vsFTPd 2.0.5)
Name (127.0.0.1:root): pruebasftp
331 Please specify the password.
Password:123qwe
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> put manuales-HTML.tar.bz2
local: manuales-HTML.tar.bz2 remote: manuales-HTML.tar.bz2
227 Entering Passive Mode (127,0,0,1,87,94)
150 Ok to send data.
226 File receive OK.
37347 bytes sent in 0.000198 secs (1.8e+05 Kbytes/sec)
ftp> ls
227 Entering Passive Mode (127,0,0,1,78,114)
150 Here comes the directory listing.
-rw-r--r--    1 553      48          37347 May 30 23:26 manuales-HTML.tar.bz2
226 Directory send OK.
ftp> bye
221 Goodbye.
```

33. Cómo configurar pure-ftpd.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

33.1. Introducción.

33.1.1. Acerca del protocolo FTP.

FTP (**F**ile **T**ransfer **P**rotocol) o Protocolo de Transferencia de Archivos (o ficheros informáticos) es uno de los protocolos estándar más utilizados en Internet siendo el más idóneo para la transferencia de grandes bloques de datos a través de redes que soporten **TCP/IP**. El servicio utiliza los puertos 20 y 21, exclusivamente sobre **TCP**. El puerto 20 es utilizado para el flujo de datos entre cliente y servidor. El puerto 21 es utilizando para el envío de órdenes del cliente hacia el servidor. Prácticamente todos los sistemas operativos y plataformas incluyen soporte para FTP, lo que permite que cualquier computadora conectada a una red basada sobre TCP/IP pueda hacer uso de este servicio a través de un cliente FTP.

URL: http://tools.ietf.org/html/rfc959

33.1.2. Acerca de pure-ftpd.

Pure-ftpd es un equipamiento lógico para servidor FTP originalmente creado por Arnt Gulbrandsen, miembro de Troll Tech, responsables de la biblioteca Qt, base de KDE. A pesar de su escasa popularidad, se distingue de otros proyectos porque ha tenido como objetivos el mantener el servicio con poco consumo de recursos, no utiliza llamadas de mandatos externos (origen de la mayoría de los problemas de seguridad en este tipo de equipamiento lógico), cumple con los estándares para el protocolo FTP, es fácil de instalar y configurar, es amistoso con el usuario y muy seguro.

URL: http://www.pureftpd.org/

33.2. Equipamiento lógico necesario.

33.2.1. Instalación a través de yum.

Pure-ftpd no está incluido en la instalación estándar de **CentOS 5**, **Red Hat™ Enterprise Linux 5**

ni **White Box Enterprise Linux 5**. Está disponible para dichos sistemas operativos utilizando el siguiente depósito Yum, mantenido por **Alcance Libre**.

```
[alcance-libre]
name=Alcance Libre para Enterprise Linux 5
baseurl=http://www.alcancelibre.org/al/el/5/
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

Una vez configurado lo anterior, si utiliza **CentOS 5**, **Red Hat™ Enterprise Linux 5** o **White Box Enterprise Linux 5**, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install pure-ftpd
```

33.3. Procedimientos.

33.3.1. Fichero de configuración /etc/pure-ftpd/pure-ftpd.conf

Los valores predeterminados del fichero **/etc/pure-ftpd/pure-ftpd.conf** hacen que el servicio funcione sin necesidad de cambio alguno y además lo haga de una forma segura. sin embargo existen varios parámetros que vale la pena conocer.

33.3.1.1. Parámetro MaxClientsNumber.

Establece el número máximo de usuarios conectados de forma simultánea. El valor predeterminado es 50. Puede modificarse de acuerdo a un propósito en particular y disponibilidad de ancho de banda. en el ejemplo a continuación, se limita el número de usuarios simultáneos a 25.

```
MaxClientsNumber            25
```

33.3.1.2. Parámetro MaxClientsPerIP.

establece el número máximo de conexiones desde una misma dirección IP. Considerando que muchos usuarios pudieran acceder desde un servidor intermediario (proxy), lo cual significa que lo harían con una misma dirección IP, el valor predeterminado de 8 puede ser modificado de acuerdo al criterio del administrador. En el ejemplo a continuación, se limita el número de conexiones desde una misma dirección IP a 5.

```
MaxClientsPerIP             5
```

33.3.1.3. Parámetro DisplayDotFiles.

Establece si se permitirá mostrar los ficheros cuyo nombre inicia con un punto (ficheros ocultos) cuando el usuario envíe un mandato de listado con la opción **-a**. En la mayoría de los casos, no es conveniente permitir mostrar los ficheros ocultos.

en el ejemplo a continuación, se define que no se permita mostrar ficheros ocultos.

```
DisplayDotFiles             no
```

33.3.1.4. Parámetro NoAnonymous.

Define si se permitirán o no los accesos anónimos. En la mayoría de los casos, como un servidor **FTP** público, es una función deseada. Si el administrador lo considera pertinente, puede desactivarse cambiando el valor predeterminado **no** por **yes**.

```
NoAnonymous              yes
```

33.3.1.5. Parámetro AnonymousCanCreateDirs.

Define si se permite a los usuarios anónimos crear directorios cuando está permitido que éstos puedan subir ficheros al servidor **FTP**. el valor predeterminado es **no**.

33.3.1.6. Parámetro MaxLoad.

Define que los usuarios anónimos no podrán descargar desde el servidor **FTP** cuando éste tenga una carga igual o superior al valor establecido. El valor predeterminado es **4**.

33.3.1.7. Parámetro AntiWarez.

Define que no sea posible descargar ficheros cuyo propietario sea el usuario **ftp**, como una medida de seguridad que permitirá al administrador supervisar lo que se ha subido al servidor **FTP** antes de permitir su distribución. El valor predeterminado es **no**, y se recomienda dejarlo de ese modo a fin de contar con una buena política de seguridad.

33.3.1.8. Parámetro AnonymousBandwidth.

Define la tasa de Kb por segundo de descarga permitida para los usuarios anónimos. En el siguiente ejemplo, se establece que los usuarios anónimos tendrán una tasa de hasta 12 Kb por segundo para descargar ficheros desde el servidor **FTP**.

```
AnonymousBandwidth            12
```

33.3.1.9. Parámetro UserBandwidth.

Define la tasa de Kb por segundo de descarga permitida para **todos** los usuarios, incluyendo los anónimos. Su utilización junto con el parámetro **AnonymousBandwidth** hace que este último no tenga sentido. Se utiliza o bien **UserBandwidth** o bien **AnonymousBandwidth**. No puede combinarse su uso. En el siguiente ejemplo, se establece que **todos** los usuarios, incluyendo los anónimos, tendrán una tasa de hasta 12 Kb por segundo para descargar ficheros desde el servidor **FTP**.

```
UserBandwidth             12
```

33.3.1.10. Parámetro umask.

Define la máscara predeterminada para los nuevos ficheros y nuevos directorios en el servidor **FTP**. El valor predeterminado es **133:022**. Si se desea que los ficheros subidos por por un usuario solo sean leídos por ese mismo usuario, se puede utilizar **177:077**. Si se desea que los ficheros solo sean leíbles y ejecutables para su propietario, se puede utilizar **077:077**Si se desea que los ficheros subidos sean ejecutables, se puede utilizar **122:022**. Si se desea que los fichero sean leíbles para otros usuarios, pero no puedan ser reescritos por éstos, se pude utilizar **022:022**. El usuario, claro,

puede cambiar desde el cliente **FTP** la máscara utilizada en sus ficheros y directorios a través de **SITE CHMOD**. en el siguiente ejemplo, se establecen los valores predeterminados.

```
umask            133:022
```

33.3.1.11. Parámetro ProhibitDotFilesWrite.

Define si se permitirá sobreescribir ficheros que inicien con punto. Su valor predeterminado es **no**. Si se trata de un servidor **FTP** que permite el acceso hacia el directorio raíz de un sitio virtual de un servidor **HTTP**, es conveniente permitir sobreescribir los ficheros **.htaccess**, **.htpasswd** y otros contenidos, por lo que no conviene activar este parámetro. De ser otro tipo de servidor, puede activarse y añadir seguridad.

33.3.1.12. Parámetro AnonymousCantUpload.

Define si se permitirá a los usuarios anónimos subir contenido hacia el servidor **FTP**. De modo predefinido, este parámetro está activo para impedir lo anterior.

```
AnonymousCantUpload            yes
```

33.3.1.13. Parámetro CreateHomeDir.

Especifica si se debe crear automática el directorio de inicio de un usuarios en caso de no existir éste. En el siguiente ejemplo, se habilita esta función.

```
CreateHomeDir            yes
```

33.3.1.14. Parámetro Quota.

Define la cuota de número máximo de ficheros y espacio utilizado por el usuario. Muy conveniente y útil si se tiene un servidor **FTP** que permite subir contenido para un servidor **HTTP** compartido por varios sitios de red virtuales. en el siguiente ejemplo se establece una cuota máxima de 1500 ficheros y 50 MB de espacio a utilizar para los usuarios.

```
Quota            1500:50
```

33.3.1.15. Parámetro MaxDiskUsage.

Define el espacio máximo permitido en la partición que contiene **/var/ftp** para el servicio **FTP** donde se está permitiendo que los usuarios anónimos suban contenido. El valor predeterminado es **99**. Conviene definir un límite más bajo si el servicio **FTP** no es prioritario en el sistema. en el siguiente ejemplo, se establece un uso máximo del 80% de la partición donde se localiza **/var/ftp**.

```
MaxDiskUsage            80
```

33.3.1.16. Parámetro CustomerProof.

este parámetro fue diseñado para lidiar con los usuarios ignorantes a fin de impedir que realicen operaciones que bloqueen el acceso hacia sus ficheros y/o directorios de forma accidental. es decir, impiden que se realicen operaciones como **chmod 0 public_html**. Si se va a utilizar el servicio como parte de un servicio de hospedaje de sitios de red a través de **HTTP**, conviene que este parámetro esté activo.

```
CustomerProof             yes
```

33.3.2. Agregar el servicio al arranque del sistema.

Para hacer que el servicio de **pure-ftpd** esté activo con el siguiente inicio del sistema, en todos los niveles de corrida (2, 3, 4, y 5) se utiliza lo siguiente

```
chkconfig pure-ftpd on
```

33.3.3. Iniciar, detener y reiniciar servicio.

Para iniciar por primera vez el servicio **pure-ftpd**, utilice:

```
service pure-ftpd start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service pure-ftpd restart
```

Para detener el servicio, utilice:

```
service pure-ftpd stop
```

33.4. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir los puerto 20 y 21 por TCP (**FTP-DATA** y **FTP**, respectivamente).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     20,21
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

34. Cómo configurar OpenSSH

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

34.1. Introducción.

34.1.1. Acerca de SSH.

SSH (**S**ecure **Sh**ell) es un conjunto de estándares y protocolo de red que permite establecer una comunicación a través de un canal seguro entre un cliente local y un servidor remoto. Utiliza una clave pública cifrada para autenticar el servidor remoto y, opcionalmente, permitir al servidor remoto autenticar al usuario. SSH provee confidencialidad e integridad en la transferencia de los datos utilizando criptografía y **MAC** (**M**essage **A**uthentication **C**odes, o Códigos de Autenticación de Mensaje). De modo predeterminado, escucha peticiones a través del puerto 22 por TCP.

34.1.2. Acerca de SFTP.

SFTP (**S**SH **F**ile **T**ransfer **P**rotocol) es un protocolo que provee funcionalidad de transferencia y manipulación de ficheros a través de un flujo confiable de datos. Comúnmente se utiliza con **SSH** para proveer a éste de transferencia segura de ficheros.

34.1.3. Acerca de SCP.

SCP (**S**ecure **C**o**p**y, o Copia Segura) es una protcolo seguro para transferir ficheros entre un anfitrión local y otro remoto, a través de **SSH**. Básicamente, es idéntico a **RCP** (**R**emote **C**o**p**y, o Copia Remota), con la diferencia de que los datos son cifrados durante la transferencia para evitar la extracción potencial de información a través de programas de captura de las tramas de red (**packet sniffers**). **SCP** solo implementa la transferencia de ficheros, pues la autenticación requerida es realizada a través de **SSH**.

34.1.4. Acerca de OpenSSH.

OpenSSH (**Open S**ecure **Sh**ell) es una alternativa de código abierto, con **licencia BSD**, hacia la implementación propietaria y de código cerrado **SSH** creada por Tatu Ylönen. **OpenSSH** es un proyecto creado por el equipo de desarrollo de OpenBSD y actualmente dirigido por Theo de Raadt. Se considera es más segura que su contraparte propietaria debido a la constante auditoría que se realiza sobre el código fuente por parte de una gran comunidad de desarrolladores, una ventaja que brinda al tratarse de un proyecto de fuente abierta.

OpenSSH incluye servicio y clientes para los protocolos **SSH**, **SFTP** y **SCP**.

URL: http://www.openssh.org/.

34.2. Equipamiento lógico necesario.

- openssh-3.5p1-6
- openssh-clients-3.5p1-6
- openssh-server-3.5p1-6

Antes de continuar verifique siempre la existencia de posibles actualizaciones de seguridad:

```
yum -y install openssh openssh-server openssh-clients
```

34.3. Ficheros de configuración.

/etc/ssh/sshd_config	Fichero central de configuración del servicio **SSH**.

34.4. Procedimientos.

Edite **/etc/ssh/sshd_config**. A continuación se analizarán los parámetros a modificar.

34.4.1. Parámetro Port.

Una forma de elevar considerablemente la seguridad al servicio de **SSH**, es cambiar el número de puerto utilizado por el servicio, por otro que solo conozca el administrador del sistema. A este tipo de técnicas se les conoce como **Seguridad por Oscuridad**. La mayoría de los delincuentes informáticos utiliza guiones que buscan servidores que respondan a peticiones a través del puerto 22. Cambiar de puerto el servicio de SSH disminuye considerablemente la posibilidad de una intrusión a través de este servicio.

```
Port 22
```

SSH trabaja a través del puerto 22 por TCP. Puede elegirse cualquier otro puerto entre el 1025 y 65535. ejemplo:

```
Port 52341
```

34.4.2. Parámetro ListenAddress.

Por defecto, el servicio de SSH responderá peticiones a través de todas las interfaces del sistema. En algunos casos es posible que no se desee esto y se prefiera limitar el acceso sólo a través de una interfaz a la que sólo se pueda acceder desde la red local. Para tal fin puede establecerse lo siguiente, considerando que el servidor a configurar posee la IP **192.168.1.254**:

```
ListenAddress 192.168.1.254
```

34.4.3. Parámetro PermitRootLogin.

Establece si se va a permitir el acceso directo del usuario root al servidor SSH. Si se va a permitir el acceso hacia el servidor desde redes públicas, resultará prudente utilizar este parámetro con el valor **no**.

```
PermitRootLogin no
```

34.4.4. Parámetro X11Forwarding.

Establece si se permite o no la ejecución remota de aplicaciones gráficas. Si se va a acceder hacia el servidor desde red local, este parámetro puede quedarse con el valor **yes**. Si se va a permitir el acceso hacia el servidor desde redes públicas, resultará prudente utilizar este parámetro con el valor **no**.

```
X11Forwarding yes
```

34.4.5. Parámetro AllowUsers.

Permite restringir el acceso por usuario y, opcionalmente, anfitrión desde el cual pueden hacerlo. El siguiente ejemplo restringe el acceso hacia el servidor **SSH** para que solo puedan hacerlo los usuarios fulano y mengano, desde cualquier anfitrión.

```
AllowUsers fulano mengano
```

Permite restringir el acceso por usuario y, opcionalmente, anfitrión desde el cual pueden hacerlo. El siguiente ejemplo restringe el acceso hacia el servidor **SSH** para que solo puedan hacerlo los usuarios fulano y mengano, solamente desde los anfitriones 10.1.1.1 y 10.2.2.1.

```
AllowUsers fulano@10.1.1.1 mengano@10.1.1.1 fulano@10.2.2.1 mengano@10.2.2.1
```

34.5. Aplicando los cambios.

El servicio de **SSH** puede iniciar, detenerse o reiniciar a través de un guión similar a los del resto del sistema. De tal modo, podrá iniciar, detenerse o reiniciar a través del mandato **service** y añadirse al arranque del sistema en un nivel o niveles de corrida en particular con el mandato **chkconfig**.

Para ejecutar por primera vez el servicio, utilice:

```
service sshd start
```

Para hacer que los cambios hechos a la configuración surtan efecto, utilice:

```
service sshd restart
```

Para detener el servicio, utilice:

```
service sshd stop
```

De forma predeterminada, el servicio **SSH** está incluido en todos los niveles de corrida con servicio de red. Para desactivar el servicio Sshd de los niveles de corrida 2, 3, 4 y 5, ejecute:

```
chkconfig --level 2345 sshd off
```

34.6. Probando OpenSSH.

34.6.1. Acceso a través de intérprete de mandatos.

Para acceder a través de intérprete de mandatos hacia el servidor, basta con ejecutar desde el sistema cliente el mandato **ssh** definiendo el usuario a utilizar y el servidor al cual conectar:

```
ssh usuario@servidor
```

Para acceder hacia un puerto en particular, se utiliza el parámetro **-p**. En el siguiente ejemplo, utilizando la cuanta del usuario **juan**, se intentará acceder hacia el servidor con dirección IP **192.168.0.99**, el cual tiene un servicio de **SSH** que responde peticiones a través del puerto 52341.

```
ssh -p 52341 juan@192.168.0.99
```

34.6.2. Transferencia de ficheros a través de SFTP.

Para acceder a través de **SFTP** hacia el servidor, basta con ejecutar desde el sistema cliente el mandato **sftp** definiendo el usuario a utilizar y el servidor al cual conectar:

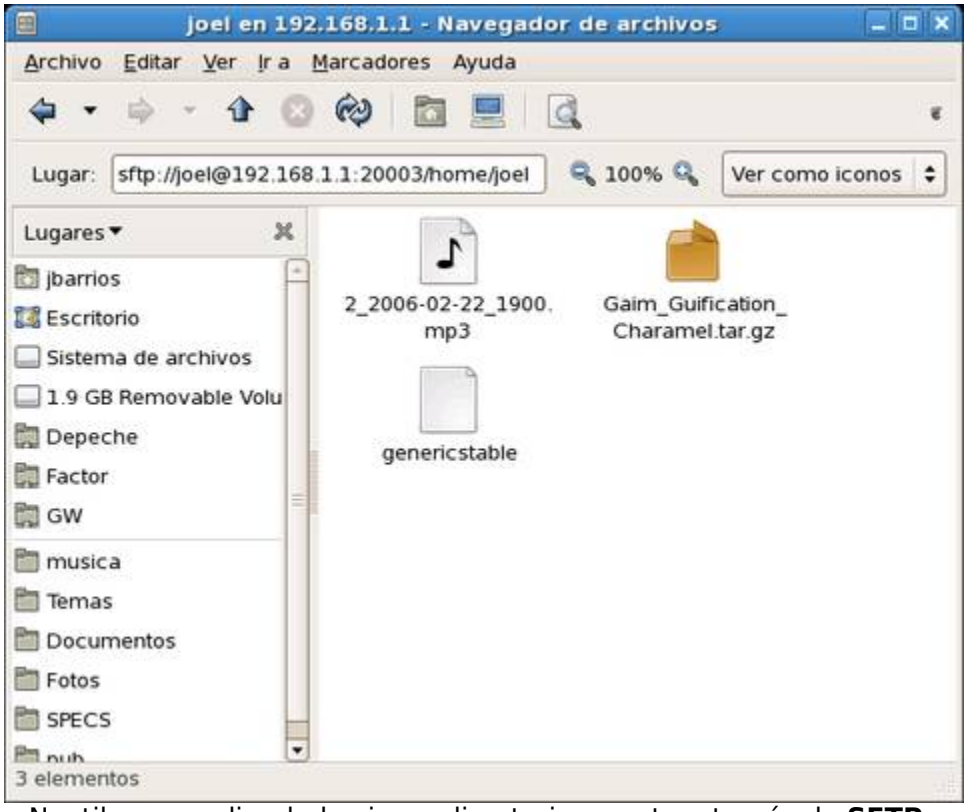
```
sftp usuario@servidor
```

El intérprete de mandatos de **SFTP** es muy similar al utilizado para el protocolo FTP y tiene las mismas funcionalidades.

Para acceder hacia un puerto en particular, en el cual está trabajando el servicio de SSH, se hace través de el parámetro **-o**, con la opción **Port=número de puerto**. En el siguiente ejemplo, utilizando la cuenta del usuario **juan**, se accederá a través de **SFTP** hacia el servidor 192.168.0.99, el cual tiene trabajando el servicio de SSH en el puerto 52341.

```
sftp -o Port=52341 juan@192.168.0.99
```

Si dispone de un escritorio en GNU/Linux, con GNOME 2.x, puede acceder hacia servidores **SSH** a través del protocolo **SFTP** utilizando el administrador de ficheros (**Nautilus**) para realizar transferencias y manipulación de ficheros, especificando el **URI** (**U**niform **R**esource **L**ocator o Localizador Uniforme de Recursos) **«sftp:»**, seguido del servidor y la ruta hacia la que se quiere acceder, seguido del puerto, en el caso que sea distinto al 22.



Nautilus, accediendo hacia un directorio remoto a través de **SFTP**.

34.6.3. Transferencia de ficheros a través de SCP.

Para realizar transferencias de ficheros a través de **SCP**, es necesario conocer las rutas de los directorios objetivo del anfitrión remoto. A continuación se describen algunas de las opciones más importantes del mandato **scp**.

-p	Preserva el tiempo de modificación, tiempos de acceso y los modos del fichero original.
-P	Especifica el puerto para realizar la conexión.
-r	Copia recursivamente los directorios especificados.

En el siguiente ejemplo, se transferirá el fichero **algo.txt**, preservando tiempos y modos, hacia el directorio de inicio del usuario fulano en el servidor 192.169.0.99.

```
scp -p algo.txt fulano@192.168.0.99:~/
```

En el siguiente ejemplo, se transferirá la carpeta **Mail**, junto con todo su contenido, preservando tiempos y modos, **hacia** el directorio de inicio del usuario fulano en el servidor 192.169.0.99.

```
scp -rp Mail fulano@192.168.0.99:~/
```

En el siguiente ejemplo, se transferirá la carpeta **Mail**, junto con todo su contenido, **desde** el directorio de inicio del usuario fulano en el servidor 192.169.0.99, cuyo servicio de **SSH** escucha peticiones a través del puerto 52341, preservando tiempos y modos, hacia el directorio del usuario con el que se está trabajando en el anfitrión local.

```
scp -P 52341 -rp fulano@192.168.0.99:~/Mail ./
```

34.7. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir el puerto 22 por UDP (**SSH**).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     22
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Si la red de área local (LAN) va a acceder hacia el servidor recién configurado, es neceario abrir el puerto correspondiente.

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     22
ACCEPT  loc     fw      tcp     22
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

35. Cómo utilizar OpenSSH con autenticación a través de clave pública.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

35.1. Introducción.

Utilizar claves públicas en lugar de claves de acceso a través de servicios como **SSH**, **SCP** o **SFTP**, resulta una técnica más segura para autenticar dichos servicios, facilitando también la operación de guiones y herramientas de respaldo que utilizan dichos protocolos.

35.2. Procedimientos

35.2.1. Modificaciones en el Servidor.

Conectarse con la cuenta que se utilizará para acceder al servidor. Cómo ese usuario, y realizar las siguientes operaciones para crear el fichero **~/.ssh/authorized_keys** y asignar a éste permiso de acceso 600 (solo lectura y escritura para el usuario):

```
ssh usuario@servidor
mkdir -m 0700 ~/.ssh/
touch ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
```

35.2.2. Modificaciones en el Cliente.

35.2.2.1. Generar clave pública.

Se debe generar una clave pública creada con **DSA** (**D**igital **S**ignature **A**lgorithm o Algoritmo de Firma digital). **Si se desea no utilizar clave de acceso para autenticar, solo se pulsa la tecla ENTER**. Si asigna clave de acceso, está será utilizada para autenticar el certificado creado cada vez que se quiera utilizar éste para autenticar remotamente.

```
ssh-keygen -t dsa
```

El procedimiento devuelve una salida similar a la siguiente:

```
Generating public/private dsa key pair.
Enter file in which to save the key (/home/usuario/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/usuario/.ssh/id_dsa.
```

```
Your public key has been saved in /home/usuario/.ssh/id_dsa.pub.
The key fingerprint is:
2c:73:30:fe:52:21:a5:82:78:49:57:cd:37:af:36:df usuario@cliente
```

Lo anterior genera los ficheros los ficheros **~/.ssh/id_dsa** y **~/.ssh/id_dsa.pub**, los cuales deben tener permiso de acceso 600 (solo lectura y escritura para el usuario).

```
chmod 600 ~/.ssh/
```

Se debe copiar el contenido de la llave pública **DSA** (**id_dsa.pub**) al fichero **~/.ssh/authorized_keys** del usuario a utilizar en servidor en donde se va a autenticar.

```
cat ~/.ssh/id_dsa.pub \
| ssh usuario@servidor \
"cat >> ~/.ssh/authorized_keys"
```

Para poder acceder al servidor desde cualquier cliente, basta copiar los ficheros **id_dsa** y **id_dsa.pub** dentro de **~/.ssh/**, de la cuenta de usuario de cada cliente desde el que se requiera realizar conexión hacia el servidor. Tendrá implicaciones de seguridad muy serias si el fichero **id_dsa** cae en manos equivocadas o se ve comprometido, por tanto, dicho fichero deberá ser considerado como altamente confidencial.

35.2.3. Comprobaciones.

Si no fue asignada clave de acceso para la llave **DSA**, deberá poderse acceder hacia el servidor remoto sin necesidad de autenticar con clave de acceso del usuario remoto. Si fue asignada una clave de acceso a la clave **DSA**, se podrá acceder hacia el servidor remoto autenticando con la clave de acceso definida a la clave **DSA**, y sin necesidad de autenticar con clave de acceso del usuario remoto.

36. Cómo configurar OpenSSH con Chroot

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

36.1. Introducción.

SSH es un protocolo que permite realizar transferencias seguras a través de un túnel seguro donde toda la información trasmitida va cifrada. Sin embargo, **SSH** potencialmente se puede volver un arma de dos filo si una cuenta de usuario se ve comprometida. Configurar un sistema con **OpenSSH** con soporte para **chroot** brinda una mayor seguridad al aislar a los usuarios dentro de un entorno separado del sistema principal con un mínimo de herramientas para trabajar y que disminuye los riesgos potenciales en caso de verse comprometida alguna cuenta.

Chroot es una operación que cambia el directorio raíz, afectando solamente al proceso actual y a los procesos derivados de éste (hijos). Específicamente se refiere a la llamada de sistema chroot(2) o al programa ejecutable chroot(8).

Este documento considera que el lector utiliza **CentOS 4**, **Red Hat™ Enterprise Linux 4** o **White Box Enterprise Linux 4**.

36.2. Equipamiento lógico necesario.

Se requiere instalar los paquetes de **OpenSSH** modificados con el parche disponible a través de http://chrootssh.sourceforge.net/ y que están disponibles a a través de Alcance Libre en el siguiente URL:

```
http://www.alcancelibre.org/al/openssh-chroot/
```

Utilice el mandato **wget**, del siguiente modo, para descargar los paquetes correspondientes:

```
wget -m -np -nH --cut-dirs=1 \
http://www.alcancelibre.org/al/openssh-chroot/
```

El directorio completo será descargado junto los paquetes **RPM** necesarios, junto con algo de contenido **HTML** que pueden eliminarse.

```
rm -f openssh-chroot/index.html*
```

Al terminar, acceda al subdirectorio **openssh-chroot** que se acaba de crear:

```
cd openssh-chroot/
```

Por motivos de seguridad, los paquetes distribuidos por **Alcance Libre** están firmados digitalmente con **GnuPG**. La clave pública está disponible en http://www.alcancelibre.org/al/AL-RPM-KEY. Conviene descargar e importar ésta a fin de verificar la integridad de los paquetes **RPM** involucrados en este documento.

```
wget http://www.alcancelibre.org/al/AL-RPM-KEY
rpm --import AL-RPM-KEY
```

Una vez importada la llave pública, se verifica la integridad de los paquetes **RPM** utilizando el mandato **rpm**, con las opciones -**v** y **-K**, que corresponden, respectivamente, a mensajes descriptivos y verificación de firmas.

```
rpm -Kv *.rpm
```

Lo anterior debe devolver algo similar a lo siguiente:

```
openssh-3.9p1-9.9.el4.al.chroot.i386.rpm:
    CabeceraFirma V3 DSA: OK, key ID 7c080b33
    resumen SHA1 de la cabecera:OK (15c28f0f6dc0dce549fe5441ef4e67054c8dbe07)
    Resumen MD5: OK (41044560482050a87274061848f39910)
    Firma V3 DSA: OK, key ID 7c080b33
openssh-askpass-3.9p1-9.9.el4.al.chroot.i386.rpm:
    CabeceraFirma V3 DSA: OK, key ID 7c080b33
    resumen SHA1 de la cabecera:OK (a3e8ab96f78d49d05cfbf43ad80ad5a5056f717e)
    Resumen MD5: OK (b5f6987c780e9f5802e716de24855f44)
    Firma V3 DSA: OK, key ID 7c080b33
openssh-askpass-gnome-3.9p1-9.9.el4.al.chroot.i386.rpm:
    CabeceraFirma V3 DSA: OK, key ID 7c080b33
    resumen SHA1 de la cabecera:OK (bd5f0e5743a05a33137cbea9cb7abc5a3bed875a)
    Resumen MD5: OK (24a8a19f83e993bbd18e048dde0b77eb)
    Firma V3 DSA: OK, key ID 7c080b33
openssh-clients-3.9p1-9.9.el4.al.chroot.i386.rpm:
    CabeceraFirma V3 DSA: OK, key ID 7c080b33
    resumen SHA1 de la cabecera:OK (679c214e1f0d147523b41b38060ca76d0fd547d7)
    Resumen MD5: OK (92f870b2f74d4410c99f44e96f00681b)
    Firma V3 DSA: OK, key ID 7c080b33
openssh-server-3.9p1-9.9.el4.al.chroot.i386.rpm:
    CabeceraFirma V3 DSA: OK, key ID 7c080b33
    resumen SHA1 de la cabecera:OK (eebb0d88596cd80c6caf7ad0d758a53c5ef653cf)
    Resumen MD5: OK (0f80de58e6d6e2d610593506142981ad)
    Firma V3 DSA: OK, key ID 7c080b33
```

A fin de satisfacer cualquier otra dependencia que pudiera faltar, utilice el mandato **yum** para instalar los paquetes RPM en el interior:

```
yum localinstall *.rpm
```

Si no se dispone del mandato **yum** en el sistema, o bien si así se prefiere, se puede utilizar directamente el mandato **rpm** del siguiente modo:

```
rpm -Uvh openssh-*
```

36.3. Procedimientos

Solo el usuario **root** deberá poder modificar la estructura de la jaula y su contenido. El objeto es poder permitir el acceso por **SSH/SFTP** a un entorno aislado del sistema principal. Adicionalmente si se configura el servicio de **FTP** con jaulas, se podrá acceder indistintamente por **FTP**, **SSH** o **SFTP**.

36.3.1. Componentes mínimos para la jaula.

Los siguientes son los componentes mínimos de la jaula basada sobre un sistema con **CentOS 4**, **Red Hat™ Enterprise Linux 4** o White Box Enterprise Linux 4:

```
/bin/sh
/bin/cp
/bin/false
/bin/ls
/bin/mv
/bin/pwd
/bin/rm
/bin/rmdir
/bin/sh
/bin/true
/etc/group
/etc/passwd
/lib/ld-linux.so.2
/lib/libacl.so.1
/lib/libattr.so.1
/lib/libc.so.6
/lib/libcom_err.so.2
/lib/libcrypt.so.1
/lib/libcrypto.so.4
/lib/libdl.so.2
/lib/libnsl.so.1
/lib/libpthread.so.0
/lib/libresolv.so.2
/lib/librt.so.1
/lib/libselinux.so.1
/lib/libtermcap.so.2
/lib/libutil.so.1
/usr/lib/libz.so.1
/usr/lib/libgssapi_krb5.so.2
/usr/lib/libk5crypto.so.3
/usr/lib/libkrb5.so.3
/usr/libexec/openssh/sftp-server
/sbin/nologin
```

Si se requiere utilizar **/bin/sh**, y suponiendo se utiliza **/chroot/** como directorio raíz para la jaula, se debe copiar dentro de éste como **/chroot/bin/sh**, si se requiere **/lib/libtermcap.so.2** se debe copiar como **/chroot/lib/libtermcap.so.2**, si se requiere **/usr/libexec/openssh/sftp-server** se debe copiar como **/chroot/usr/libexec/openssh/sftp-server**, y así sucesivamente.

Cualquier otra herramienta que se quiera agregar, solo requerirá estén presentes, dentro de las **rutas relativas** de la jaula, las bibliotecas correspondientes. Éstas se determinan a través del mandato **ldd** aplicado sobre la herramienta que se quiere utilizar. Por ejemplo, si se quiere añadir el binario del mandato **more** a la jaula, primero se determina que bibliotecas requiere para funcionar:

```
ldd /bin/more
```

Lo anterior devuelve algo como lo siguiente:

```
        libtermcap.so.2 => /lib/libtermcap.so.2 (0x00bea000)
        libc.so.6 => /lib/tls/i586/libc.so.6 (0x00515000)
        /lib/ld-linux.so.2 (0x004fe000)
```

Lo anterior significa que para poder utilizar el binario del mandato **more** dentro de la jaula deberán estar presentes dentro de ésta y en el subdirectorio **lib/** las bibliotecas libtermcap.so.2, libc.so.6 y ld-linux.so.2.

36.3.2. Ficheros /etc/passwd y /etc/group.

Los ficheros **/etc/group** y **/etc/passwd** solo necesitan contener la información de los usuarios que interese enjaular así como la **ruta relativa** al directorio donde se encuentra la jaula de sus directorios de inicio (es decir, se define **/home/usuario**, suponiendo que realmente se localiza en **/var/www/sitiocliente/home/usuario**). **Es indispensable esté presente esta información dentro de la jaula** o de otro modo no será posible realizar el ingreso al sistema.

36.3.2.1. Ejemplo del contenido de /etc/passwd dentro de la jaula

```
usuario:x:503:503::/home/usuario:/bin/bash
```

36.3.2.2. Ejemplo del contenido de /etc/group dentro de la jaula

```
usuario:x:503:
```

36.3.3. Dispositivos de bloque.

Aunque no del todo indispensable para utilizar OpenSSH con Chroot, es buena idea crear los siguiente nodos dentro de la jaula:

```
mkdir dev
mknod -m 0666 dev/tty c 5 0
mknod -m 0644 dev/urandom c 1 9
mknod -m 0666 dev/null c 1 3
mknod -m 0666 dev/zero c 1 12
```

36.4. Ejemplo práctico.

Suponiendo que se tiene un cliente, y éste ha solicitado servicio de hospedaje para su sitio de red a través de HTTP. El cliente quiere dos usuarios diferentes para subir distinto contenido al sitio de red. Los usuarios serán fulano y mengano. El dominio a administrar sera sitio.com, que será administrado exclusivamente por fulano, y se quiere un sub-dominio denominado ventas.sitio.com que será administrado por mengano.

36.4.1. Crear las cuentas de los usuarios

Se crea el directorio **/var/www/sitio.com** y se copia la estructura de la jaula antes mencionada dentro de subdirectorios relativos a **/var/www/sitio.com**, teniendo cuidado de dejar a root como

propietario a fin de impedir que los usuarios puedan borrar algún subdirectorio del interior.

Se crean las cuentas de los dos usuarios, tomando en cuenta que si se asigna **/sbin/nologin** o **/bin/false** como interprete de mandatos, se podrá acceder por FTP pero no se podrá acceder por **SSH** o **SFTP**, y si se asigna **/usr/libexec/openssh/sftp-server**, solo se podrá acceder por **SFTP**. Si se asigna **/bin/sh** como interprete de mandatos, se podrá acceder por **SSH**, **SFTP** y **FTP**.

```
useradd -s /bin/sh -d /var/www/sitio.com/./ fulano
mkdir /var/www/sitio.com
chown root.apache /var/www/sitio.com
passwd fulano

useradd -s /bin/sh -m -d /var/www/sitio.com/./ventas mengano
mkdir /var/www/sitio.com/ventas
chown root.apache /var/www/sitio.com/ventas
passwd mengano
```

Cabe señalar que los directorios de inicio pertenecen a root, de este modo se impide que el usuario pueda borrar subdirectorio relativos que se utilizarán para guardar las bitácoras de Apache.

Suponiendo que el ususario *fulano* tiene **UID 513** y que el usuario *mengano* tiene **UID 514**, el fichero **/var/www/sitio.com/etc/passwd** debería tener el siguiente contenido:

```
fulano:x:513:513::/var/www/sitio.com/./home/fulano:/bin/sh
mengano:x:514:514::/var/www/sitio.com/./home/mengano:/bin/sh
```

Basado sobre lo anterior, e fichero **/var/www/sitio.com/etc/group** debería tener el siguiente contenido:

```
apache:x:48:
fulano:x:513:
mengano:x:514:
```

36.4.2. Ejemplo aplicado a sitio de red virtual con Apache.

El dominio **www.sitio.com** se configurará del siguiente modo:

```
        <VirtualHost *:80>
                ServerName www.sitio.com
                ServerAlias sitio.com
                DocumentRoot /var/www/sitio.com/html
                ErrorLog /var/www/sitio.com/logs/error_log
                CustomLog /var/www/sitio.com/logs/access_log combined
                <Directory "/var/www/sitio.com/html/">
                        Options Indexes Indexes Includes
                        AllowOverride all
                </Directory>
        </VirtualHost>
```

Los directorios necesarios se crearán del siguiente modo con siguientes permisos:

```
mkdir /var/www/sitio.com
```

```
chown root.apache /var/www/sitio.com
mkdir -p /var/www/sitio.com/html
chown fulano.apache /var/www/sitio.com/html
mkdir -p /var/www/sitio.com/configs
chown fulano.apache /var/www/sitio.com/configs
```

El subdominio **ventas.sitio.com** se configurará del siguiente modo:

```
        <VirtualHost *:80>
                ServerName ventas.sitio.com
                DocumentRoot /var/www/sitio.com/ventas/html
                ErrorLog /var/www/sitio.com/ventas/logs/error_log
                CustomLog /var/www/sitio.com/ventas/logs/access_log combined
                <Directory "/var/www/sitio.com/ventas/html/">
                        Options Indexes Indexes Includes
                        AllowOverride all
                </Directory>
        </VirtualHost>
```

Los directorios necesarios se crearán del siguiente modo, asignando estos con el mandato **chown** al usuario **root**, **fulano** y el grupo **apache**:

```
mkdir /var/www/sitio.com/ventas
chown root.apache /var/www/sitio.com/ventas
mkdir -p /var/www/sitio.com/ventas/html
chown fulano.apache /var/www/sitio.com/ventas/html
mkdir -p /var/www/sitio.com/ventas/configs
chown fulano.apache /var/www/sitio.com/ventas/configs
```

36.4.2.1. Comprobaciones del ejemplo.

Al acceder con el usuario **fulano** a través de **SSH** o **FTP** hacia *www.sitio.com* se deberá acceder hacia **/var/www/sitio.com**, el cual será presentado como **"/"**. El usuario publicará el contenido **HTML** dentro del subdirectorio **/html**, , podrá guardar contenido fuera del directorio raíz público, del sitio virtual en Apache, en el subdirectorio **/configs** y podrá acceder hacia las bitácoras generadas por apache en **/logs**, para ser utilizadas por cualquier herramienta de análisis, como **Webalizer**. Es importante mencionar que el usuario **fulano** no podrá borrar contenido, ni deberá tener capacidad tal, del directorio **/**, como son el subdirectorio de bitácoras **/logs** y el subdirectorio **/html**. Éste último se mostrará a través de Apache como *http://ventas.sitio.com/*. En la ausencia de estos, tras una eliminación accidental de los mismos, Apache no podría iniciar, lo cual afectaría a todos los sitios hospedados en el servidor.

Al acceder con el usuario **mengano** a través de **SSH** o **FTP** hacia *www.sitio.com* se deberá acceder hacia **/var/www/sitio.com**, el cual será presentado como **"/"**. El usuario publicará el contenido **HTML** dentro del subdirectorio **/ventas/html**, podrá guardar contenido fuera del directorio raíz público, del sitio virtual en Apache, en el subdirectorio **/ventas/configs** y podrá acceder hacia las bitácoras generadas por Apache, en el subdirectorio **/ventas/logs**, para ser utilizadas por cualquier herramienta de análisis, como **Webalizer**. Es importante mencionar que el usuario **mengano** no podrá borrar contenido, ni deberá tener capacidad tal, del directorio **/ventas**, como serían el subdirectorio de bitácoras (**/ventas/logs**) y el subdirectorio de contenido **HTML** (**/ventas/html**). Éste último se mostrará a través de Apache como *http://ventas.sitio.com/*. En la ausencia de estos, tras una eliminación accidental de los mismos, Apache no podría iniciar, lo cual afectaría a todos los sitios hospedados en el servidor.

37. Cómo configurar NTP.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

37.1. Introducción.

37.1.1. Acerca de NTP.

NTP (**N**etwork **T**ime **P**rotocol) es un protocolo, de entre los más antiguos protocolos de Internet (1985), utilizado para la sincronización de relojes de sistemas computacionales a través de redes, haciendo uso de intercambio de paquetes (unidades de información transportadas entre nodos a través de enlaces de datos compartidos) y latencia variable (tiempo de demora entre el momento en que algo inicia y el momento en que su efecto inicia). **NTP** fue originalmente diseñado, y sigue siendo mantenido, por Dave Mills, de la universidad de Delaware.

NTP Utiliza el algoritmo de Marzullo (inventado por Keith Marzullo), el cual es un utilizado para seleccionar fuentes para la estimación exacta del tiempo a partir de un número de fuentes, utilizando la escala **UTC**.

La versión 4 del protocolo puede mantener el tiempo con un margen de 10 milisegundos a través de la red mundial, alcanzado exactitud de 200 microsegundos. En redes locales, bajo condiciones idóneas, este margen se reduce considerablemente.

El servicio trabaja a través del puerto 123, únicamente por **UDP**.

URL: http://www.ietf.org/rfc/rfc1305.txt

37.1.1.1. Estratos.

NTP utiliza el sistema jerárquico de estratos de reloj.

Estrato 0: son dispositivos, como relojes **GPS** o radio relojes, que no están conectados hacia redes sino computadoras.

Estrato 1: Los sistemas se sincronizan con dispositivos del estrato 0. Los sistemas de este estrato son referidos como servidores de tiempo.

Estrato 2: Los sistemas envían sus peticiones NTP hacia servidores del estrato 1, utilizando el algoritmo de Marzullo para recabar la mejores muestra de datos, descartando que parezcan proveer datos erróneos, y compartiendo datos con sistemas del mismo estrato 2. Los sistemas de este estrato actúan como servidores para el estrato 3.

Estrato 3: Los sistemas utilizan funciones similares a las del estrato 2, sirviendo como servidores para el estrato 4.

Estrato 4: Los sistemas utilizan funciones similares a las del estrato 3.

Lista de servidores públicos, de estrato 1 y 2, en http://kopernix.com/?q=ntp y http://www.eecis.udel.edu/~mills/ntp/servers.html

37.1.2. Acerca de UTC.

UTC (**C**oordinated **U**niversal **T**ime, o Tiempo Universal Coordinado) es un estándar de alta precisión de tiempo atómico. Tiene segundos uniformes definidos por **TAI** (**T**iempo **A**tómico **I**nternacional, o International Atomic Time), con segundos intercalares o adicionales que se anuncian a intervalos irregulares para compensar la desaceleración de la rotación de la Tierra, así como otras discrepancias. Estos segundos adicionales permiten a **UTC** estar casi a la par del Tiempo Universal (**UT**, o **U**niversal **T**ime), el cual es otro estándar pero basado sobre el ángulo de rotación de la Tierra, en lugar de el paso uniforme de los segundos.

URL: http://es.wikipedia.org/wiki/UTC

37.2. Equipamiento lógico necesario.

37.2.1. Instalación a través de yum.

Si utiliza **CentOS 4** o **White Box Enterprise Linux 4**, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum –y install ntp
```

37.2.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date –i ntp
```

37.3. Procedimientos.

37.3.1. Herramienta ntpdate

Una forma muy sencilla de sincronizar el reloj del sistema con cualquier servidor de tiempo es a través de **ntpdate**. Es una herramienta similar a **rdate**, y se utiliza para establecer la fecha y hora del sistema utilizando **NTP**. El siguiente ejemplo realiza una consulta directa **NTP**, utilizando un puerto sin privilegios (opción **-u**, muy útil si hay un cortafuegos que impida la salida) hacia el servidor *2.pool.ntp.org*.

```
ntpdate -u 2.pool.ntp.org
```

37.3.2. Fichero de configuración /etc/ntp.conf.

Los sistemas operativos como Red Hat™ Enterprise Linux 4 y CentOS 4, se incluye un fichero de configuración **/etc/ntp.conf**, con fines demostrativo. La recomendación es respaldarlo para futura consulta, y comenzar con un fichero con una configuración nuevo, mismo que a continuación se describe.

```
# Se establece la política predeterminada para cualquier
# servidor de tiempo utilizado: se permite la sincronización
# de tiempo con las fuentes, pero sin permitir a la fuente
# consultar (noquery), ni modificar el servicio en el
# sistema (nomodify) y declinando proveer mensajes de
# registro (notrap).
restrict default nomodify notrap noquery

# Permitir todo el acceso a la interfaz de retorno del
# sistema.
restrict 127.0.0.1

# Se le permite a la red local sincronizar con el servidor
# pero sin permitirles modificar la configuración del
# sistema, y sin usar a éstos como iguales para sincronizar.
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

# Reloj local indisciplinado.
# Este es un controlador emulado que se utiliza solo como
# respaldo cuando ninguna de las fuentes reales están
# disponibles.
fudge   127.127.1.0 stratum 10
server  127.127.1.0

# Fichero de variaciones.
driftfile /var/lib/ntp/drift
broadcastdelay  0.008

# Fichero de claves si acaso fuesen necesarias para realizar
# consultas
keys            /etc/ntp/keys

# Lista de servidores de tiempo de estrato 1 o 2.
# Se recomienda tener al menos 3 servidores listados.
# Mas servidores en:
#               http://kopernix.com/?q=ntp
#               http://www.eecis.udel.edu/~mills/ntp/servers.html
server 0.pool.ntp.org
server 1.pool.ntp.org
server 2.pool.ntp.org

# Permisos que se asignarán para cada servidor de tiempo.
# En los ejemplos, no se permite a las fuente consultar, ni
# modificar el servicio en el sistema ni enviar mensaje de
# registro.
restrict 0.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery
restrict 1.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery
restrict 2.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery

# Se Activ la difusión hacia los clientes
broadcastclient
```

37.3.3. Iniciar, detener y reiniciar el servicio ntpd.

Para ejecutar por primera vez el servicio **ntpd**, utilice:

```
service ntpd start
```

Para hacer que los cambios hechos, tras modificar la configuración, surtan efecto, utilice:

```
service ntpd restart
```

Para detener el servicio **ntpd**, utilice:

```
service ntpd stop
```

37.3.4. Agregar el servicio ntpd al arranque del sistema.

Para hacer que el servicio de **ntpd** esté activo con el siguiente inicio del sistema, en todos los niveles de corrida (2, 3, 4, y 5), se utiliza lo siguiente:

```
chkconfig ntpd on
```

37.4. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir el puerto 123 por UDP (**NTP**, tanto para tráfico entrante como saliente.

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      udp     123
ACCEPT  fw      net     udp     123
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Si la red de área local (LAN) va a acceder hacia el servidor recién configurado, es necesario abrir el puerto correspondiente.

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      udp     123
ACCEPT  fw      net     udp     123
ACCEPT  loc     fw      udp     123
ACCEPT  fw      loc     udp     123
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

38. Cómo configurar el sistema para sesiones gráficas remotas

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

38.1. Introducción

Cuando se tienen distintas máquinas en una LAN y se desea aprovechar el poder y recursos de una de éstas y ahorrar trabajo, una sesión gráfica remota será de gran utilidad. Lograr esto es muy fácil. Se puede hacer de dos formas, una accediendo vía SSH, RHS o Telnet, y la otra utilizando alguna de las pantallas de acceso gráfico, como GDM.

38.2. Sesión gráfica remota con GDM

GDM tiene una característica poco usada, pero muy útil. El método será de mucha utilidad suponiendo que se tiene un servidor central con buena cantidad de memoria y un buen microprocesador y lo más nuevo en sustento lógico; y en la red de área local (LAN) se tienen una o varias máquinas con muy poco espacio en disco y/o poco poder en el microprocesador, o resulta mucho trabajo instalarles todo un sistema optimizado y personalizado.

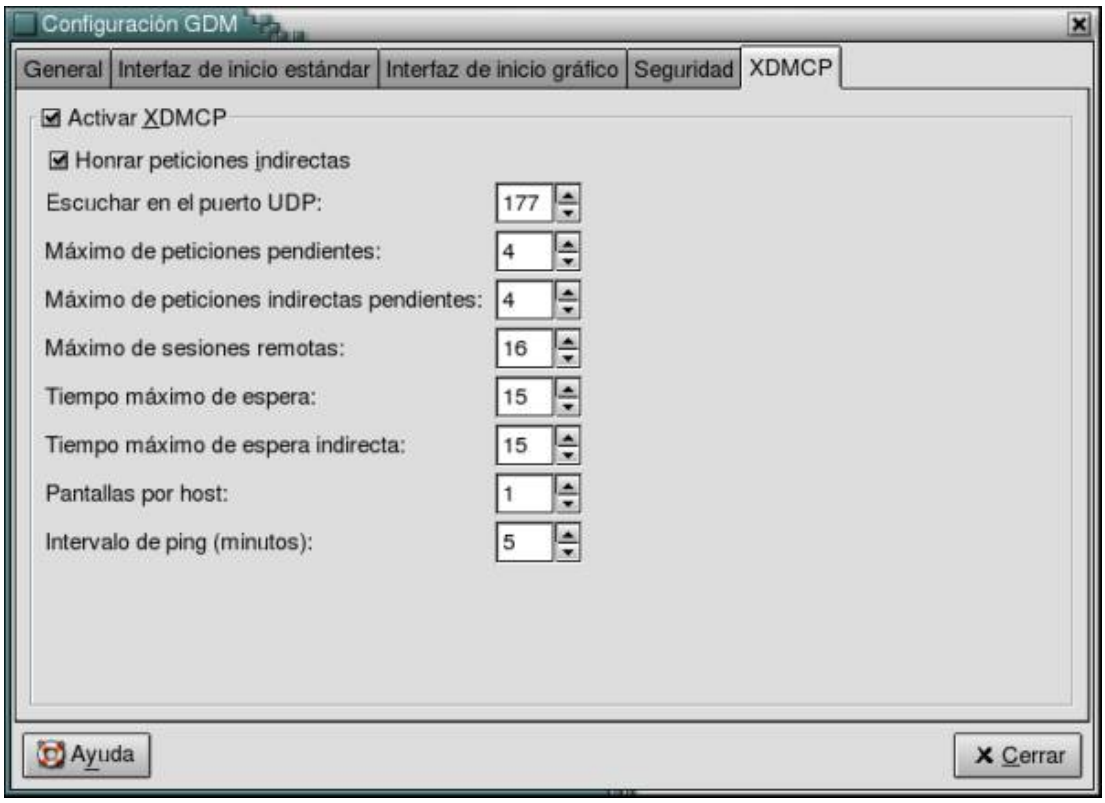
El objetivo será entonces que los usuarios puedan utilizar el servidor con mayor poder y recursos para que se ejecuten ahí las sesiones gráficas y así tener un mayor control en toda la red.

38.2.1. Procedimiento

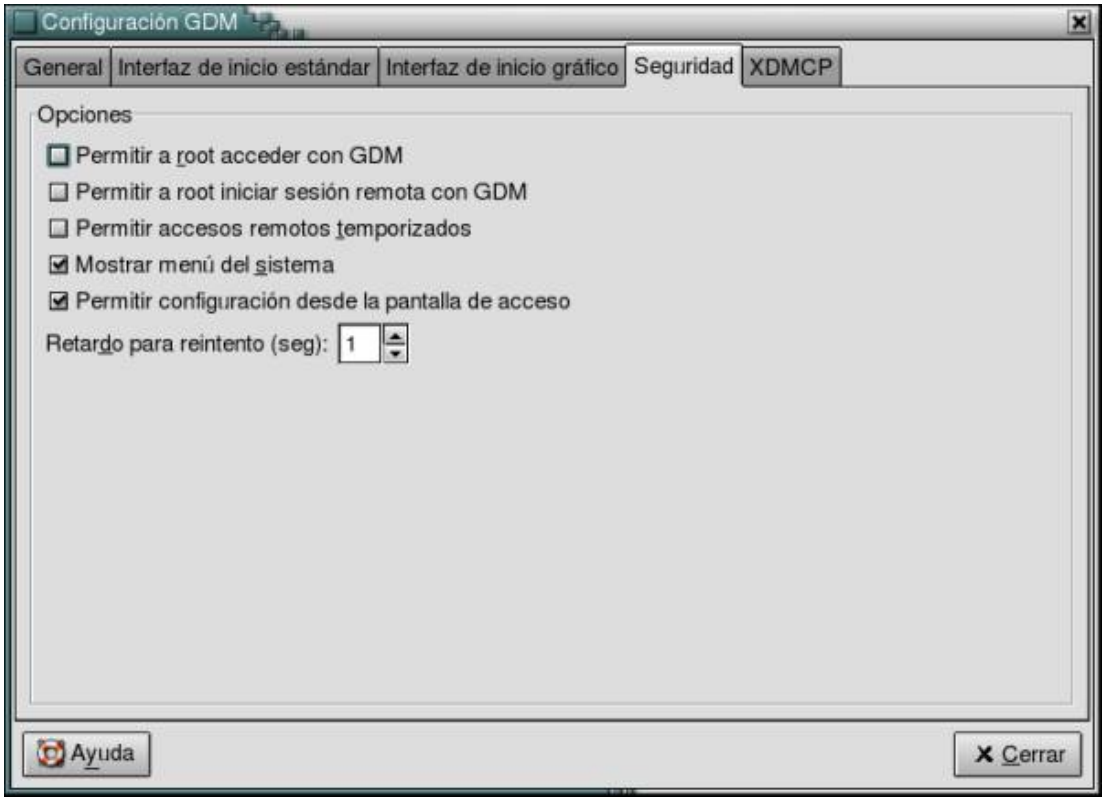
1. Actualice gdm al menos a la versión 2.2.x o, de ser posible, más reciente:

   ```
   yum -y install gdm
   ```

2. En el servidor, abra una terminal como súperusuario y ejecute el mandato *gdmsetup*; vaya a la solapa de *XDMCP* y de allí a la pestaña XDMCP. Deben habilitarse las casillas de "*Activar XDMCP*" y "*Honrar peticiones indirectas*" como se muestra a continuación:



3. Como medida de seguridad, deshabilite el acceso de *root* tanto local como remotamente.



4. Debe determinarse la localización de X con el mandato which:

   ```
   which X
   ```

5. En los clientes, debe respaldarse y editarse el archivo /etc/X11/prefdm y debe hacerse que contenga únicamente lo siguiente, considerando que se debe poner la ruta completa de X:

   ```
   #!/bin/sh
   /usr/X11R6/bin/X -query dirección_IP_del_Servidor
   ```

   Ejemplo:

   ```
   #!/bin/sh
   /usr/X11R6/bin/X -query 192.168.1.254
   ```

6. En todas las máquinas, ya sea si se utiliza webmin o linuxconf o alguna otra herramienta, debe hacer que el modo de ejecución sea gráfico y con red, es decir que arranque en modo de ejecución 5 (o nivel de corrida 5).

   Puede modificar /etc/inittab y cambiar:

   *id:**3**:initdefault:*

   Por:

   *id:**5**:initdefault:*

7. Deben reiniciarse los servidores X de las máquinas clientes.

8. Las máquinas clientes verán a GDM ejecutándose como si se estuviese en el mismo servidor, y permitirá iniciar GNOME o KDE o cualquier otro entorno gráfico utilizado. Si cuenta con buenos adaptadores de red, ni siquiera se notará si se está en un cliente o en el servidor.

Si lo prefiere también puede iniciar el servidor de vídeo remoto simplemente ejecutando lo siguiente desde cualquier terminal:

```
X -query dirección_IP_del_Servidor
```

39. Cómo configurar un servidor NFS

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

39.1. Introducción

NFS, acrónimo de ***N****etwork* ***F****ile* ***S****ystem*, es un popular protocolo utilizado para compartir volúmenes entre máquinas dentro de una red de manera transparente, más comúnmente utilizado entre sistemas basados sobre UNIX®. Es útil y fácil de utilizar, sin embargo no en vano es apodado *cariñosamente* como "*No File Security*". NFS no utiliza un sistema de contraseñas como el que tiene SAMBA, sólo una lista de control de acceso determinada por direcciones IP o nombres. Es por esto que es importante que el administrador de la red local o usuario entienda que un servidor NFS puede ser un verdadero e inmenso agujero de seguridad si éste no es configurado apropiadamente e implementado detrás de un corta-fuegos o firewall.

Personalmente, recomiendo utilizar NFS dentro de una red local detrás de un corta-fuegos o firewall que permita el acceso sólo a las máquinas que integren la red local, nunca para compartir sistemas de archivos a través de Internet. Al no contar con un sistema de autenticación por contraseñas, es un servicio susceptible del ataque de algún delincuente infomático. SAMBA es un protocolo mucho mejor y más seguro para compartir sistemas de archivos.

39.2. Procedimientos

Teniendo en cuenta los aspectos de seguridad mencionados, es importante que siga los procedimientos descritos a continuación al pie de la letra, y que posteriormente se comprometa también consultar a detalle la documentación incluida en el paquete nfs-utils, ya que ésta le proporcionará información adicional y completa sobre aspectos avanzados de configuración y utilización.

39.2.1. Instalación del sustento lógico necesario

```
yum -y install nfs-utils portmap
```

39.3. Configurando la seguridad

Lo siguiente será configurar un nivel de seguridad para *portmap*. Esto se consigue modificando los ficheros */etc/hosts.allow* y */etc/hosts.deny*. Debemos especificar qué direcciones IP o rango de direcciones IP pueden acceder a los servicios de portmap y quiénes no pueden hacerlo. Podemos entonces determinar en /etc/hosts.allow como rango de direcciones IP permitidas los siguiente:

```
portmap:192.168.1.0/255.255.255.0
```

Esto corresponde a la dirección IP de la red completa y la máscara de la subred. Adicionalmente

podemos especificar direcciones IP individuales sin necesidad de establecer una máscara. Esto es de utilidad cuando se desea compartir volúmenes con otras máquinas en otras redes a través de Internet. Ejemplo:

```
portmap:192.168.1.0/255.255.255.0
portmap:192.168.20.25
portmap:192.168.30.2
portmap:216.200.152.96
portmap:148.240.28.171
```

Una vez que se han determinado las direcciones IP que pueden acceder a portmap, sólo resta determinar quiénes no pueden hacerlo. Evidentemente nos referimos al resto del mundo, y esto se hace agregando la siguiente línea:

```
portmap:ALL
```

Es importante destacar que la línea anterior es **INDISPENSABLE** y **NECESARIA** si quiere tener un nivel de seguridad decente. De manera predeterminada las versiones más recientes de nfs-utils no permitirán iniciar el servicio si esta línea no se encuentra presente en /etc/hosts.deny.

Una vez configurado portmap, debe reiniciarse el servicio de portmap:

```
service portmap restart
```

Si tiene un DNS, añada los registros de las direcciones IP asociadas a un nombre o bien modifique /etc/hosts y agregue las direcciones IP asociadas con un nombre. Esto nos servirá como listas de control de accesos. Ejemplo del fichero **/etc/hosts**:

```
127.0.0.1       localhost.localdomain   localhost
192.168.1.254   servidor.mi-red-local.org servidor
192.168.1.2     algun_nombre.mi-red-local.org    algun_nombre
192.168.1.3     otro_nombre.mi-red-local.org     otro_nombre
192.168.1.4     otro_nombre_mas.mi-red-local.org otro_nombre_mas
192.168.1.5     como_se_llame.mi-red-local.org    como_se_llame
192.168.1.6     como_sea.mi-red-local.org como_sea
192.168.1.7     lo_que_sea.mi-red-local.org       lo_que_sea
```

39.3.1. Compartir un volumen NFS

Procederemos a determinar qué directorio se va a compartir. Puede crear también uno nuevo:

```
mkdir -p /var/nfs/publico
```

Una vez hecho esto, necesitaremos establecer qué directorios en el sistema serán compartidos **con el resto de las máquinas de la red, o bien a qué máquinas, de acuerdo al DNS o /etc/hosts** se permitirá el acceso. Éstos deberemos agregarlos en /**etc/exports** determinado con qué máquinas y el modo en que se compartirá el recurso. Se puede especificar una dirección IP o bien nombrar alguna máquina, o bien un patrón común con comodín para definir qué máquinas pueden acceder. Podemos utilizar el siguiente ejemplo (la separación de espacios se hace con un tabulador):

```
/var/nfs/publico        *.mi-red-local.org(ro,sync)
```

En el ejemplo anterior se está definiendo que se compartirá /var/nfs/publico/ a todas las máquinas cuyo nombre, de acuerdo al DNS o /etc/hosts, tiene como patrón común **mi-red-local.org**, en modo de lectura escritura. Se utilizó un asterisco (*) como comodín, seguido de un punto y el nombre del dominio. Esto permitirá que *como_se_llame.mi-red-local.org*, *como_sea.mi-red-local.org*, *lo_que_sea.mi-red-local.org*, etc., podrán acceder al volumen /var/nfs/publico/ en modo de sólo lectura. Si queremos que el accesos a este directorio sea en modo de lectura y escritura, cambiamos (ro) por (rw):

```
/var/nfs/publico        *.mi-red-local.org(rw,sync)
```

Ya que se definieron los volúmenes a compartir, sólo resta iniciar o reiniciar el servicio nfs. Utilice cualquiera de las dos líneas dependiendo del caso:

```
service nfs start
service nfs restart
```

A fin de asegurar de que el servicio de *nfs* esté habilitado, la próxima vez que se encienda el equipo, de deberá ejecutar lo siguiente:

```
chkconfig --level 345 nfs on
```

El mandato anterior hace que se habilite *nfs* en los niveles de corrida 3, 4 y 5.

Como medida de seguridad adicional, si tiene un corta-fuegos o *firewall* implementado. Cierre, para todo aquello que no sea parte de su red local, los puertos tcp y udp 2049, ya que éstos son utilizados por NFS para escuchar peticiones.

39.3.2. Configurando las máquinas clientes

Para probar la configuración, es necesario que las máquinas clientes se encuentren definidas en el DNS o en el fichero */etc/hosts* del servidor. Si no hay un DNS configurado en la red, deberán definirse los nombres y direcciones IP correspondientes en el fichero /etc/hosts de todas las máquinas que integran la red local.

Como root, en el equipo cliente, ejecute el siguiente mandato para consultar los volúmenes exportados (-e) a través de NFS por un servidor en particular:

```
showmount -e 192.168.1.254
```

Lo anterior mostrará una lista con los nombres y rutas exactas a utilizar. Ejemplo:

```
Export list for 192.168.1.254:
/var/nfs/publico          192.168.1.0/24
```

A continuación creamos, como *root*, desde cualquier otra máquina de la red local un punto de montaje:

```
mkdir /mnt/servidornfs
```

Por último, para proceder a montar el volumen remoto, utilizaremos la siguiente línea de mandato :

```
mount servidor.mi-red-local.org:/var/nfs/publico /mnt/servidornfs
```

Si por alguna razón en el DNS de la red local, o el fichero **/etc/hosts** de la máquina cliente, decidió no asociar el nombre de la máquina que fungirá como servidor NFS a su correspondiente dirección IP, puede especificar ésta en lugar del nombre. Ejemplo:

```
mount -t nfs 192.168.1.254:/var/nfs/publico /mnt/servidornfs
```

Podremos acceder entonces a dicho volumen remoto cambiando al directorio local definido como punto de montaje, del mismo modo que se haría con un disquete o una unidad de CDROM:

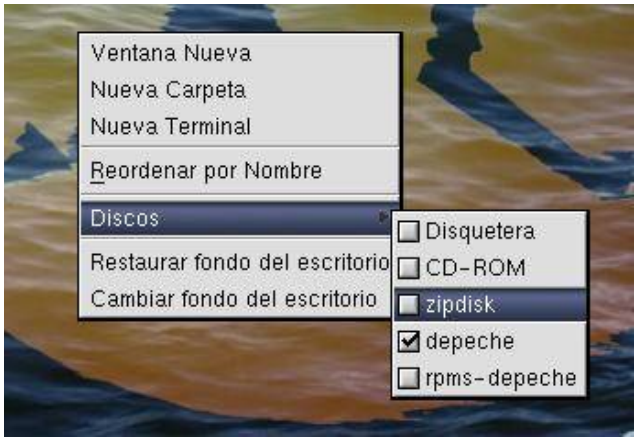
```
cd /mnt/servidornfs
```

Si queremos montar este volumen NFS con una simple línea de mandato o bien haciendo doble clic en un icono sobre el escritorio, será necesario agregar la correspondiente línea en /etc/fstab. Ejemplo:

```
servidor.mi-red-local.org:/var/nfs/publico              /mnt/servidornfs              nfs
user,exec,dev,nosuid,rw,noauto 0 0
```

La línea anterior especifica que el directorio /var/nfs/publico/ de la máquina servidor.mi-red-local.org será montado en el directorio local /mnt/servidor/nfs, permitiéndole a los usuarios poder montarlo, en modo de lectura y escritura y que este volumen no será montado durante el arranque del sistema. Esto último es de importancia, siendo que si el servidor no está encendido al momento de arrancar la máquina cliente, éste se colgará durante algunos minutos.

Una vez agregada la línea en /etc/fstab de la máquina cliente, si utiliza GNOME-1.4 o superior, éste incorpora Nautilus como administrador de archivos, mismo que auto-detecta cualquier cambio en /etc/fstab. Debe hacerse clic derecho sobre el escritorio y posteriormente seleccionar el disco que se desee montar.



39.4. Instalación de GNU/Linux a través de un servidor NFS

Este es quizás el uso más común para un volumen NFS. Permite compartir un volumen que contenga una copia del CD de instalación de alguna distribución y realizar inclusive instalaciones simultáneas en varios equipos. Tiene como ventaja que la instalación puede resultar más rápida que si se hiciese con un CDROM, siendo que la tasa de trasferencia de archivos será determinada por el ancho de banda de la red local, y nos permitirá instalar GNU/Linux en máquinas que no

tengan unidad de CDROM.

Una vez creado y configurado un volumen a compartir copiaremos todo el contenido del CD de instalación en éste:

```
cp -r /mnt/cdrom/* /var/nfs/publico/
```

En el directorio *images* del CD encontraremos varias imágenes para crear disquetes de arranque. Utilizaremos bootnet.img para crear el número de disquetes necesarios para cada máquina en la que realizaremos una instalación y que nos permitirán acceder a la red. Inserte un disquete y ejecute lo siguiente:

```
cd /var/nfs/publico/images/
dd if=bootnet.img of=/dev/fd0 bs=1440k
```

Añada en /etc/hosts, o bien de de alta en el DNS, las direcciones IP, que serán utilizadas por las nuevas máquinas, asociadas a un nombre con el dominio que específico como regla de control de acceso en /etc/exports -*es decir *.mi-red-local.org*-. Para /etc/hosts, puede quedar como sigue:

```
127.0.0.1       localhost.localdomain   localhost
192.168.1.254   servidor.mi-red-local.org servidor
192.168.1.2     algun_nombre.mi-red-local.org    algun_nombre
192.168.1.3     otro_nombre.mi-red-local.org     otro_nombre
192.168.1.4     otro_nombre_mas.mi-red-local.org otro_nombre_mas
192.168.1.5     como_se_llame.mi-red-local.org    como_se_llame
192.168.1.6     como_sea.mi-red-local.org como_sea
192.168.1.7     lo_que_sea.mi-red-local.org       lo_que_sea
192.168.1.8     nueva_maquina.mi-red-local.org       nueva_maquina
192.168.1.9     otra_nueva_maquina.mi-red-local.org
otra_nueva_maquina
```

Utilice estos disquetes para arrancar en los equipos, ingrese una dirección IP y demás parámetros para esta máquina y cuando se le pregunte ingrese la dirección IP del servidor NFS y el directorio en éste en el que se encuentra la copia del CD de instalación. El resto continuará como cualquier otra instalación.

40. Cómo configurar SAMBA

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

40.1. Introducción

40.1.1. Acerca del protocolo SMB

SMB (acrónimo de **S**erver **M**essage **B**lock) es un protocolo, del **Nivel de Presentación** del modelo OSI de TCP/IP, creado en 1985 por IBM. Algunas veces es referido también como **CIFS** (Acrónimo de **C**ommon **I**nternet **F**ile **S**ystem, http://samba.org/cifs/) tras ser renombrado por Microsoft en 1998. Entre otras cosas, Microsoft añadió al protocolo soporte para enlaces simbólicos y duros así como también soporte para ficheros de gran tamaño. *Coincidentalmente* esto ocurrió por la misma época en que Sun Microsystems realizó el lanzamiento de WebNFS (una versión extendida de **NFS**, http://www.sun.com/software/webnfs/overview.xml).

SMB fue originalmente diseñado para trabajar a través del protoclo NetBIOS, el cual a su vez trabaja sobre **NetBEUI** (acrónimo de **N**etBIOS **E**xtended **U**ser **I**nterface, que se traduce como Interfaz de Usuario Extendida de NetBIOS), **IPX/SPX** (acrónimo de **I**nternet **P**acket E**x**change/**S**equenced **P**acket E**x**change, que se traduce como **Intercambio de paquetes interred/Intercambio de paquetes secuenciales**) o **NBT**, aunque también puede trabajar directamente sobre **TCP/IP**

40.1.2. Acerca de Samba

SAMBA es un conjunto de programas, originalmente creados por Andrew Tridgell y actualmente mantenidos por The SAMBA Team, bajo la Licencia Publica General GNU, y que se implementan en sistemas basados sobre UNIX® el protocolo **SMB**. Sirve como reemplazo total para Windows® NT, Warp®, NFS® o servidores Netware®.

40.2. Equipamiento lógico necesario

Los procedimientos descritos en este manual han sido probados para poder aplicarse en sistemas con Red Hat™ Enterprise Linux 4, o equivalentes, o en versiones posteriores, y al menos Samba 3.0.10 o versiones posteriores.

Necesitará tener instalados los siguientes paquetes, que **seguramente vienen incluidos** en los discos de instalación de su distribución predilecta:

- samba: Servidor SMB.
- samba-client: Diversos clientes para el protoclo SMB.
- samba-common: Ficheros necesarios para cliente y servidor.

Consulte a la base de datos RPM del sistema si se encuentran instalados estos paquetes, utilizando el siguiente mandato:

```
rpm -q samba samba-client samba-common
```

Si se utiliza Red Hat™ Enterprise Linux, bastará realizar lo siguiente para instalar o actualizar el sustento lógico necesario:

```
up2date -i samba samba-client
```

Si utiliza CentOS 4 o White Box Enterprise Linux 4, bastará realizar lo siguiente para instalar o actualizar el sustento lógico necesario:

```
yum -y install samba samba-client
```

40.3. Configuración básica de Samba

Para la mayoría de los casos la configuración de Samba como servidor de archivos es suficiente.

40.3.1. Alta de cuentas de usuario

Es importante sincronizar las cuentas entre el servidor Samba y las estaciones Windows®. Es decir, si en una máquina con Windows® ingresamos como el usuario "*paco*" con clave de acceso "*elpatito16*", en el servidor Samba deberá existir también dicha cuenta con ese mismo nombre y la misma clave de acceso. Como la mayoría de las cuentas de usuario que se utilizarán para acceder hacia samba no requieren acceso al intérprete de mandatos del sistema, no es necesario asignar clave de acceso con el mandato **passwd** y se deberá definir **/sbin/nologin** o bien **/bin/false** como intérprete de mandatos para la cuenta de usuario involucrada.

```
useradd -s /sbin/nologin usuario-windows
smbpasswd -a usuario-windows
```

No hace falta asignar una clave de acceso en el sistema con el mandato **passwd** puesto que la cuenta no tendrá acceso al intérprete de mandatos.

Si se necesita que las cuentas se puedan utilizar para acceder hacia otros servicios como serían Telnet, SSH, etc, es decir, que se permita acceso al intérprete de mandatos, será necesario especificar **/bin/bash** como intérprete de mandatos y al mismo tiempo se deberá asignar una clave de acceso en el sistema con el mandato **passwd**:

```
useradd -s /bin/bash usuario-windows
passwd usuario-windows
smbpasswd -a usuario-windows
```

40.3.2. El fichero lmhosts

Es necesario dar inicio resolviendo localmente los nombres NetBIOS asociándolos con direcciones IP correspondientes. Para fines prácticos el nombre *NetBIOS* debe tener un máximo de 11 caracteres. Normalmente tomaremos como referencia el nombre corto del servidor o el nombre corto que se asignó como alias a la interfaz de red. Éste lo estableceremos en el fichero **/etc/samba/lmhosts**, en donde encontraremos lo siguiente:

```
127.0.0.1       localhost
```

Debemos añadir entonces el nombre que hayamos elegido asociado a la dirección IP que se tenga dentro de la red local. **Opcionalmente** se podrá añadir también los nombres y dirección IP del resto de las máquinas que conformen la red local. La separación de espacios se hace con un tabulador. Ejemplo:

```
127.0.0.1       localhost
192.168.1.5     maquinalinux
192.168.1.6     isaac
192.168.1.7     finanzas
192.168.1.8     direccion
```

40.3.3. Parámetros principales del fichero smb.conf

Modifique el fichero **/etc/samba/smb.conf** con cualquier editor de texto. Dentro de éste notará que la información que le será de utilidad viene comentada con un símbolo **#** y los ejemplos con **;** (punto y coma), siendo estos últimos los que tomaremos como referencia.

Empezaremos por establecer el grupo de trabajo editando el valor del parámetro **workgroup** asignando un grupo de trabajo deseado:

```
workgroup = MIGRUPO
```

Opcionalmente puede establecer con el parámetro **netbios name** otro nombre distinto para el servidor si fuese necesario, pero siempre tomando en cuenta que dicho nombre deberá corresponder con el establecido en el fichero **/etc/samba/lmhosts**:

```
netbios name = maquinalinux
```

El parámetro **server string** es de carácter descriptivo. Puede utilizarse un comentario breve que dé una descripción del servidor.

```
server string = Servidor Samba %v en %L
```

40.3.4. Parámetros útiles para la seguridad

La seguridad es importante y ésta se puede establecer primeramente estableciendo la lista de control de acceso que definirá qué máquinas o redes podrán acceder hacia el servidor. El parámetro **hosts allow** sirve para determinar esto. Si la red consiste en la máquinas con dirección IP desde 192.168.1.1 hasta 192.168.1.254, el rango de direcciones IP que se definirá en hosts allow será **192.168.1.** de modo tal que sólo se permitirá el acceso dichas máquinas. Note por favor el punto al final de cada rango. Modifique ésta de manera que quede del siguiente modo:

```
hosts allow = 192.168.1. 127.
```

El parámetro **interfaces** permite establecer desde qué interfaces de red del sistema se escucharán peticiones. Samba no responderá a peticiones provenientes desde cualquier interfaz no especificada. Esto es útil cuando Samba se ejecuta en un servidor que sirve también de puerta de enlace para la red local, impidiendo que se establezcan conexiones desde fuera de la red local.

```
interfaces = 192.168.1.254/24
```

40.3.5. Impresoras en Samba

Las impresoras se comparten de modo predeterminado, así que sólo hay que realizar algunos ajustes. Si se desea que sea posible acceder hacia la impresora como usuario invitado sin clave de acceso, basta con añadir **public = Yes** en la sección de impresoras del siguiente modo:

```
[printers]
        comment = El comentario que guste.
        path = /var/spool/samba
        printable = Yes
        browseable = No
        writable = no
        printable = yes
        public = Yes
```

Windows NT, 2000 y XP no tendrán problema alguno para acceder e imprimir hacia las impresoras; sin embargo Windows 95, 98 y ME suelen tener problemas para comunicarse con Samba para poder imprimir. Por tanto, si se quiere evitar problemas de conectividad con dichos sistemas operativos hay que agregar algunos parámetros que resolverán cualquier eventualidad:

```
[printers]
        comment = Impresoras.
        path = /var/spool/samba
        printable = Yes
        browseable = No
        writable = no
        printable = yes
        public = Yes
        print command = lpr -P %p -o raw %s -r
        lpq command = lpstat -o %p
        lprm command = cancel %p-%j
```

Se pude definir también a un usuario o bien un grupo (**@grupo_que_sea**) para la administración de las «colas» en las impresoras:

```
[printers]
        comment = Impresoras.
        path = /var/spool/samba
        printable = Yes
        browseable = No
        writable = no
        printable = yes
        public = Yes
        print command = lpr -P %p -o raw %s -r
        lpq command = lpstat -o %p
        lprm command = cancel %p-%j
        printer admin = fulano, @opers_impresion
```

Con lo anterior se define que el usuario **fulano** y quien pertenezca al grupo **opers_impresion** podrán realizar tareas de administración en las impresoras.

40.3.6. Compartiendo directorios a través de Samba

Para los directorios o volúmenes que se irán a compartir, en el mismo fichero de configuración encontrará distintos ejemplos para distintas situaciones particulares. En general, puede utilizar el siguiente ejemplo que funcionará para la mayoría:

```
[Lo_que_sea]
        comment = Comentario que se le ocurra
        path = /cualquier/ruta/que/desee/compartir
```

El volumen puede utilizar cualquiera de las siguientes opciones:

Opción	Descripción
`guest ok`	Define si se permitirá el acceso como usuario invitado. El valor puede ser `Yes` o `No`.
`public`	Es un **equivalente** del parámetro **guest ok**, es decir, define si se permitirá el acceso como usuario invitado. El valor puede ser `Yes` o `No`.
`browseable`	Define si se permitirá mostrar este recurso en las listas de recursos compartidos. El valor puede ser `Yes` o `No`.
`writable`	Define si ser permitirá la escritura. Es el parámetro contrario de `read only`. El valor puede ser `Yes` o `No`. Ejemplos: «`writable = Yes`» **es lo mismo que** «`read only = No`». Obviamente «`writable = No`» **es lo mismo que** «`read only = Yes`»
`valid users`	Define que usuarios o grupos pueden acceder al recurso compartido. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: `fulano, mengano, @administradores`
`write list`	Define qué usuarios o grupos pueden acceder con permiso de escritura. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: `fulano, mengano, @administradores`
`admin users`	Define qué usuarios o grupos pueden acceder con permisos administrativos para el recurso. Es decir, podrán acceder hacia el recurso realizando todas las operaciones como súperusuarios. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: `fulano, mengano, @administradores`
`directory mask`	Es lo mismo que `directory mode`. Define qué permiso en el sistema tendrán los subdirectorios creados dentro del recurso. Ejemplo: `1777`
`create mask`	Define qué permiso en el sistema tendrán los nuevos ficheros creados dentro del recurso. Ejemplo: `0644`

En el siguiente ejemplo se compartirá a través de Samba el recurso denominado **ftp**, el cual está localizado en el directorio **/var/ftp/pub** del disco duro. Se permitirá el acceso a cualquiera pero será

un recurso de sólo lectura salvo para los usuarios administrador y fulano. Todo directorio nuevo que sea creado, en su interior tendrá permiso 755 y todo fichero que sea puesto en su interior tendrá permiso 644.

```
[ftp]
        comment = Directorio del servidor FTP
        path = /var/ftp/pub
        guest ok = Yes
        read only = Yes
        write list = fulano, administrador
        directory mask = 0755
        create mask = 0644
```

40.4. Configuración avanzada de Samba

Samba fue creado con un objetivo: ser en un reemplazo definitivo para Windows como servidor en una red local. Esto, por supuesto, requiere algunos procedimientos adicionales dependiendo de las necesidades de la red local.

40.4.1. Reasignación de grupos de Windows en Samba

Los grupos que existen en Windows también se utilizan en Samba para ciertas operaciones, principalmente relacionadas con lo que involucra un Controlador Primario de dominio (o **PDC** que significa **P**rimary **D**omain **C**ontroler). Estos grupos existen de modo predefinido en Samba. Sin embargo, si se ejecuta lo siguiente:

```
net groupmap list
```

Devolverá la siguiente información:

```
System Operators (S-1-5-32-549) -> -1
Domain Admins (S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-512) -> -1
Replicators (S-1-5-32-552) -> -1
Guests (S-1-5-32-546) -> -1
Domain Guests (S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-514) -> -1
Power Users (S-1-5-32-547) -> -1
Print Operators (S-1-5-32-550) -> -1
Administrators (S-1-5-32-544) -> -1
Account Operators (S-1-5-32-548) -> -1
Domain Users (S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-513) -> -1
Backup Operators (S-1-5-32-551) -> -1
Users (S-1-5-32-545) -> -1
```

Lo anterior corresponde al mapa de los grupos que, de modo predeterminado, utilizará Samba si éste fuese configurado como Controlador Primario de Dominio. **XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX** corresponde a un número generado aleatoriamente al iniciarse Samba por primera vez. **Tome nota de dicho número, ya que lo requerirá más adelante** para reasignar los nombres al español en el mapa de grupos.

Los grupos anteriormente descritos **trabajarán perfecta y limpiamente** asociándolos contra grupos en el sistema, pero **sólamente si utiliza alguna versión de Windows en inglés**. Si utiliza alguna versión de Windows en español, **habrá que reasignar los nombres de los grupos a los correspondientes al español** y asociarles a grupos en el sistema, esto a fin de permitir asignar usuarios a dichos grupos y de este modo delegar tareas de administración del mismo modo que en Windows.

Es por tal motivo que si se tiene la intención de configurar Samba como Controlador Primario de Dominio y al mismo tiempo poder hacer uso de los grupos del mismo modo que en Windows, es decir, por mencionar un ejemplo, permitir a ciertos usuarios pertenecer al grupo de administradores del dominio con privilegios de administrador, lo primero será entonces generar los grupos en el sistema ejecutando como root los siguientes mandatos:

```
groupadd -r administradores
groupadd -r admins_dominio
groupadd -r duplicadores
groupadd -r invitados
groupadd -r invs_dominio
groupadd -r opers_copias
groupadd -r opers_cuentas
groupadd -r opers_impresion
groupadd -r opers_sistema
groupadd -r usrs_avanzados
groupadd -r usuarios
groupadd -r usuarios_dominio
```

Una vez creados los grupos en el sistema, sólo resta reasignar los nombres al español en el mapa de grupo de Samba y asociarles a éstos los grupos recién creados en el sistema. El procedimiento se resume a ejecutar algo como lo siguiente:

```
net groupmap modify \
ntgroup="Nombre grupo Windows en español" \
sid="número-de-identidad-en-sistema" \
unixgroup="grupo_en_linux" \
comment="comentario descriptivo acerca del grupo"
```

Lo anterior establece que se modifique el registro del grupo que corresponda al **sid** (identidad de sistema) definido con el nombre establecido con **ntgroup**, asociándolo al grupo en el servidor con **unixgroup** y añadiendo un comentario descriptivo acerca de dicho grupo con **comment**.

De modo tal, y a fin de facilitar las cosas a quien haga uso de este manual, puede utilizar el siguiente guión para convertir los nombres al español y asociarlos a grupos en Linux, donde solamente deberá definir el número de identidad del sistema que corresponda al servidor:

```
#!/bin/sh
SIDSAMBA=XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX

net groupmap modify ntgroup="Administradores" \
sid="S-1-5-32-544" unixgroup=administradores \
comment="Los administradores tienen acceso completo y sin restricciones al equipo o
dominio"

net groupmap modify ntgroup="Admins. del dominio" \
sid="S-1-5-21-$SIDSAMBA-512" unixgroup=admins_dominio \
comment="Administradores designados del dominio"

net groupmap modify ntgroup="Duplicadores" \
sid="S-1-5-32-552" unixgroup=duplicadores \
comment="Pueden duplicar archivos en un dominio"

net groupmap modify ntgroup="Invitados del dominio" \
sid="S-1-5-21-$SIDSAMBA-514" unixgroup=invitados \
comment="Todos los invitados del dominio"

net groupmap modify ntgroup="Invitados" \
sid="S-1-5-32-546" unixgroup=invitados \
comment="Los invitados tienen de modopredeterminado el mismo acceso que los miembros del
grupo Usuarios, excepto la cuenta Invitado que tiene mas restricciones"

net groupmap modify ntgroup="Operadores de copias" \
sid="S-1-5-32-551" unixgroup=opers_copias \
```

```
comment="Los operadores de copia pueden sobrescribir restricciones de seguridad con el
unico proposito de hacer copias de seguridad o restaurar archivos"

net groupmap modify ntgroup="Opers. de cuentas" \
sid="S-1-5-32-548" unixgroup=opers_cuentas \
comment="Pueden administrar cuentas de usuarios y grupos del dominio"

net groupmap modify ntgroup="Opers. de impresión" \
sid="S-1-5-32-550" unixgroup=opers_impresion \
comment="Pueden operar impresoras del dominio"

net groupmap modify ntgroup="Opers. de servidores" \
sid="S-1-5-32-549" unixgroup=opers_sistema \
comment="Pueden administrar sistemas del dominio"

net groupmap modify ntgroup="Usuarios avanzados" \
sid="S-1-5-32-547" unixgroup=usrs_avanzados \
comment="Los usuarios avanzados tienen mas derechos administrativos con algunas
restricciones. De este modo, pueden ejecutar aplicaciones heredadas junto con
aplicaciones certificadas"

net groupmap modify ntgroup="Usuarios del dominio" \
sid="S-1-5-21-$SIDSAMBA-513" unixgroup=usuarios_dominio \
comment="Todos los usuarios del dominio"

net groupmap modify ntgroup="Usuarios" \
sid="S-1-5-32-545" unixgroup=usuarios \
comment="Los usuarios no pueden hacer cambios accidentales o intencionados en el sistema.
Pueden ejecutar aplic. certificadas, pero no la mayoría de las heredadas"

exit 0
```

Nota: Este guión se encuentra incluido en el disco de “Extras de curso” de Alcance Libre. Solo basta editarlo y definir la variable SIDSAMBA y ejecutarlo como root.

Una vez hecho lo anterior, al volver a realizar lo siguiente:

```
net groupmap list
```

Se deberá de mostrar ahora esto otro:

```
Opers. de servidores (S-1-5-32-549) -> opers_sistema
Admins. del dominio (S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-512) -> admins_dominio
Duplicadores (S-1-5-32-552) -> duplicadores
Invitados (S-1-5-32-546) -> invitados
Invitados del dominio (S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-514) -> invitados
Usuarios avanzados (S-1-5-32-547) -> usrs_avanzados
Opers. de impresión (S-1-5-32-550) -> opers_impresion
Administradores (S-1-5-32-544) -> administradores
Opers. de cuentas (S-1-5-32-548) -> opers_cuentas
Usuarios del dominio (S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-513) -> usuarios_dominio
Operadores de copias (S-1-5-32-551) -> opers_copias
Usuarios (S-1-5-32-545) -> usuarios
```

De este modo, si por ejemplo, se agrega al usuario fulano al grupo **admins_dominio**, se tendrá el mismo efecto que si se hiciera lo mismo en Windows agregando al usuario al grupo **Admins. del dominio**. Esto por supuesto solamente tendrá utilidad si Samba se configura y utiliza como Controlador Primario de Dominio.

40.4.2. Alta de cuentas de usuario en Controlador Primario de Dominio

Si se configuró Samba para funcionar como Controlador Primario de Dominio, será necesario asignar a root una clave de acceso en Samba, la cual por supuesto puede ser diferente a la del sistema,

debido a que las estaciones de trabajo necesitan autenticar primero con el usuario root de Samba para poder unirse dominio y poder crear de este modo una cuenta de máquina en el sistema a través del parámetro **add machine script** ya descrito anteriormente.

Es necesario dar de alta a los usuarios de modo que queden agregados a los que correspondan en el sistema a grupos **Usuarios** y **Usuarios del dominio** de Windows, es decir a los grupos **usuarios** y **usuarios_dominio**.

```
useradd -s /sbin/nologin -G usuarios,usuarios_dominio usuario-windows
smbpasswd -a usuario-windows
```

Si el usuario ya existiese, será necesario agregarlo a los grupos **usuarios** y **usuarios_dominio** con **gpassswd** del siguiente modo:

```
gpasswd -a usuario-windows usuarios
gpasswd -a usuario-windows usuarios_dominio
```

En teoría en el directorio definido para el recurso **Profiles** se deben crear automáticamente los directorios de los usuarios donde se almacenarán los perfiles. De ser necesario es posible generar éstos directorios utilizando el siguiente guión:

```
cd /home
for user in *
do
mkdir -p /var/lib/samba/profiles/$user
chown $user.$user /var/lib/samba/profiles/$user
done
```

40.4.3. Parámetros de configuración avanzada en el fichero smb.conf

40.4.3.1. Anunciando el servidor Samba en los grupos de trabajo

La opción **remote announce** se encarga de que el servicio nmbd se anuncie a si mismo de forma periódica hacia una red en particular y un grupo de trabajo específico. Esto es particularmente útil si se necesita que el servidor Samba aparezca no solamente en el grupo de trabajo al que pertenece sino también en otros grupos de trabajo. El grupo de trabajo de destino puede estar en cualquier lugar en tanto exista una ruta y sea posible la transmisión exitosa de paquetes.

```
remote announce = 192.168.1.255/MI-DOMINIO 192.168.2.255/OTRO-DOMINIO
```

El ejemplo anterior definió que el servidor Samba se anuncie a si mismo al los grupos de trabajo MI-DOMINIO y OTRO-DOMINIO en las redes cuyas IP de transmisión son 192.168.1.255 y 192.168.2.255 correspondientemente.

40.4.3.2. Ocultando y denegando acceso a ficheros

No es conveniente que los usuarios accedan o bien puedan ver la presencia de ficheros ocultos en el sistema, es decir ficheros cuyo nombre comienza con un punto, particularmente si acceden a su directorio personal en el servidor Samba (.bashrc, .bash_profile, .bash_history, etc.). Puede utilizarse el parámetro **hide dot files** para mantenerlos ocultos.

```
hide dot files = Yes
```

En algunos casos puede ser necesario denegar el acceso a cierto tipo de ficheros del sistema. El parámetro **veto files** se utiliza para especificar la lista, separada por diagonales, de aquellas cadenas de texto que denegarán el acceso a los ficheros cuyos nombres contengan estas cadenas. En el siguiente ejemplo, se denegará el acceso hacia los ficheros cuyos nombres incluyan la palabra *«Security»* y los que tengan extensión o terminen en *«.tmp»*:

```
veto files = /*Security*/*.tmp/
```

40.4.3.3. Opciones para cliente o servidor Wins

Puede habilitar convertirse en servidor WINS o bien utilizar un servidor WINS ya existente. Se puede ser un servidor WINS o un cliente WINS, pero **no** ambas cosas a al vez.

Si se va ser el servidor WINS, debe habilitarse lo siguiente:

```
wins support = Yes
```

Si se va a utilizar un servidor WINS ya existente, debe descomentar la siguiente línea y especificar qué dirección IP utiliza dicho servidor WINS:

```
wins server = 192.168.1.1
```

40.4.3.4. Opciones específicas para Controlador Primario de Dominio (PDC)

Si se va a configurar Samba como Controlador Primario de Dominio, se debe especificar todos los parámetros descritos a continuación.

Si se quiere que las claves de acceso del sistema y Windows se mantengan sincronizadas, es necesario descomentar las siguiente líenas:

```
unix password sync = Yes
passwd program = /usr/bin/passwd %u
passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password* %n\n
*passwd:*all*authentication*tokens*updated*successfully*
```

El parámetro **local master** define al servidor como examinador del dominio (o master browser); El parámetro **domain master** define al servidor maestro del dominio; El parámetro **preferred master** define al servidor como maestro del domino preferido, en caso de haber más servidores presentes en el mismo dominio como controladores de dominio. El parámetro **time server** se utiliza para definir que las estaciones deberán sincronizar la hora con el servidor al unirse al dominio; El parámetro **domain logons** define que el servidor permitirá a las estaciones autenticar contra Samba.

```
local master = Yes
domain master = Yes
preferred master = Yes
time server = Yes
domain logons = Yes
```

La configuración de Controlador Primario de Dominio requiere además definir dónde se almacenarán los perfiles de los usuarios. Windows 95, 98 y ME que solicitan se defina con el parámetro **logon home**, en tanto que Windows NT, 2000 y XP requieren se haga con el parámetro **logon path.** Para efectos prácticos y de previsión, utilice ambos parámetros y defina la unidad H para dicho volumen:

```
logon path = \\%L\Profiles\%U
logon home = \\%L\%U\.profile
logon drive = H:
```

Si se va a utilizar Samba como Controlador Primario de Dominio, es necesario establecer el guión que ejecutarán las estaciones Windows al conectarse hacia el servidor. Esto se hace a través del parámetro **logon script** el cual puede definir o bien un guión a utilizar por cada usuario (%u.bat) o bien por cada máquina (%m.bat) o bien de modo general para todos (logon.cmd). Para no complicar las cosas, defina inicialmente un guión general para todos del siguiente modo:

```
logon script = logon.cmd
```

El fichero **/var/lib/samba/netlogon/logon.cmd** deberá contener algo como lo siguiente:

```
REM windows client logon script
REM

net time \\mi-servidor /SET /YES
net use H: \\mi-servidor\homes /PERSISTENT:NO
```

El Controlador Primario de Dominio va a necesitar también se definan los guiones a ejecutar para distintas tareas como alta de máquinas, usuarios y grupos así como la baja de éstos.

```
add user script = /usr/sbin/useradd %u
add machine script = /usr/sbin/useradd -d /dev/null -g 100 -s /bin/false -c "Cuenta de
máquina" -M %u
delete user script = /usr/sbin/userdel %u
delete group script = /usr/sbin/groupdel %g
add user to group script = /usr/bin/gpasswd -a %u %g
set primary group script = /usr/sbin/usermod -g %g %u
```

El parámetro **add user script** sirve para definir lo que se deberá ejecutar en el trasfondo del sistema para crear una nueva cuenta de usuario. El parámetro **add machine script** es particularmente importante porque es el mandato utilizado para **dar de alta cuentas de máquinas** (trust accounts o cuentas de confianza) **de modo automático**. El parámetro **delete user script** es para definir lo propio para eliminar usuarios, **delete group script** para eliminar grupos, **add user to group** para añadir usuarios a grupos y set **primary group script** para establecer un grupo como el principal para un usuario.

Directorio para Netlogon y perfiles en Controlador Primario de Dominio (PDC)

Si se va a utilizar Samba como Controlador Primario de Dominio, es necesario definir los recursos donde residirá netlogon y también dónde se almacenarán los perfiles de los usuarios:

```
[netlogon]
comment = Network Logon Service
path = /var/lib/samba/netlogon
write list = @administradores, @admins_dominio
guest ok = Yes
browseable = Yes

[Profiles]
path = /var/lib/samba/profiles
read only = No
guest ok = Yes
create mask = 0600
directory mask = 0700
```

Genere con el mandato mkdir los directorios **/var/lib/samba/profiles** y **/var/lib/samba/netlogon**. El directorio **/var/lib/samba/profiles** deberá pertenecer a root y al grupo **users** y tener permiso 1777 a fin de permitir crear el directorio de perfil correspondiente para cada usuario.

```
mkdir -p -m 1777 /var/lib/samba/profiles
mkdir -p /var/lib/samba/netlogon
chgrp users /var/lib/samba/profiles
```

40.5. Iniciar el servicio y añadirlo al arranque del sistema

Si iniciara Samba por primera vez realice lo siguiente:

```
/sbin/service smb start
```

Si va a reiniciar el servicio, realice lo siguiente:

```
/sbin/service smb restart
```

Para que Samba inicie automáticamente cada vez que inicie el servidor sólo ejecute el siguiente mandato:

```
/sbin/chkconfig smb on
```

40.6. Accediendo hacia Samba

40.6.1. Modo texto

40.6.1.1. Smbclient

Indudablemente el método más práctico y seguro es el mandato *smbclient*. Éste permite acceder hacía cualquier servidor Samba o Windows® como si fuese el mandato ftp en modo texto.

Para acceder al cualquier recurso de alguna máquina Windows® o servidor SAMBA determine primero qué volúmenes o recursos compartidos posee ésta. Utilice el mandato *smbclient* del siguiente modo:

```
smbclient -U usuario -L alguna_maquina
```

Lo cual le devolvería más menos lo siguiente:

```
Domain=[MI-DOMINIO] OS=[Unix] Server=[Samba 3.0.7-1.3E]

          Sharename       Type      Comment
          ---------       ----      -------
          homes           Disk      Home Directories
          netlogon        Disk      Network Logon Service
          ftp             Disk      ftp
          IPC$            IPC       IPC Service (Servidor Samba 3.0.7-1.3E en mi-servidor)
          ADMIN$          IPC       IPC Service (Servidor Samba 3.0.7-1.3E en mi-servidor)
          epl5900         Printer   Created by redhat-config-printer 0.6.x
          hp2550bw        Printer   Created by redhat-config-printer 0.6.x
```

```
Anonymous login successful
Domain=[MI-DOMINIO] OS=[Unix] Server=[Samba 3.0.7-1.3E]

          Server               Comment
          ---------            -------
          mi-servidor          Servidor Samba 3.0.7-1.3E en mi-servidor

          Workgroup            Master
          ---------            -------
          MI-DOMINIO           MI-SERVIDOR
```

Lo siguiente corresponde a la sintaxis básica para poder navegar los recursos compartidos por la máquina Windows® o el servidor SAMBA:

```
smbclient //alguna_maquina/recurso -U usuario
```

Ejemplo:

```
smbclient //LINUX/FTP -U jbarrios
```

Después de ejecutar lo anterior, el sistema solicitará se proporcione la clave de acceso del usuario *jbarrios* en el equipo denominado *LINUX*.

```
smbclient //LINUX/FTP -U jbarrios
added interface ip=192.168.1.254 bcast=192.168.1.255 nmask=255.255.255.0
Password:
Domain=[miusuario] OS=[Unix] Server=[Samba 2.2.1a]
smb: \>
```

Pueden utilizarse virtualmente los mismos mandatos que en el intérprete de *ftp*, como serían get, mget, put, del, etc.

40.6.1.2. Por montaje de unidades de red

Si necesita poder visualizar desde GNU/Linux a las máquinas con Windows® e interactuar con los directorios compartidos por éstas, necesitará realizar algunos pasos adicionales. De manera predeterminada, y por motivos de seguridad, solo *root* puede utilizar los mandatos *smbmnt* y *smbumount*. Deberá entonces establecer permisos de SUID a dichos mandatos. Puede hacerlo ejecutando, como *root* lo siguiente:

```
chmod 4755 /usr/bin/smbmnt
chmod 4755 /usr/bin/smbumount
```

Para acceder hacia una máquina Windows® determine primero qué volúmenes o recursos compartidos posee ésta. Utilice el mandato *smbclient* del siguiente modo:

```
smbclient -N -L alguna_maquina
```

Lo cual le devolvería más menos lo siguiente:

```
Anonymous login successful
Domain=[MI-DOMINIO] OS=[Unix] Server=[Samba 3.0.7-1.3E]
```

```
          Sharename       Type      Comment
          ---------       ----      -------
          homes           Disk      Home Directories
          netlogon        Disk      Network Logon Service
          ftp             Disk      ftp
          IPC$            IPC       IPC Service (Servidor Samba 3.0.7-1.3E en mi-servidor)
          ADMIN$          IPC       IPC Service (Servidor Samba 3.0.7-1.3E en mi-servidor)
          epl5900         Printer   Created by redhat-config-printer 0.6.x
          hp2550bw        Printer   Created by redhat-config-printer 0.6.x
Anonymous login successful
Domain=[MI-DOMINIO] OS=[Unix] Server=[Samba 3.0.7-1.3E]

          Server               Comment
          ---------            -------
          mi-servidor          Servidor Samba 3.0.7-1.3E en mi-servidor

          Workgroup            Master
          ---------            -------
          MI-DOMINIO           MI-SERVIDOR
```

En el ejemplo anterior hay un volumen compartido llamado *algún_volumen*. Si queremos montarlo, debemos crear un punto de montaje. Éste puede crearse en cualquier directorio sobre el que tengamos permisos de escritura. Para montarlo, utilizamos entonces la siguiente línea de mandato:

```
smbmount //alguna_maquina/algún_volumen /punto/de/montaje/
```

Si la máquina Windows® requiere un usuario y una clave de acceso, puede añadir a lo anterior las opciones *-username=el_necesario -password=el_requerido -workgroup=MIGRUPO*

Si la distribución de GNU/Linux utilizada es reciente, también puede utilizar el ya conocido mandato *mount* del siguiente modo:

```
mount -t smbfs -o username=el_necesario,password=el_requerido
//alguna_maquina/algún_volumen /punto/de/montaje/
```

Si se genera una cuenta *pcguest*, similar a la cuenta *nobody*, podemos montar volúmenes SMB sin ingresar una clave de acceso pero con privilegios restringidos, o aquellos que definamos a un volumen accedido por un usuario invitado. Esto sería el método por elección para compartir volúmenes en una red de área local. Puede generarse una cuenta *pcguest* o bien dejar que el sistema tome al usuario *nobody*. Si opta por lo primero, sólo dé de alta la cuenta, **NO** asigne clave de acceso alguna. Montar volúmenes remotos como usuario invitado es muy sencillo. Un ejemplo real sería:

```
mount -t smbfs -o guest //LINUX/FTP //var/ftp
```

Lo anterior monta un volumen SAMBA de una máquina con GNU/Linux en otra máquina con GNU/Linux.

Puede añadirse también una entrada en */etc/fstab* de modo que sólo tenga que ser tecleado *mount /punto/de/montaje*. Esta línea sería de modo similar al siguiente:

```
//LINUX/FTP   /var/ftp   smbfs   user,auto,guest,ro,gid=100   0 0
```

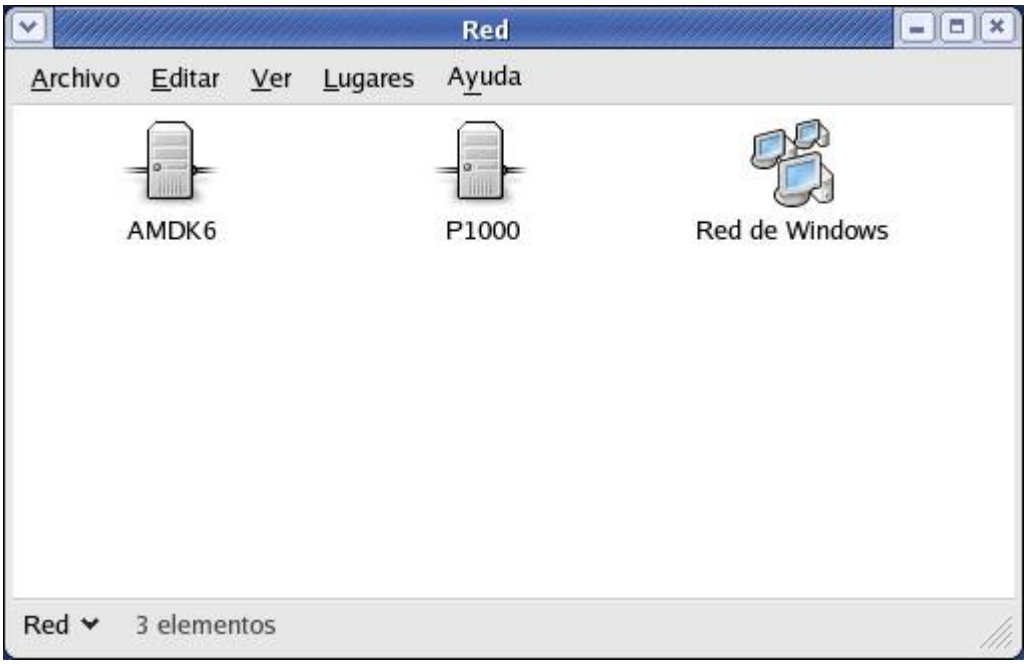
Recuérdese que el volumen compartido debe estar configurado para permitir usuarios invitados:

```
[FTP]
        comment = Programática libre (RPMS)
        path = /var/ftp/pub
        public = Yes
        guest ok = Yes
```

40.6.2. Modo gráfico

40.6.2.1. Desde el entorno de GNOME

Si utiliza GNOME 2.x o superior, éste incluye un módulo para Nautilus que permite acceder hacia los recursos compartidos a través de Samba sin necesidad de modificar cosa alguna en el sistema. Solamente hay que hacer clic en **Servidores de red** en el menú de GNOME.



40.6.2.2. Desde Windows

Por su parte, desde Windows deberá ser posible acceder sin problemas hacia Samba como si fuese hacia cualquier otra máquina con Windows. Ni Windows ni el usuario notarán siquiera la diferencia.

40.7. Uniendo máquinas al dominio del Controlador Primario de Dominio

El controlador de dominio permite utilizar Samba como servidor de autenticación y servidor de archivos que además permite almacenar el perfil, preferencias y documentos del usuario en el servidor automáticamente sin la intervención del usuario.

40.7.1. Creando manualmente cuentas de máquinas

Bajo algunas circunstancias será necesario crear cuentas de máquinas (trust accounts o cuentas de confianza) a fin de permitir unirse al dominio. El procedimiento es simple:

```
/usr/sbin/useradd -d /dev/null -g 100 -s /bin/false -c "Cuenta de máquina" -M maquina-windows$
smbpasswd -a maquina-windows$
```

Cabe resaltar que las cuentas de máquinas deben incluir **obligatoriamente** un símbolo $ al final del nombre.

40.7.2. Windows 95/98/ME y Windows XP Home

Ya que los sistemas con Windows 95/98/ME y Windows XP Home no incluyen una implementación completa como miembros de dominio, no se requieren cuentas de confianza. El procedimiento para unirse al dominio es el siguiente:

- Acceder hacia Menú de inicio → Configuraciones → Panel de control → Red.
- Seleccione la pestaña de Configuración.
- Seleccione «Cliente de redes Microsoft».
- Haga clic en el botón de propiedades.
- Seleccione Acceder a dominio de Windows NT y especifique el dominio correspondiente.
- Haga clic en todos los botones de «Aceptar» y reinicie el sistema.
- Acceda con cualquier usuario que haya sido dado de alta en el servidor Samba y que además cuente con una clave de acceso asignada con smbpasswd.

40.7.3. Windows NT

- Crear manualmente la cuenta de máquina como se describió anteriormente.
- Acceder hacia Menú de inicio → Configuraciones → Panel de control → Red.
- Seleccionar la pestaña de «Identificación».
- Clic en el botón de «Cambiar».
- Ingrese el nombre del dominio y el nombre del sistema. **No selecione** «Crear una cuenta de máquina en el Dominio».
- Clic en «Aceptar».
- Espere algunos segundos.
- Deberá mostrarse un mensaje emergente de confirmación que dice «Bienvenido a MI-DOMINIO».
- Reinicie el sistema.
- Acceda con cualquier usuario que haya sido dado de alta en el servidor Samba y que además cuente con una clave de acceso asignada con smbpasswd.

40.7.4. Windows 2000/2003 y Windows XP Profesional

- Clic derecho en el icono de «Mi PC».
- Seleccionar «Propiedades».

- Haga clic en la pestaña de «Identificación de red» o «Nombre del sistema».
- Clic en el botón de «Propiedades».
- Clic en el botón «Miembro de dominio».
- Ingrese el nombre del dominio y el nombre de la máquina y haga clic en el botón de «Aceptar».
- Aparecerá un diálogo que preguntará por una cuenta y clave de acceso con privilegios de administración en el servidor. Especifique la root y la clave de acceso que asignó a la cuenta de root con el mandato smbpasswd (**NO LA CLAVE DE ACCESO DE ROOT EN EL SISTEMA**).
- Espere algunos segundos.
- Deberá mostrarse un mensaje emergente de confirmación que dice «Bienvenido a MI-DOMINIO».
- Reinicie el sistema.
- Acceda con cualquier usuario que haya sido dado de alta en el servidor Samba y que además cuente con una clave de acceso asignada con smbpasswd.

41. La ingeniería social y los [incorrectos] hábitos del usuario

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

El «Talón de Aquiles» de cualquier red lo componen los usuarios que la integran. La mejor tecnología y seguridad del mundo es inservible cuando un usuario es incapaz de mantener en secreto una clave de acceso o información confidencial. Es por tal motivo que tiene particular relevancia el impulsar una cultura de concienciar a los usuarios acerca de los peligros de la Ingeniería Social en la seguridad informática. El más célebre personaje que utilizó ésta tan exitosamente, que durante algún tiempo se convirtió en el hombre más buscado por el FBI fue Kevin Mitnick.

> *Ingeniería Social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que "los usuarios son el eslabón débil" en seguridad; éste es el principio por el que se rige la ingeniería social.*
>
> *Wikipedia, la enciclopedia libre.*

Clásicos ejemplos de ataques exitosos aprovechando la ingeniería social es el envío de los adjuntos en el correo electrónico (virus, troyanos y gusanos) que pueden ejecutar código malicioso en una estación de trabajo o computadora personal.

Lo anterior fue lo que obligó a los proveedores de sustento lógico a desactivar le ejecución automática de los adjuntos al abrir el mensaje de correo electrónico, por lo que es necesario que el usuario active esta funcionalidad de modo explícito a fin de volver a ser vulnerable. Sin embargo, la mayoría de los usuarios simplemente hacen clic con el ratón a cualquier cosa que llegue en el correo electrónico, haciendo que éste método de ingeniería social sea exitoso.

Otro tipo de ataque de ingeniería social e increíblemente el más fácil de realizar, consiste en engañar a un usuario haciéndole pensar que se trata de un administrador de la red donde se labora solicitando claves de acceso u otro tipo de información confidencial. Buena parte del correo electrónico que llega al buzón del usuario consiste de engaños solicitando claves de acceso, número de tarjeta de crédito y otra información, haciendo pensar que es con una finalidad legítima, como sería el caso de reactivar o crear una cuenta o configuración. Este tipo de ataque se conoce actualmente como *phising* (pesca).

Lamentablemente muchos estudios muestran que los usuarios tienen una pobre conciencia acerca de la importancia de la seguridad. Una encuesta de InfoSecurity arrojó como resultados que 90% de los oficinistas revelaría una clave de acceso a cambio de un bolígrafo.

Un tipo de ingeniería social muy efectivo es incluir grandes cantidades de texto a un acuerdo de licenciamiento. La gran mayoría de los usuarios, incluyendo administradores, rara vez leen siquiera una palabra contenida en dicho texto y sencillamente dan clic en la aceptación de licenciamientos y acuerdos. Esto regularmente es aprovechado por Adware (sustento lógico que despliega anuncios comerciales) y Spyware (sustento lógico que espía la actividad del usuario). En Latinoamérica este problema es aún mayor debido al vergonzoso y pobre índice de lectura (menos de un libro por año).

La principal defensa contra la ingeniería social es la educación del usuario, empezando por los propios administradores de redes. La mejor forma de combatir la ingeniería social es la prevención.

41.1. Recomendaciones para evitar ser víctimas de la ingeniería social a través del correo electrónico

- No utilizar cuentas de correo electrónico para uso personal para asuntos laborales.
- No utilizar cuentas de correo electrónico destinadas para uso laboral para asuntos personales.
- Adiestrar a los usuarios para jamás publicar cuentas de correo en áreas públicas que permitan sean cosechadas a través de sustento lógico hecho para este fin.
- Adiestrar al usuario para no publicar cuentas de correo electrónico en lugares públicos.
- Adiestrar al usuario para evitar proporcionar cuentas de correo electrónico y otros datos personales a personas o entidades que puedan utilizar éstos con otros fines.
- Evitar publicar direcciones de correo electrónico en formularios destinados a recabar datos de los clientes utilizando formularios que oculten la dirección de correo electrónico.
- Si es inevitable, utilizar una cuenta destinada y dedicada para ser mostrada a través de HTTP.
- Adiestrar al usuario a utilizar claves de acceso más complejas.
- Adiestrar al usuario a no abrir y dar clic a todo lo que llegue por correo.
- Adiestrar al usuario para jamás responder a un mensaje de spam.
- Adiestrar al usuario a no hacer clic en los enlaces en los mensajes de spam y que pueden ser utilizados para confirmar al spammer que se trata de una cuenta de correo activa.

42. Configuración básica de Sendmail

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

42.1. Introducción

42.1.1. Acerca de Sendmail

Es el más popular agente de transporte de correo (MTA o **M**ail **T**ransport **A**gent), responsable quizá de poco más del 70% del correo electrónico del mundo. Aunque por largo tiempo se le ha criticado por muchos incidentes de de seguridad, lo cierto es que éstos siempre han sido resueltos en pocas horas.

URL: http://www.sendmail.org/.

42.1.2. Acerca de Dovecot

Dovecot es un servidor de POP3 e IMAP de fuente abierta que funciona en Linux y sistemas basados sobre Unix™ y está diseñado con la seguridad como principal objetivo. **Dovecot** puede utilizar tanto el formato **mbox** como **maildir** y es compatible con las implementaciones de los servidores UW-IMAP y Courier IMAP.

URL: http://dovecot.procontrol.fi/.

42.1.3. Acerca de SASL y Cyrus SASL

SASL (**S**imple **A**uthentication and **S**ecurity **L**ayer) es un estructura para la seguridad de datos en protocolos de Internet. Desempareja mecanismos de la autenticación desde protocolos de aplicaciones, permitiendo, en teoría, cualquier mecanismo de autenticación soportado por SASL para ser utilizado en cualquier protocolo de aplicación que capaz de utilizar SASL. Actualmente SASL es un protocolo de la IETF (**I**nternet **E**ngineering **T**ask **F**orce) que ha sido propuesto como estándar. Está especificado en el **RFC 2222** creado por John Meyers en la Universidad Carnegie Mellon.

Cyrus SASL es una implementación de **SASL** que puede ser utilizada del lado del servidor o del lado del cliente y que incluye como principales mecanismos de autenticación soportados a ANONYMOUS, CRAM-MD5, DIGEST-MD5, GSSAPI y PLAIN. El código fuente incluye también soporte para los mecanismos LOGIN, SRP, NTLM, OPT y KERBEROS_V4.

URL: http://asg.web.cmu.edu/sasl/sasl-library.html.

42.1.4. Protocolos utilizados

42.1.4.1. SMTP (Simple Mail Transfer Protocol)

Es un **protocolo estándar** de Internet del **Nivel de Aplicación** utilizado para la transmisión de correo electrónico a través de una conexión TCP/IP. Este es de hecho el único protocolo utilizado para la transmisión de correo electrónico a través de Internet. Es un protocolo basado sobre texto y relativamente simple donde se especifican uno más destinatarios en un mensaje que es transferido. A lo largo de los años han sido muchas las personas que han editado o contribuido a las especificaciones de **SMTP**, entre las cuales están Jon Postel, Eric Allman, Dave Crocker, Ned Freed, Randall Gellens, John Klensin y Keith Moore.

Para determinar el servidor **SMTP** para un dominio dado, se utilizan los registros **MX** (**M**ail E**x**changer) en la Zona de Autoridad correspondiente a ese mismo dominio contestado por un **Servidor DNS**. Después de establecerse una conexión entre el remitente (el cliente) y el destinatario (el servidor), se inicia una sesión **SMTP**, ejemplificada a continuación.

```
Cliente:  $ telnet 127.0.0.1 25
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^]'.
          220 nombre.dominio ESMTP Sendmail 8.13.1/8.13.1; Sat, 18 Mar 2006
          16:02:27 -0600
Cliente:  HELO localhost.localdomain
Servidor: 250 nombre.dominio Hello localhost.localdomain [127.0.0.1], pleased to
          meet you
Cliente:  MAIL FROM:<fulano@localhost.localdomain>
Servidor: 250 2.1.0 <fulano@localhost.localdomain>... Sender ok
Cliente:  RCPT TO:<root@localhost.localdomain>
Servidor: 250 2.1.5 <root@localhost.localdomain>... Recipient ok
Cliente:  DATA
Servidor: 354 Enter mail, end with "." on a line by itself
Cliente:  Subject: Mensaje de prueba
          From: fulano@localhost.localdomain
          To: root@localhost.localdomain

          Hola. Este es un mensaje de prueba.
          Adios.
          .
Servidor: 250 2.0.0 k2IM2RjA003987 Message accepted for delivery
Cliente:  QUIT
Servidor: 221 2.0.0 nombre.dominio closing connection
Servidor: Connection closed by foreign host.
```

La descripción completa del protocolo original **STMP** está definido en el **RFC 821**, aunque el protocolo utilizado hoy en día, también conocido como **ESMTP** (**E**xtended **S**imple **M**ail **T**ransfer **P**rotocol), está definido en el **RFC 2821**. **SMTP** trabaja sobre **TCP** en el puerto 25.

42.1.4.2. POP3 (Post Office Protocol, version 3)

Es un **protocolo estándar** de Internet del **Nivel de Aplicación** que recupera el correo electrónico desde un servidor remoto a través de una conexión TCP/IP desde un cliente local. El diseño de **POP3** y sus predecesores es permitir a los usuarios recuperar el correo electrónico al estar conectados hacia una red y manipular los mensajes recuperados sin necesidad de permanecer conectados. A pesar de que muchos clientes de correo electrónico incluyen soporte para dejar el correo en el servidor, todos los clientes de POP3 recuperan todos los mensajes y los almacenan como **mensajes nuevos** en la computadora o anfitrión utilizado por el usuario, eliminan los mensajes en el servidor y terminan la conexión.

Después de establecerse una conexión entre el cliente y el servidor, se inicia una sesión **POP3**,

ejemplificada a continuación.

```
Cliente:  $ telnet 127.0.0.1 110
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^]'.
          +OK dovecot ready.
Cliente:  USER fulano
Servidor: +OK
Cliente:  PASS clave de accceso
Servidor: +OK Logged in.
Cliente:  STAT
Servidor: +OK 1 728
Cliente:  LIST
Servidor: +OK 1 messages:
          1 728
          .
Cliente:  RETR 1
Servidor: +OK 728 octets
          Return-Path: <fulano@localhost.localdomain>
          Received: from localhost.localdomain (localhost.localdomain
          [192.168.1.254])
                   by localhost.localdomain (8.13.1/8.13.1) with SMTP id
          k2IM2RjA003987
                   for <root@localhost.localdomain>; Sat, 18 Mar 2006 16:03:21
          -0600
          Date: Sat, 18 Mar 2006 16:02:27 -0600
          Message-Id: <200603182203.k2IM2RjA003987@localhost.localdomain>
          Subject: Mensaje de prueba
          From: fulano@localhost.localdomain
          To: root@localhost.localdomain
          Status: O
          Content-Length: 43
          Lines: 2
          X-UID: 202
          X-Keywords:

          Hola. Este es un mensaje de prueba.
          Adios.
          .
Cliente:  QUIT
Servidor: +OK Logging out.
          Connection closed by foreign host.
```

POP3 está definido en el **RFC 1939**. **POP3** trabaja sobre **TCP** en el puerto 110.

42.1.4.3. IMAP (Internet Message Access Protocol)

Es un **protocolo estándar** de Internet del **Nivel de Aplicación** utilizado para acceder hacia el correo electrónico en un servidor remoto a través de una conexión TCP/IP desde un cliente local.

La versión más reciente de **IMAP** es la 4, revisión 1, y está definida en el **RFC 3501**. **IMAP** trabaja sobre **TCP** en el puerto 143.

Fue diseñado por Mark Crispin en 1986 como una alternativa más moderna que cubriera las deficiencias de **POP3**. Las características más importantes de **IMAP** incluyen:

- Soporte para los modos de operación conectado (connected) y desconectado (disconnected), permitiendo a los clientes de correo electrónico permanezcan conectados el tiempo que su interfaz permanezca activa, descargando los mensajes conforme se necesite.
- A diferencia de **POP3**, permite accesos simultáneos desde múltiples clientes y proporciona los mecanismos necesarios para éstos para que se detecten los

cambios hechos por otro cliente de correo electrónico concurrentemente conectado en el mismo buzón de correo.

- Permite a los clientes obtener individualmente cualquier parte **MIME** (acrónimo de **M**ulti-Purpose **I**nternet **M**ail **E**xtensions o Extensiones de correo de Internet de propósitos múltiples), así como también obtener porciones de las partes individuales o bien los mensajes completos.
- A través de **banderas** definidas en el protocolo, vigilar la información de estado de los mensajes de correo electrónico que se mantengan en el servidor. Por ejemplo si el estado del mensaje es **leído**, **no leído**, **respondido** o **eliminado**.
- Incluye soporte para múltiples buzones de correo electrónico que permite crear, renombrar o eliminar mensajes de correo electrónico presentados en el servidor dentro de carpetas, y mover éstos mensajes entre distintas cuentas de correo electrónico. Esta característica también permite al servidor proporcionar acceso hacia los carpetas públicas y compartidas.
- Incluye soporte para realizar búsquedas del lado del servidor a través de mecanismos que permiten obtener resultados de acuerdo a varios criterios, permitiendo evitar que los clientes de correo electrónico tengan que descargar todos los mensajes desde el servidor.
- Las especificaciones del protocolo **IMAP** definen un mecanismo explícito mediante el cual puede ser mejorada su funcionalidad a través de extensiones. Un ejemplo es la extensión **IMAP IDLE**, la cual permite sincronizar ente el servidor y el cliente a través de avisos.

Después de establecerse una conexión entre el cliente y el servidor, se inicia una sesión **IMAP**, ejemplificada a continuación.

```
Cliente:  $ telnet 127.0.0.1 143
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^]'.
          * OK dovecot ready.
          +OK dovecot ready.
Cliente:  x LOGIN fulano clave de acceso
Servidor: x OK Logged in.
Cliente:  x SELECT inbox
Servidor: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
          * OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags
          permitted.
          * 1 EXISTS
          * 0 RECENT
          * OK [UNSEEN 1] First unseen.
          * OK [UIDVALIDITY 1100569382] UIDs valid
          * OK [UIDNEXT 203] Predicted next UID
          x OK [READ-WRITE] Select completed.
Cliente:  x FETCH 1 (flags body[header.fields (subject)])
Servidor: * 1 FETCH (FLAGS (\Seen) BODY[HEADER.FIELDS (SUBJECT)] {30}
          Subject: Mensaje de prueba

          )
          x OK Fetch completed.
          .
Cliente:  x FETCH 1 (body[text])
Servidor: * 1 FETCH (BODY[TEXT] {45}
          Hola. Este es un mensaje de prueba.
          Adios.
          )
          x OK Fetch completed.
Cliente:  x LOGOUT
Servidor: * BYE Logging out
          x OK Logout completed.
          Connection closed by foreign host.
```

42.2. Equipamiento lógico necesario

- sendmail
- sendmail-cf
- dovecot (o bien imap)
- m4
- make
- cyrus-sasl
- cyrus-sasl-md5
- cyrus-sasl-plain

42.2.1. Instalación a través de yum

Si se utiliza de CentOS 4 o White Box Enterprise Linux 4, el paquete imap es reemplazado por el paquete **dovecot**. De tal modo que se ejecuta lo siguiente:

```
yum -y install sendmail sendmail-cf dovecot m4 make cyrus-sasl cyrus-sasl-md5 cyrus-sasl-plain
```

Si se utiliza de CentOS 3 o White Box Enterprise Linux 3, el paquete imap es reemplazado por el paquete **dovecot**. De tal modo que se ejecuta lo siguiente:

```
yum -y install sendmail sendmail-cf imap m4 make cyrus-sasl cyrus-sasl-md5 cyrus-sasl-plain
```

Si acaso estuviese instalado, elimine el paquete cyrus-sasl-gssapi, ya que éste utiliza el método de autenticación GSSAPI, mismo que requeriría de la base de datos de cuentas de usuario de un servidor Kerberos:

```
yum -y remove cyrus-sasl-gssapi
```

42.2.2. Instalación a través de Up2date

Si se utiliza de Red Hat™ Enterprise Linux 4, el paquete imap es reemplazado por el paquete **dovecot**. De tal modo que se ejecuta lo siguiente:

```
up2date -i sendmail sendmail-cf dovecot m4 make cyrus-sasl cyrus-sasl-md5 cyrus-sasl-plain
```

Si se utiliza de Red Hat™ Enterprise Linux 3, el paquete imap es reemplazado por el paquete **dovecot**. De tal modo que se ejecuta lo siguiente:

```
up2date -i sendmail sendmail-cf imap m4 make cyrus-sasl cyrus-sasl-md5 cyrus-sasl-plain
```

Si acaso estuviese instalado, elimine el paquete **cyrus-sasl-gssapi**, ya que éste utiliza el método de autenticación **GSSAPI**, mismo que requeriría de la base de datos de cuentas de usuario de un servidor Kerberos:

```
rpm -e cyrus-sasl-gssapi
```

42.3. Procedimientos

42.3.1. Alta de cuentas de usuario y asignación de claves de acceso

El alta de usuarios a través de este método será diferente de la manera tradicional, debido a que para utilizar el método de autenticación para **SMTP**, Sendmail utilizará **SASL**. Por tal motivo, el alta de cuentas de usuario de correo deberá de seguir el siguiente procedimiento:

1. Alta de la cuenta del usuario en el sistema, la cual se sugiere no deberá tener acceso a intérprete de mandato alguno:

```
useradd -s /sbin/nologin fulano
```

2. Asignación de claves de acceso en el sistema para permitir autenticar a través de los métodos **PLAIN** y **LOGIN** para autenticar **SMTP** y a través de los protocolos **POP3** e **IMAP**:

```
passwd usuario
```

3. Asignación de claves de acceso para autenticar **SMTP** a través de métodos cifrados (**CRAM-MD5** y **DIGEST-MD5**) en sistemas con versión de Sendmail compilada contra **SASL-2** (Red Hat™ Enterprise Linux 4, CentOS 4 o White Box Enterprise Linux 4), requieren utilizar el mandato **saslpasswd2** del siguiente modo:

```
saslpasswd2 usuario
```

4. Asignación de claves de acceso para autenticar **SMTP** a través de métodos cifrados (**CRAM-MD5** y **DIGEST-MD5**) en sistemas con versión de Sendmail compilada contra **SASL-1** (Red Hat™ Enterprise Linux 3, CentOS 3 o White Box Enterprise Linux 3), requieren utilizar el mandato **saslpasswd** del siguiente modo:

```
saslpasswd usuario
```

5. La autenticación para **SMTP** a través de cualquier mecanismo requiere se active e inicie el servicio de **saslauthd** del siguiente modo:

```
chkconfig saslauthd on
service saslauthd start
```

Puede mostrarse la lista de los usuarios con clave de acceso a través de SASL-2 utilizando el mandato **sasldblistusers2**. Puede mostrarse la lista de los usuarios con clave de acceso a través de SASL-1 utilizando el mandato **sasldblistusers**. Si ya se cuenta con un grupo de claves de acceso de usuarios dados de alta en SASL-1, se pueden convertir hacia SASL-2 con el mandato **dbconverter-2**.

42.3.2. Dominios a administrar

Establecer dominios a administrar en el fichero **/etc/mail/local-host-names** del siguiente modo:

```
dominio.com
mail.dominio.com
mi-otro-dominio.com
mail.mi-otro-dominio.com
```

Establecer dominios permitidos para poder enviar correo en:

```
vi /etc/mail/relay-domains
```

Por defecto, no existe dicho fichero, hay que generarlo. Para fines generales tiene el mismo contenido de **/etc/mail/local-host-names** a menos que se desee excluir algún dominio en particular.

```
dominio.com
mail.dominio.com
dominio2.com
mail.dominio2.com
```

42.3.3. Control de acceso

Definir lista de control de acceso en:

```
vi /etc/mail/access
```

Incluir solo las IPs locales del servidor y la lista negra de direcciones de correo, dominios e IPs denegadas. Considere que cualquier IP que vaya acompañada de RELAY se le permitirá enviar correo sin necesidad de autenticar, lo cual puede ser útil si se utiliza un cliente de correo con interfaz HTTP (Webmail) en otro servidor. Ejemplo:

```
# Check the /usr/share/doc/sendmail/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail/README.cf is part of the sendmail-doc
# package.
#
# by default we allow relaying from localhost...
localhost.localdomain   RELAY
localhost               RELAY
127.0.0.1               RELAY
#
# Dirección IP del propio servidor.
192.168.1.254           RELAY
#
# Otros servidores de correo en la LAN a los que se les permitirá enviar
# correo libremente a través del propio servidor de correo.
192.168.1.253           RELAY
192.168.1.252           RELAY
#
# Direcciones IP que solo podrán entregar correo de forma local, es decir,
# no pueden enviar correo fuera del propio servidor.
192.168.2.24            OK
192.168.2.23            OK
192.168.2.25            OK
#
# Lista negra
usuario@molesto.com     REJECT
productoinutil.com.mx   REJECT
10.4.5.6                REJECT
#
# Bloques de Asia Pacific Networks, ISP desde el cual se emite la mayor
# parte del Spam del mundo.
# Las redes involucradas abarcan Australia, Japón, China, Korea, Taiwan,
```

```
# Hong Kong e India por lo que bloquear el correo de dichas redes significa
# cortar comunicación con estos países, pero acaba con entre el 60% y 80%
# del Spam.
222                     REJECT
221                     REJECT
220                     REJECT
219                     REJECT
218                     REJECT
212                     REJECT
211                     REJECT
210                     REJECT
203                     REJECT
202                     REJECT
140.109                 REJECT
133                     REJECT
61                      REJECT
60                      REJECT
59                      REJECT
58                      REJECT
```

42.3.4. Alias de la cuenta de root

No es conveniente estar autenticando la cuenta de root a través de la red para revisar los mensajes originados por el sistema. Se debe definir alias para la cuenta de root a donde redireccionar el correo en el fichero **/etc/aliases** del siguiente modo:

```
root:           fulano
```

42.3.5. Configuración de funciones de Sendmail

Modificar el fichero **/etc/mail/sendmail.mc** y desactivar o habilitar funciones:

```
vi /etc/mail/sendmail.mc
```

42.3.5.1. confSMTP_LOGIN_MSG

Este parámetro permite establecer el mensaje de bienvenida al establecer la conexión al servidor. Es posible ocultar el nombre y al versión de Sendmail, esto con el objeto de agregar seguridad por secreto. Funciona simplemente haciendo que quien se conecte hacia el servidor no pueda saber qué sustento lógico y versión del mismo se está utilizando y con ellos dificultar a un delincuente o abusador de servicio el determinar qué vulnerabilidad específica explotar. Recomendamos utilizar lo siguiente:

```
define(`confSMTP_LOGIN_MSG',`$j ; $b')dnl
```

Lo anterior regresará algo como lo siguiente al realizar una conexión hacia el puerto 25 del servidor:

```
$ telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to nombre.dominio.
Escape character is '^]'.
220 nombre.dominio ESMTP ; Mon, 17 May 2004 02:22:29 -0500
quit
```

```
221 2.0.0 nombre.dominio closing connection
Connection closed by foreign host.
$
```

Está configuración se puede poner justo antes de la líena correspondiente al parámetro **confAUTH_OPTIONS**.

42.3.5.2. confAUTH_OPTIONS

Si se utiliza la siguiente línea, habilitada por defecto, se permitirá realizar autenticación a través del puerto 25 por cualquier método, incluyendo PLAIN, el cual se realiza en texto simple. Esto implica cierto riesgo de seguridad.

```
define(`confAUTH_OPTIONS',`A')dnl
```

Si comenta la anterior línea con **dnl**, y se utiliza en cambio la siguiente línea, se desactiva la autenticación por una de texto simple en conexiones no seguras (TLS), de modo tal que sólo se podrá autenticar a través de métodos que utilicen cifrado, como sería CRAM-MD5 y DIGEST-MD5. **Esto obliga a utilizar clientes de correo electrónico con soporte para autenticación a través de CRAM-MD5 y DIGEST-MD5**.

```
define(`confAUTH_OPTIONS',`A p')dnl
```

42.3.5.3. TRUST_AUTH_MECH y confAUTH_MECHANISMS

Si se desea utilizar SMTP autenticado para equipos no incluidos dentro del fichero **/etc/mail/access**, se requieren descomentar las siguientes dos líneas, eliminando el **dnl** que les precede:

```
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5LOGIN PLAIN')dnl
```

42.3.5.4. DAEMON_OPTIONS

De modo predefinido **Sendmail** escucha peticiones a través de la interfaz de retorno del sistema por medio de **IPv4** (127.0.0.1) y no a través de otros dispositivos de red. Sólo se necesita eliminar las restricción de la interfaz de retorno para poder recibir correo desde Internet o la LAN. Localice la siguiente línea:

```
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
```

Elimine de dicho parámetro el valor **Addr=127.0.0.1** y la coma (,) que le antecede, del siguiente modo:

```
DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl
```

42.3.5.5. FEATURE(`accept_unresolvable_domains')

De modo predefinido, como una forma de permitir el correo del propio sistema en una computadora de escritorio o una computadora portátil, está se utiliza el parámetro **FEATURE(`accept_unresolvable_domains')**. Sin embargo se recomienda desactivar esta función a fin de impedir aceptar correo de dominios inexistentes (generalmente utilizado para el envío de correo masivo no solicitado o **Spam**), basta con comentar esta configuración precediendo un **dnl**,

del siguiente modo:

```
dnl FEATURE(`accept_unresolvable_domains')dnl
```

42.3.5.6. Enmascaramiento

Habilitar las siguientes lineas y adaptar valores para definir la máscara que utilizará el servidor:

```
MASQUERADE_AS(`dominio.com')dnl
FEATURE(masquerade_envelope)dnl
FEATURE(masquerade_entire_domain)dnl
```

Si va a administrar múltiples dominios, declare los dominios que no se quiera enmascarar con el parámetro **MASQUERADE_EXCEPTION** del siguiente modo:

```
MASQUERADE_AS(`dominio.com')dnl
MASQUERADE_EXCEPTION(`dominio2.net')dnl
MASQUERADE_EXCEPTION(`dominio3.org')dnl
MASQUERADE_EXCEPTION(`dominio4.com.mx')dnl
FEATURE(masquerade_envelope)dnl
FEATURE(masquerade_entire_domain)dnl
```

42.3.5.7. Parámetro Cw

Añadir al final del fichero **/etc/mail/sendmail.mc** un parámetro que defina qué *dominio.com* se trata de un dominio local. Note que no debe haber espacios entre **Cw** y **dominio.com**, y que **Cw** se escribe con una **C** mayúscula y una **w** minúscula.

```
Cwdominio.com
```

42.3.6. Usuarios Virtuales

Si se desea brindar un servicio de hospedaje de dominios virtuales permitiendo que los usuarios envíen y reciban correo utilizando sus propios dominios, se deben añadir los siguientes parámetros debajo de la función de **virtusertable** del fichero **/etc/mail/sendmail.mc**:

```
FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable.db')dnl
FEATURE(`genericstable',`hash -o /etc/mail/genericstable.db')dnl
GENERICS_DOMAIN_FILE(`/etc/mail/generics-domains')dnl
```

Se generan tres ficheros **nuevos** dentro del directorio `/etc/mail`:

```
touch /etc/mail/{virtusertable,genericstable,generics-domains}
```

El fichero **/etc/mail/virtusertable** sirve para definir qué cuentas de correo virtuales se entregan en los buzones correspondientes. **La separación de columnas se hace con tabuladores**. En el ejemplo se entrega el correo de webmaster@dominio1.net en la cuenta mengano y el correo de webmaster@dominio2.com en el buzón del usuario perengano:

```
webmaster@dominio1.net          mengano
webmaster@dominio2.com          perengano
```

Para hacer que el correo del usuario mengano salga del servidor como webmaster@dominio1.net y el de perengano salga como webmaster@dominio2.com, es necesario hacer el contenido contrario de **/etc/mail/virtusertable** del siguiente modo:

```
mengano                 webmaster@dominio1.net
perengano               webmaster@dominio2.com
```

Para efector prácticos, se pueden mantener sincronizados ambos ficheros trabajando directamente con **/etc/mail/virtusertable** y ejecutando el siguiente guión que se encargará de pasar el texto desde **/etc/mail/virtusertable** con orden invertido de columnas hacia **/etc/mail/genericstable**.

```
while read cuenta usuario garbage
do
echo -e "${usuario}\t${cuenta}" >> /tmp/genericstable
done < /etc/mail/virtusertable
mv /tmp/genericstable /etc/mail/genericstable
```

El fichero **/etc/mail/generics-domains** debe contener prácticamente lo mismo que **/etc/mail/local-host-names** más los dominios que vayan a estar siendo utilizados por dominios virtuales.

```
dominio.com
dominio1.net
dominio2.com
```

Invariablemente los ficheros **/etc/mail/virtusertable.db** y **/etc/mail/genericstable.db** deben actualizarse con el contenido de **/etc/mail/virtusertable** y **/etc/mail/genericstable**, respectivamente, cada vez que se se realice cualquier tipo de cambio, como actualizar, añadir o eliminar cuentas de correo virtuales.

```
for f in virtusertable genericstable
do
makemap hash /etc/mail/${f}.db < ${f}
done
```

42.3.7. Control del correo chatarra (Spam) a través de DNSBLs

Si se desea cargar *listas negras* para mitigar el Spam, pueden añadirse las siguientes líneas justo arriba de *MAILER(smtp)dnl*:

```
FEATURE(dnsbl, `blackholes.mail-abuse.org', `Rechazado - vea http://www.mail-abuse.org/rbl/')dnl
FEATURE(dnsbl, `dialups.mail-abuse.org', `Rechazado - vea http://www.mail-abuse.org/dul/')dnl
FEATURE(dnsbl, `relays.mail-abuse.org', `Rechazado - vea http://work-rss.mail-abuse.org/rss/')dnl
FEATURE(dnsbl, `sbl-xbl.spamhaus.org', `"550 Su IP esta en lista negra en Spamhaus - Por favor vea
http://www.spamhaus.org/query/bl?ip=+"$&{client_addr}')dnl
FEATURE(dnsbl, `bl.spamcop.net', `"550 Su IP esta en lista negra en SpamCOP - Por favor vea
http://spamcop.net/bl.shtml?"$&{client_addr}')dnl
FEATURE(dnsbl, `list.dsbl.org', `"550 Su IP esta en lista negra en DSBL - Por favor vea
http://dsbl.org/listing?"$&{client_addr}')dnl
FEATURE(dnsbl, `multihop.dsbl.org', `"550 Su IP esta en lista negra en DSBL - Por favor vea
http://dsbl.org/listing?"$&{client_addr}')dnl
FEATURE(dnsbl, `dnsbl.ahbl.org',`"550 Su IP esta en lista negra en AHBL - Por favor vea
http://www.ahbl.org/tools/lookup.php?ip="$&{client_addr}')dnl
FEATURE(dnsbl, `rhsbl.ahbl.org',`"550 Su IP esta en lista negra en AHBL - Por favor vea
http://www.ahbl.org/tools/lookup.php?ip="$&{client_addr}')dnl
FEATURE(dnsbl, `bl.csma.biz', `"550 Su IP esta en lista negra en CSMA - Por favor vea
http://bl.csma.biz/cgi-bin/listing.cgi?ip="$&{client_addr}')dnl
FEATURE(dnsbl, `dnsbl.antispam.or.id', `"550 Su IP esta en lista negra en ADNSBL - Por favor vea
http://antispam.or.id/?ip="$&{client_addr}')dnl
FEATURE(dnsbl, `blacklist.spambag.org', `"550 Su IP esta en lista negra en SPAMBAG - Por favor vea
```

```
http://www.spambag.org/cgi-bin/spambag?query="$&{client_addr}')dnl
```

42.3.8. Protocolos para acceder hacia el correo

Si utiliza Red Hat™ Enterprise Linux 4, CentOS 4 o White Box Enterprise Linux 4, el paquete imap es reemplazado por **dovecot**, el cual funciona como otros servicios. Se debe modificar el fichero **/etc/dovecot.conf** y habilitar los servicios de imap y/o pop3 del siguiente modo (de modo predefinido están habilitados imap e imaps):

```
# Protocols we want to be serving:
# imap imaps pop3 pop3s
protocols = imap pop3
```

El servicio se agrega al arranque del sistema y se inicia del siguiente modo:

```
chkconfig dovecot on
service dovecot start
```

Si utiliza Red Hat™ Enterprise Linux 3, CentOS 3 o White Box Enterprise Linux 3, el procedimiento utilizará el paquete imap, el cual requiere un simple mandato para activar el servicio.

```
chkconfig imap on
chkconfig ipop3 on
```

42.3.9. Reiniciando servicio

Para reiniciar servicio de Sendmail bastará con ejecutar:

```
service sendmail restart
```

Probar servidor enviando/recibiendo mensajes con CUALQUIER cliente estándar de correo electrónico con soporte para POP3/IMAP/SMTP con soporte para autenticar a través de SMTP utilizando los métodos DIGEST-MD5 o CRAM-MD5.

Para depurar posibles errores, se puede examinar el contenido de la bitácora de correo del sistema en **/var/log/maillog** del siguiente modo:

```
tail -f /var/log/maillog
```

42.4. Encaminamiento de dominios

Sendmail incluye soporte para realizar en re-encaminamiento de dominios de correo a través del parámetro **FEATURE(`mailertable',`hash -o /etc/mail/mailertable.db')** que debe estar **habilitado de modo predefinido** en el fichero **/etc/mail/sendmail.mc**. Esta función permite a Sendmail realizar traducción de dominios, especificar un agente de entrega y cambiar el encaminamiento establecido en un DNS.

42.4.1. Redundancia del servidor de correo.

Cuando se tiene un dominio de correo electrónico que recibe mucho tráfico, es conveniente establecer redundancia en el servicio para garantizar que el correo siempre será recibido y llegará a

los buzones de correo hacia los que está destinado.

Se requieren dos servidores de correo. Uno deberá estar registrado en la zona del dominio en el DNS como **servidor de correo primario** (*mail.dominio.com*) y otro deberá estar registrado en la zona del dominio en el DNS como **servidor de correo secundario** (*mail2.dominio.com*) a fin de contar con redundancia.

1. Defina en la zona de DNS de dominio.com un servidor de correo primario (*mail.dominio.com*) y un servidor de correo secundario (*mail2.dominio.com*)
2. Configure normalmente el servidor de correo primario (*mail.dominio.com*) para administrar el correo de dominio.com.
3. Configure el servidor de correo secundario (*mail2.dominio.com*) del mismo modo, pero no añada dominio.com en el fichero **/etc/mail/local-host-names** ya que de otro modo el correo será tratado como local y jamás podrá ser entregado en el servidor de correo primario.
4. Debe estar listado dominio.com en el fichero **/etc/mail/relay-domains** en el servidor de correo secundario (*mail2.dominio.com*) a fin de permitir la retransmisión de éste hacia el servidor de correo primario (*mail.dominio.com*).
5. En el servidor de correo secundario (*mail2.dominio.com*) modifique el fichero **/etc/mail/mailertable** y defina qué dominio.com será entregado en el servidor de correo primario utilizando el nombre plenamente resuelto en la zona del DNS.

   ```
   dominio.com             smtp:mail.dominio.com
   ```

   Si lo desea, puede especificar la dirección IP en lugar del nombre:

   ```
   dominio.com             smtp:[192.168.1.254]
   ```

6. Reinicie Sendmail

   ```
   service sendmail restart
   ```

7. En adelante el correo de dominio.com será entregado normalmente y de primera instancia en el servidor de correo primario (*mail.dominio.com*), pero cuando éste, por alguna razón, se vea imposibilitado para recibir conexiones, el servidor de correo secundario (*mail2.dominio.com*) definido en la zona de DNS recibirá todo el correo de dominio.com y lo entregará en el servidor de correo primario (*mail.dominio.com*) cuando éste reestablezca operaciones normalmente.

42.4.2. Servidor de correo intermediario

Sendmail puede servir de intermediario de correo electrónico ya sea para filtrado de correo con un antivirus, sustento lógico para filtrado de correo chatarra o bien como intermediario entre una red pública y un servidor en red local. Se requieren dos servidores de correo. Uno que será el servidor de correo intermediario (*proxy.dominio.com*), que de forma obligatoria deberá estar definido en la zona de DNS del dominio como servidor de correo primario (un registro MX), y otro que servirá como servidor de correo de destino (*mail.dominio.com*).

1. El servidor de correo que funcionará como intermediario (*proxy.dominio.com*) se configura normalmente, pero no añada dominio.com en el fichero **/etc/mail/local-host-names** ya que de otro modo el correo será tratado como local y jamás podrá ser entregado en el servidor de correo de destino (*mail.dominio.com*).
2. Debe estar listado dominio.com en el fichero **/etc/mail/relay-domains** en el servidor de correo intermediario (*proxy.dominio.com*) a fin de permitir la retransmisión de éste hacia el servidor de correo primario (*mail.dominio.com*).

3. La dirección P del servidor de destino (*mail.dominio.com*) debe estar listada en el fichero **/etc/mail/access** con **RELAY** (retransmisión autorizada) del servidor de correo intermediario (*proxy.dominio.com*).
4. La dirección P del servidor de intermediario (*proxy.dominio.com*) debe estar listada en el fichero **/etc/mail/access** con **RELAY** (retransmisión autorizada) del servidor de correo de destino (*mail.dominio.com*).
5. En el servidor de correo intermediario (*proxy.dominio.com*) modifique el fichero **/etc/mail/mailertable** y defina qué dominio.com será entregado en el servidor de correo de destino (*mail.dominio.com*) utilizando el nombre **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) y plenamente resuelto.

```
dominio.com             smtp:mail.dominio.com
```

6. Si lo desea, puede especificar la dirección IP en lugar del nombre:

```
dominio.com             smtp:[192.168.1.254]
```

7. En el servidor de correo de destino (*mail.dominio.com*), descomente y defina **proxy.dominio.com** como valor para el parámetro **define(`SMART_HOST',`smtp.your.provider')**, de modo que **proxy.dominio.com** sea el servidor de retransmisión (smart host:

```
define(`SMART_HOST',`proxy.dominio.com')
```

8. Reinicie Sendmail en ambos servidores de correo.

```
service sendmail restart
```

42.5. Verificando el servicio

Desde una terminal, ejecute el programa **telnet** dirigido hacia el puerto 25 de la dirección IP principal del sistema:

```
$ telnet 192.168.0.254 25
```

Si Sendmail está funcionando correctamente, se establecerá una conexión exitosa y deberá devolver una salida similar a la siguiente:

```
Trying 192.168.1.254...
Connected to nombre.dominio (192.168.1.254).
Escape character is '^]'.
220 nombre.dominio ESMTP Sendmail 8.13.1/8.13.1; Sun, 5 Mar 2006 21:45:51 -0600
```

Ejecute el mandato **HELO** seguido del nombre del anfitrión:

```
HELO nombre.dominio
```

Obtendrá una salida similar a esta:

```
250 nombre.dominio Hello nombre.dominio [192.168.1.254], pleased to meet you
```

Ejecute el mandato **EHLO** seguido del nombre del anfitrión:

```
EHLO nombre.dominio
```

Obtendrá una salida similar a ésta y que mostrará las funciones del servidor:

```
250-nombre.dominio Hello nombre.dominio [192.168.1.254], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
```

Ejecute el mandato **QUIT** para cerrar la conexión.

```
QUIT
```

El servidor deberá contestar lo siguiente al terminar la conexión:

```
221 2.0.0 nombre.dominio closing connection
Connection closed by foreign host.
```

La salida completa de todo el procedimiento anterior debe lucir similar a esto (mandatos utilizados resaltados en **negrita**):

```
[fulano@nombre ~]$ telnet 192.168.1.254 25
Trying 192.168.1.254...
Connected to nombre.dominio (192.168.1.254).
Escape character is '^]'.
220 nombre.dominio ESMTP Sendmail 8.13.1/8.13.1; Sun, 5 Mar 2006 21:45:51 -0600
HELO nombre.dominio
250 nombre.dominio Hello nombre.dominio [192.168.1.254], pleased to meet you
EHLO nombre.dominio
250-nombre.dominio Hello nombre.dominio [192.168.1.254], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
QUIT
221 2.0.0 nombre.dominio closing connection
Connection closed by foreign host.
```

42.6. Pruebas para el envío de correo

42.6.1. Utilizando telnet

Utilizar el mandato **telnet** permite conocer y examinar cómo funciona realmente la interacción entre un servidor de correo y un cliente de correo.

Abra una sesión con **telnet** dirigido hacia el puerto 25 de la dirección IP principal del sistema.

```
telnet 192.168.1.254 25
```

Salude al sistema con el mandato **HELO** seguido del nombre del anfitrión.

```
HELO nombre.dominio
```

El servidor de correo deberá contestarle:

```
250 nombre.dominio Hello nombre.dominio [192.168.1.254], pleased to meet you
```

Ejecute el mandato **MAIL FROM** especificando la cuenta de correo de un usuario local de sus sistema del siguiente modo:

```
MAIL FROM: <fulano@nombre.dominio>
```

El servidor de correo deberá contestarle lo siguiente, a menos que especifique una cuenta de correo con un dominio distinto a los especificados en el fichero **/etc/mail/relay-domains**:

```
250 2.1.0 <fulano@nombre.dominio>... Sender ok
```

Ejecute el mandato **RCPT TO** especificando una cuenta de correo existente en el servidor del siguiente modo:

```
RCPT TO: <root@nombre.dominio>
```

El servidor de correo deberá contestarle lo siguiente:

```
250 2.1.5 <root@nombre.dominio>... Recipient ok
```

Ejecute el mandato **DATA**:

```
DATA
```

El servidor de correo deberá contestarle lo siguiente:

```
354 Enter mail, end with "." on a line by itself
```

Enseguida ingrese el texto que desee incluir en le mensaje de correo electrónico. Al terminar finalice con un punto en una nueva línea.

```
Hola, este es un mensaje de prueba.
.
```

El sistema deberá contestarle algo similar a lo siguiente:

```
250 2.0.0 k263wEKK006209 Message accepted for delivery
```

Ejecute el mandato **QUIT**:

```
QUIT
```

El servidor deberá contestar lo siguiente al terminar la conexión:

```
221 2.0.0 nombre.dominio closing connection
Connection closed by foreign host.
```

La salida completa de todo el procedimiento anterior debe lucir similar a esto (mandatos utilizados resaltados en **negrita**):

```
[fulano@nombre ~]$ telnet 192.168.1.254 25
Trying 192.168.1.254...
Connected to nombre.dominio (192.168.1.254).
Escape character is '^]'.
220 nombre.dominio ESMTP Sendmail 8.13.1/8.13.1; Sun, 5 Mar 2006 21:58:14 -0600
HELO nombre.dominio
250 nombre.dominio Hello nombre.dominio [192.168.1.254], pleased to meet you
MAIL FROM: <fulano@nombre.dominio>
250 2.1.0 <fulano@nombre.dominio>... Sender ok
RCPT TO: <root@nombre.dominio>
250 2.1.5 <root@nombre.dominio>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Hola, este es un mensaje de prueba.
.
250 2.0.0 k263wEKK006209 Message accepted for delivery
QUIT
221 2.0.0 nombre.dominio closing connection
Connection closed by foreign host.
```

42.6.2. Utilizando mutt

Mutt, término utilizado en lengua inglesa para referirse a perros mestizos, es un cliente de correo electrónico (MUA o **M**ail **U**ser **A**gent) para modo texto. Incluye soporte para color, hilos, MIME, PGP/GPG, protocolos POP3, IMAP y NNTP, y para los formatos de correo **Maildir** y **mbox**.

Basta ejecutar mutt y pulsar las teclas indicadas la interfaz de texto para realizar diversas tareas. Para enviar un mensaje de correo electrónico siga este procedimiento:

1. Como usuario sin privilegios, ejecute **mutt**.
2. Responda con la tecla **«s»** para confirmar que se creará **~/Mail**.
3. Una vez iniciada la interfaz de texto de **mutt**, pulse la tecla **«m»** para crear un nuevo mensaje.
4. En la parte inferior de la pantalla aparece un diálogo para el destinatario (**To:**). Ingrese una cuenta de correo electrónico válida o alguna que exista al menos en el dominio de la Red Local (**LAN**).
5. En la parte inferior de la pantalla aparece un diálogo para ingresar el asunto del mensaje (**Subject:**). Ingrese un título para el mensaje.
6. Enseguida mutt iniciará **vi** para crear el texto que se enviará en el mensaje. Inicie el modo de **insertar** texto (**i**) de **vi** e ingrese algunas palabras. Al terminar, guarde y salga de **vi** (**:wq**).
7. Tras terminar con el editor de texto simple **vi**, **mutt** presentará una vista previa del mensaje. Confirme que los datos son los correctos y pulse la tecla **«y»** para enviar el mensaje. Si necesita cambiar alguno de éstos, pulse **«t»** para cambiar el destinatario o **«s»** para cambiar el campo de asunto del mensaje.
8. Mutt le devolverá a la pantalla principal. Si recibe un mensaje de respuesta, seleccione éste y pulse la tecla **ENTER** para visualizar el contenido.
9. Si desea responder el mensaje, pulse la tecla **«r»** y repita los procedimientos del paso 4 al 7.

Si lo desea, también puede utilizar mutt desde la linea de mandatos.

```
echo -e \
"Hola, soy ${USER} en ${HOSTNAME}.\n\
Por favor responde este mensaje.\n\nSaludos." \
| mutt \
-s "Mensaje enviado desde ${HOSTNAME}" \
fulano@maquina.dominio
```

Lo anterior envía un mensaje de correo electrónico hacia la cuenta fulano@maquina.dominio, con el asunto «**Mensaje enviado desde nombre.dominio**» con el siguiente contenido como texto del mensaje:

```
Hola, soy usuario en nombre.dominio
Por favor responde este mensaje.

Saludos.
```

42.7. Referencias

http://www.ietf.org/rfc/rfc2222.txt
http://www.ietf.org/rfc/rfc821.txt
http://www.ietf.org/rfc/rfc2821.txt
http://www.ietf.org/rfc/rfc1939.txt
http://www.ietf.org/rfc/rfc3501.txt

43. Opciones avanzadas de seguridad para Sendmail.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

43.1. Introducción

Debido a la naturaleza del correo electrónico es posible para un atacante inundar fácilmente el servidor y desencadenar en una denegación de servicio. Fenómenos como el denominado correo masivo no solicitado o Spam no hacen las cosas más fáciles y las administración de un servidor de correo puede tornarse una pesadilla. Es por todo esto que añadir opciones avanzadas de seguridad se convierte en algo indispensable.

43.2. Funciones

Todas las funciones explicadas a continuación pueden incluirse en el fichero `/etc/mail/sendmail.mc` justo debajo de la última línea que incluya `define` y arriba de la primera línea que incluya `FEATURE`.

43.2.1. confMAX_RCPTS_PER_MESSAGE

Este parámetro sirve para establecer un número máximo de destinatarios para un mensaje de correo electrónico. De modo predefinido, sendmail establece un máximo de 256 destinatarios. En el siguiente ejemplo se limitará el número de destinatarios a 20:

```
define(`confMAX_RCPTS_PER_MESSAGE', `20')dnl
```

43.2.2. confBAD_RCPT_THROTTLE

Este parámetro sirve para establecer el tiempo de letargo que se utilizará por cada destinatario que sobrepase el límite establecido por `confMAX_RCPTS_PER_MESSAGE`. De modo predefinido Sendmail no establece tiempo de letargo. En el siguiente ejemplo se establecerán 2 segundos de letargo por cada destinatario rechazado por sobrepasar el límite de destinatarios permitidos:

```
define(`confBAD_RCPT_THROTTLE', `2')dnl
```

43.2.3. confPRIVACY_FLAGS

Cuando se establece como valor `goaway', se deshabilitan varios mandatos SMTP como EXPN y VRFY, los cuales pudieran ser utilizados para revelar los nombres de usuarios locales a alguien con pretensiones de enviar spam. También deshabilita las notificaciones de entrega, el cual es un mecanismo comúnmente utilizado por quienes envían spam para verificar la existencia de una cuenta, y hace que el sistema solicite obligatoriamente HELO o EHLO antes de utilizar el mandato

MAIL. Muchos programas son utilizados para enviar correo masivo no solicitado ni siquiera se molestan en utilizar HELO o EHLO. Por defecto los valores de confPRIVACY_FLAGS son `authwarnings,novrfy,noexpn,restrictqrun', cambie por lo siguiente:

```
define(`confPRIVACY_FLAGS',`goaway')dnl
```

43.2.4. confMAX_HEADERS_LENGTH

Esté parámetro se utiliza para definir el tamaño máximo permitido para la cabecera de un mensaje en bytes. Algunos programas utilizados para enviar spam tratan de impedir que los MTA puedan registrar transacciones generando cabeceras muy grandes.

Limitar el tamaño de las cabeceras hace más difícil la ejecución de guión que explote vulnerabilidades recientes (desbordamientos de búfer) en UW IMAP, Outlook y Outlook Express.

La mayor parte de los mensajes de correo electrónico tendrán cabeceras de menos de 2 Kb (2048 bytes). Un mensaje de correo electrónico ordinario, por muy exagerado que resulte el tamaño de la cabecera, rara vez utilizará una cabecera que sobrepase los 5 Kb o 6 Kb, es decir, de 5120 o 6144 bytes. En el siguiente ejemplo se limitará el tamaño máximo de la cabecera de un mensaje a 16 Kb:

```
define(`confMAX_HEADERS_LENGTH', `16384')dnl
```

El valor sugerido es 16 Kb (16384 bytes). Aumente o disminuya el valor a su discresión.

43.2.5. confMAX_MESSAGE_SIZE

Este parámetro sirve para especificar el tamaño máximo permitido para un mensaje de correo electrónico en bytes. Puede especificarse lo que el administrador considera apropiado. En el siguiente ejemplo se limitará el tamaño máximo de un mensaje a 3 MB:

```
define(`confMAX_MESSAGE_SIZE', `3145728')dnl
```

43.2.6. confMAX_DAEMON_CHILDREN

Este parámetro sirve para especificar cuántos procesos hijos se permitirán simultáneamente en el servidor de correo. De modo predefinido sendmail no establece límites para este parámetro. Si se sobrepasa el límite de conexiones simultáneas, el resto serán demoradas hasta que se terminen las conexiones existentes y dejen lugar para nuevas conexiones. En el siguiente ejemplo se limitará el número de conexiones simultáneas hacia el servidor a 5:

```
define(`confMAX_DAEMON_CHILDREN', `5')dnl
```

43.2.7. confCONNECTION_RATE_THROTTLE

Este parámetro sirve para establecer el número de conexiones máximas por segundo. De modo predefinido sendmail no establece límites para este parámetro. En el siguiente ejemplo se limitará a 4 conexiones por segundo:

```
define(`confCONNECTION_RATE_THROTTLE', `4')dnl
```

44. Cómo configurar Sendmail y Dovecot con soporte SSL/TLS.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

44.1. Introducción.

Este documento requiere la lectura y comprensión previa de los siguientes temas:

- Configuración básica de Sendmail.

44.1.1. Acerca de DSA.

DSA (**D**igital **S**ignature **A**lgorithm o Algoritmo de Firma digital) es un algoritmo creado por el NIST (**N**ational **I**nstitute of **S**tandards and **T**echnology o Instituto Nacional de Normas y Tecnología de EE.UU.), publicado el 30 de agosto de 1991, como propuesta para el proceso de firmas digitales. Se utiliza para firmar información, más no para cifrar ésta.

URL: http://es.wikipedia.org/wiki/DSA

44.1.2. Acerca de RSA.

RSA, acrónimo de los apellidos de sus autores, Ron **R**ivest, Adi **S**hamir y Len **A**dleman, es un algoritmo para el cifrado de claves públicas que fue publicado en 1977, patentado en EE.UU. en 1983 por el el Instituto Tecnológico de Michigan (**MIT**). **RSA** es utilizado ampliamente en todo el mundo para los protocolos destinados para el comercio electrónico.

URL: http://es.wikipedia.org/wiki/RSA

44.1.3. Acerca de X.509.

X.509 es un estándar **ITU-T** (estandarización de **T**elecomunicaciones de la **I**nternational **T**elecommunication **U**nion) para infraestructura de claves públicas (**PKI**, o **P**ublic **K**ey **I**nfrastructure). Entre otras cosas, establece los estándares para certificados de claves públicas y un algoritmo para validación de ruta de certificación. Este último se encarga de verificar que la ruta de un certificado sea válida bajo una infraestructura de clave pública determinada. Es decir, desde el certificado inicial, pasando por certificados intermedios, hasta el certificado de confianza emitido por una Autoridad Certificadora (**CA**, o **C**ertification **A**uthority).

URL: http://es.wikipedia.org/wiki/X.509

44.1.4. Acerca de OpenSSL.

OpenSSL es una implementación libre, de código abierto, de los protocolos **SSL** (**S**ecure **S**ockets **L**ayer o Nivel de Zócalo Seguro) y **TLS** (**T**ransport **L**ayer **S**ecurity, o Seguridad para Nivel de Transporte). Está basado sobre el extinto proyecto **SSLeay**, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation.

URL: http://www.openssl.org/

44.2. Procedimientos.

Acceda al sistema como el usuario **root**.

Se debe crear el directorio donde se almacenarán los certificados para todos los sitios SSL. El directorio, **por motivos de seguridad**, debe ser solamente accesible para el usuario **root**.

```
mkdir -m 0700 /etc/ssl
```

A fin de mantener cierta organización, es conveniente crear un directorio específico para almacenar el certificado del servidor. Igualmente, **por motivos de seguridad**, debe ser solamente accesible para el usuario **root**.

```
mkdir -m 0700 /etc/ssl/midominio.org
```

Acceder al directorio que se acaba de crear.

```
cd /etc/ssl/midominio.org
```

44.2.1. Sendmail.

44.2.1.1. Generando clave y certificado.

Sendmail requiere una llave creada con algoritmo **DSA** de 1024 octetos. Para tal fin, se crea primero un fichero de parámetros **DSA**:

```
openssl dsaparam 1024 -out dsa1024.pem
```

A continuación, se utiliza este fichero de parámetros **DSA** para crear una llave con algoritmo **DSA** y estructura **x509**, así como también el correspondiente certificado. En el ejemplo a continuación, se establece una validez por 730 días (dos años) para el certificado creado.

```
openssl req -x509 -nodes -newkey dsa:dsa1024.pem \
-days 730 -out sendmail.crt -keyout sendmail.key
```

Lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.

- Nombre de la empresa o razón social.
- Unidad o sección.
- Nombre del anfitrión.
- Dirección de correo.

La salida devuelta sería similar a la siguiente:

```
Generating a 1024 bit DSA private key
writing new private key to 'sendmail.key'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:Mexico
Organization Name (eg, company) [My Company Ltd]:
Mi empresa, S.A. de C.V.
Organizational Unit Name (eg, section) []:Direccion Comercial
Common Name (eg, your name or your server's hostname) []:
midominio.org
Email Address []:webmaster@midominio.org
```

El certificado solo será válido cuando el servidor de correo electrónico sea invocado con el nombre definido en el campo **Common Name**. Es decir, solo podrá utilizarlo cuando se defina **midominio.org** como servidor **SMTP** con soporte **TLS**. No funcionará si se invoca al servidor como, por mencionar un ejemplo, **mail.midominio.org**.

Al terminar, ya no será necesario conservar el fichero **dsa1024.pem**, mismo que puede eliminarse con plena seguridad.

```
rm -f dsa1024.pem
```

Es indispensable que todos los ficheros de claves y certificados tengan permisos de acceso de solo lectura para el usuario **root**:

```
chmod 400 /etc/ssl/midominio.org/sendmail.*
```

44.2.1.2. Parámetros de /etc/mail/sendmail.mc.

Es necesario configurar los siguiente parámetros en el fichero

/etc/mail/sendmail.mc a fin de que Sendmail utilice la clave y certificado recién creados:

```
define(`confCACERT_PATH',`/etc/ssl/midominio.org')
define(`confCACERT',`/etc/ssl/midominio.org/sendmail.crt')
define(`confSERVER_CERT',`/etc/ssl/midominio.org/sendmail.crt')
```

```
define(`confSERVER_KEY',`/etc/ssl/midominio.org/sendmail.key')
```

Solo resta activar el puerto que será utilizado para SMTPS (465 por TCP).

```
DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl
```

El acceso cifrado con TLS es opcional si se realizan conexiones a través del puerto 25, y obligatorio si se hacen a través del puerto 465. El puerto 587 (submission), puede ser también utilizado para envío de correo electrónico. Por estándar se utiliza como puerto alternativo en los casos donde un cortafuegos impide a los usuarios acceder hacia servidores de correo trabajando por puerto 25. MS Outlook Express no tiene soporte para usar TLS a través del puerto 587, pero el resto de los clientes de correo electrónico con soporte TLS si.

```
DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio sendmail.

```
service sendmail restart
```

44.2.1.3. Comprobación.

Realice una conexión con **telnet** al puerto 25 del sistema. Ingrese el mandato **EHLO**. La salida deberá devolver, entre todas las funciones del servidor, una línea que indica **STARTTLS**. La salida puede ser similar a la siguiente:

```
telnet 127.0.0.1 25
EHLO midominio.org

Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 midominio.org ESMTP Sendmail 8.13.1/8.13.1; Mon, 2 Oct 2006 13:18:02 -0500
ehlo midominio.org
250-midominio.org Hello localhost.localdomain [127.0.0.1], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH LOGIN PLAIN
250-STARTTLS
250-DELIVERBY
250 HELP
```

Al realizar la configuración del cliente de correo electrónico, deberá especificarse conexión por TLS. Tras aceptar el certificado, deberá ser posible autenticar, con nombre de usuario y clave de acceso, y enviar correo electrónico.

44.2.2. Dovecot.

44.2.2.1. Generando clave y certificado.

La creación de la llave y certificado para **Dovecot** es más simple, pero requiere utilizar una clave con algoritmo **RSA** de 1024 octetos, con estructura **X.509**. En el ejemplo a continuación, se establece una validez por 730 días (dos años) para el certificado creado.

```
openssl req -x509 -nodes -newkey rsa:1024 \
-days 730 -out dovecot.crt -keyout dovecot.key
```

De forma similar a como ocurrió con **Sendmail**, lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o razón social.
- Unidad o sección.
- Nombre del anfitrión.
- Dirección de correo.

La salida devuelta sería similar a la siguiente:

```
Generating a 1024 bit RSA private key
................++++++
.++++++
writing new private key to 'dovecot.key'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:Mexico
Organization Name (eg, company) [My Company Ltd]:
Mi empresa, S.A. de C.V.
Organizational Unit Name (eg, section) []:Direccion Comercial
Common Name (eg, your name or your server's hostname) []:
midominio.org
Email Address []:webmaster@midominio.org
```

El certificado solo será válido cuando el servidor de correo electrónico sea invocado con el nombre definido en el campo **Common Name**. Es decir, solo podrá utilizarlo cuando se defina **midominio.org** como servidor **POP3** o **IMAP** con soporte **TLS**. No funcionará si se invoca al servidor como, por mencionar un ejemplo, **mail.midominio.org**.

Es indispensable que todos los ficheros de claves y certificados tengan permisos de acceso de solo lectura para el usuario **root**:

```
chmod 400 /etc/ssl/midominio.org/dovecot.*
```

44.2.2.2. Parámetros de /etc/dovecot.conf.

En el parámetro **protocols**, se activan todos los servicios (imap, imaps, pop3 y pop3s).

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

De modo predeterminado, el soporte SSL de **Dovecot** está activo. Verifique que el parámetro **ssl_disable** tenga el valor **no**, o bien solo esté comentado.

```
#ssl_disable = no
```

Y se especifican las rutas del certificado y clave a través de los parámetros **ssl_cert_file** y **ssl_key_file**, del siguiente modo:

```
ssl_cert_file = /etc/ssl/midominio.org/dovecot.crt
ssl_key_file = /etc/ssl/midominio.org/dovecot.key
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **dovecot**.

```
service dovecot restart
```

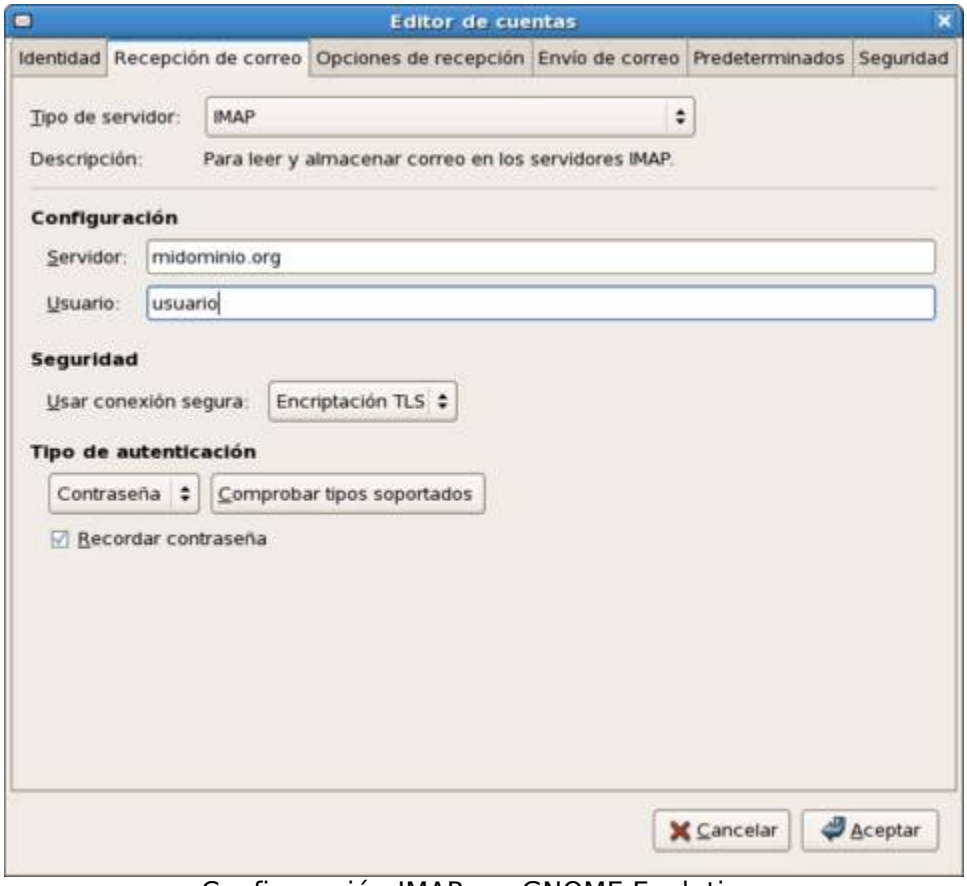
44.2.2.3. Comprobación.

Utilice cualquier cliente de correo electrónico con soporte para TLS y configure éste para conectarse hacia el sistema a través de **IMAPS** (puerto 993) o bien **POP3S** (puerto 995). Tras aceptar el certificado del servidor, el sistema deberá permitir autenticar, con nombre de usuario y clave de acceso, y realizar la lectura del correo electrónico.

44.2.3. Configuración de GNOME Evolution.

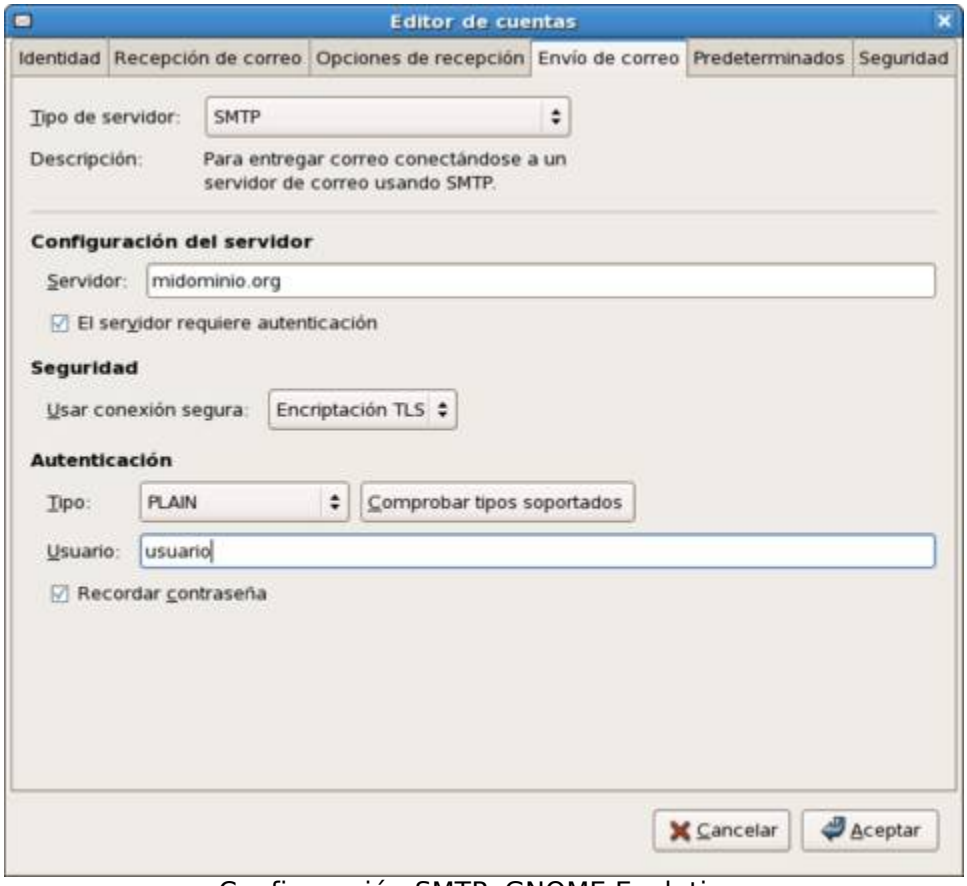
44.2.3.1. Configuración GNOME Evolution.

Para GNOME Evolution, la configuración de IMAP o POP3 se realiza selecionando el tipo de servidor, definiendo el nombre del servidor utilizado para crear el certificado, nombre de usuario, y usar encriptación segura TLS.



Configuración IMAP, en GNOME Evolution.

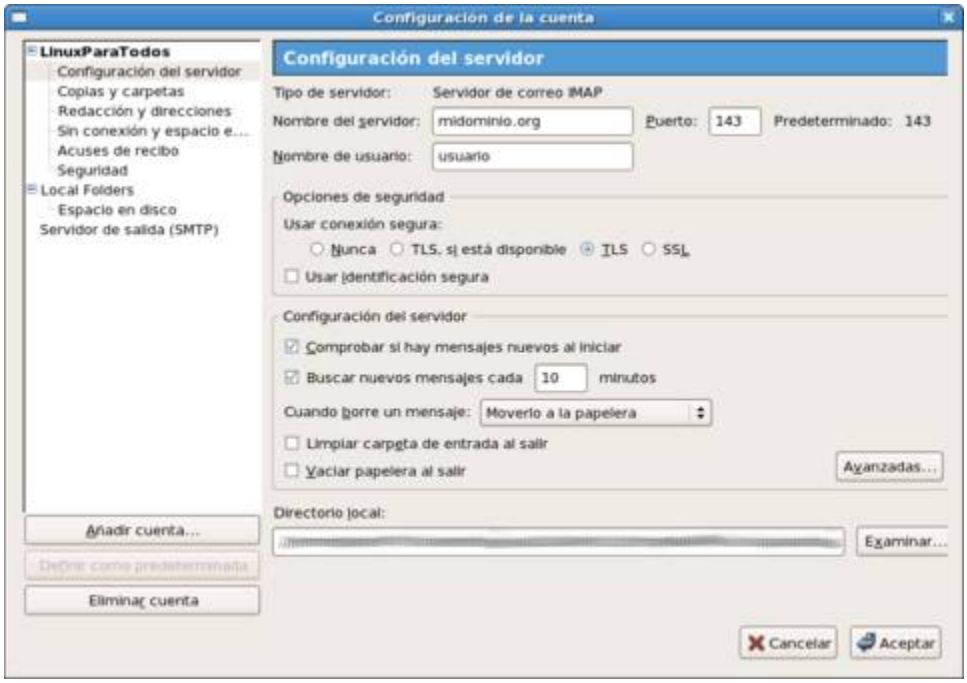
Se hace lo mismo para SMTP.



Configuración SMTP, GNOME Evolution.

44.2.3.2. Configuración Mozilla Thunderbird.

Para Mozilla Thunderbird, se define el nombre del servidor utilizado para crear el certificado, usuario y usar conexión segura TLS.



Configuración IMAP, Mozilla Thunderbird.

Se hace lo mismo para SMTP.

Configuración SMTP, Mozilla Thunderbird.

44.2.4. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir, además de los puertos 25, 110, 143 y 587 por TCP (**SMTP**, **POP3**, **IMAP** y **Submission**, respectivamente), los puertos 465, 993 y 995 por TCP (**SMTPS**, **IMAP** y **POP3S**, respectivamente).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     25,110,143,465,587,993,995
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

45. Cómo configurar Cyrus IMAP.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

45.1. Introducción.

Proyecto que dio inicio en 1994, en la **Universidad Carnegie Mellon**, el servidor **Cyrus IMAP** se distingue del resto de los equipamientos lógicos con la misma finalidad en que utiliza un formato para los buzones de correo que mejora el rendimiento y escalabilidad del formato **Maildir**, utilizado por otros equipamientos lógicos como **Dovecot**. Este formato almacena los datos por partes del sistema de archivos y que solo pueden ser accedidos por el servicio de **Cyrus IMAP**. Esto permite gestionar grandes cantidades de datos de forma eficiente y con un intérprete de mandatos para su administración. Incluye soporte para los protocolos **IMAP**, **IMAP**, **POP3** y **POP3S**, así como soporte para listas de control de acceso y cuotas en la jerarquía de buzones.

URL: http://asg.web.cmu.edu/cyrus/imapd/

45.2. Equipamiento lógico necesario.

- **cirus-imapd**: servidor **IMAP**, **IMAP**, **POP3** y **POP3S**.
- **cyrus-imapd-utils**: herramientas de administración.
- **cyrus-sasl**: servicio de autenticación.
- **cyrus-sasl-plain**: soporte para autenticación a través de texto simple.
- **cyrus-sasl-md5**: soporte para autenticación a través de métoos cifrados.

45.2.1. Instalación a través de yum.

Si utiliza **CentOS 4** o **White Box Enterprise Linux 4**, y versiones posteriores, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install cyrus-imapd cyrus-imapd-utils cyrus-sasl cyrus-sasl-plain cyrus-sasl-md5
```

45.2.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date -i cyrus-imapd cyrus-imapd-utils cyrus-sasl cyrus-sasl-plain cyrus-sasl-md5
```

45.3. Procedimientos.

Cyrus IMAP no requiere modificar fichero alguno de configuración. Los valores predeterminados

permiten su funcionamiento normal. Sin embargo, requiere de algunos procedimientos adicionales en relación a otros equipamientos lógicos.

Se debe asignar una clave de acceso para el usuario administrador de **Cyrus IMAP**, a fin de impedir accesos no autorizados al intérprete de mandatos para administración. Esto se realiza a través del mandato **passwd**, del siguiente modo:

```
passwd cyrus
```

45.3.1. Alta de cuentas de usuario y asignación de claves de acceso.

El alta de usuarios a través de este método será diferente a la manera tradicional, debido a que para utilizar el método de autenticación para acceder hacia los servicios **IMAP**, **IMAPS**, **POP3** y **POP3S**, **Cyrus IMAP** utilizará **SASL**. Por tal motivo, el alta de cuentas de usuario de correo deberá de seguir el siguiente procedimiento:

1. Alta de la cuenta del usuario en el sistema, la cual se sugiere no deberá tener acceso a intérprete de mandato alguno:
   ```
   useradd -s /sbin/nologin fulano
   ```
2. Asignación de claves de acceso en el sistema para permitir autenticar a través de los métodos **PLAIN** y **LOGIN** para autenticar a través de los protocolos **POP3** e **IMAP**:
   ```
   passwd usuario
   ```
3. Asignación de claves de acceso para autenticar **IMAP**, **IMAPS**, **POP3** y **POP3S** a través de métodos cifrados (**CRAM-MD5** y **DIGEST-MD5**) en sistemas con versión de **Cyrus IMAP** compilada contra **SASL-2** (Red Hat™ Enterprise Linux 4, CentOS 4 o White Box Enterprise Linux 4), requieren utilizar el mandato **saslpasswd2** del siguiente modo:
   ```
   saslpasswd2 usuario
   ```
4. Acceder hacia el intérprete de mandatos para administración de **Cyrus IMAPD**, **cyradm**, del siguiente modo:
   ```
   cyradm -user cyrus -auth login localhost
   ```
5. Crear los buzones de correo para el usuario a través del intérprete de mandatos para administración de **Cyrus IMAPD**, **cyradm**, del siguiente modo:
   ```
   createmailbox user.usuario
   ```

   Para mostrar la lista de buzones existentes, se utiliza el mandato **listmailbox**. Para salir del intérprete, solo se ingresa el mandato **exit**
6. La autenticación para **IMAP**, **IMAPS**, **POP3** y **POP3S** a través de cualquier mecanismo requiere se active e inicie el servicio de **saslauthd** del siguiente modo:
   ```
   chkconfig saslauthd on
   service saslauthd start
   ```

En el caso en que se haya decidido utilizar métodos cifrados (**CRAM-MD5** y **DIGEST-MD5**), puede mostrarse la lista de los usuarios con clave de acceso a través de SASL-2 utilizando el mandato **sasldblistusers2**. Puede mostrarse la lista de los usuarios con clave de acceso a través de SASL-1 utilizando el mandato **sasldblistusers**. Si ya se cuenta con un grupo de claves de acceso de

usuarios dados de alta en SASL-1, se pueden convertir hacia SASL-2 con el mandato **dbconverter-2**.

45.3.2. Iniciar, detener y reiniciar el servicio cyrus-imapd.

Para iniciar por primera vez el servicio **cyrus-imapd**, utilice:

```
/sbin/service cyrus-imapd start
```

Para hacer que los cambios hechos a la configuración del servicio **cyrus-imapd** surtan efecto, utilice:

```
/sbin/service cyrus-imapd restart
```

Para detener el servicio **cyrus-imapd**, utilice:

```
/sbin/service cyrus-imapd stop
```

45.3.3. Agregar el servicio cyrus-imapd al arranque del sistema.

Para hacer que el servicio de **cyrus-imapd** esté activo con el siguiente inicio del sistema, en todos los niveles de corrida (2, 3, 4, y 5), se utiliza lo siguiente:

```
/sbin/chkconfig cyrus-imapd on
```

45.3.4. Integración con Sendmail.

Para hacer que el correo que llega a través de **Sendmail** sea almacenado en su totalidad en los buzones de **Cyrus IMAP** a través de **LMTP** (**L**ocal **M**ail **T**ransfer **P**rotocol o Protocolo de trasferencia de correo local, descrito en el RFC 2033), es necesario descomentar/agregar las siguientes líneas de configuración en el fichero **/etc/mail/sendmail.mc**, justo antes de **DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl**.

```
define(`confLOCAL_MAILER', `cyrusv2')dnl
define(`CYRUSV2_MAILER_ARGS', `FILE /var/lib/imap/socket/lmtp')dnl
```

Y descomentar/agregar la siguiente línea al final del fichero **/etc/mail/sendmail.mc**, justo debajo de **MAILER(procmail)dnl**.

```
MAILER(cyrusv2)dnl
```

Tras realizado lo anterior, solo se necesita reiniciar el servicio **sendmail**.

```
service sendmail restart
```

45.4. Comprobaciones.

Envíe un mensaje de correo electrónico utilizando el mandato **mail** y establezca una conexión entre el cliente y el servidor a través de **POP3**, como se ejemplificada a continuación.

```
Cliente:  $ telnet 127.0.0.1 110
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^]'.
          +OK localhost.localdomain Cyrus POP3 v2.2.12-Invoca-RPM-2.2.12-3.RHEL4.1 server ready.
Cliente:  USER fulano
Servidor: +OK
Cliente:  PASS clave de accceso
Servidor: +OK Logged in.
Cliente:  STAT
Servidor: +OK 1 728
Cliente:  LIST
Servidor: +OK 1 messages:
          1 728
          .
Cliente:  RETR 1
Servidor: +OK 728 octets
          Return-Path: <fulano@localhost.localdomain>
          Received: from localhost.localdomain (localhost.localdomain [192.168.1.254])
                   by localhost.localdomain (8.13.1/8.13.1) with SMTP id k2IM2RjA003987
                   for <root@localhost.localdomain>; Sat, 18 Mar 2006 16:03:21 -0600
          Date: Sat, 18 Mar 2006 16:02:27 -0600
          Message-Id: <200603182203.k2IM2RjA003987@localhost.localdomain>
          Subject: Mensaje de prueba
          From: fulano@localhost.localdomain
          To: root@localhost.localdomain
          Status: O
          Content-Length: 43
          Lines: 2
          X-UID: 202
          X-Keywords:

          Hola. Este es un mensaje de prueba.
          Adios.
          .
Cliente:  QUIT
Servidor: +OK Logging out.
          Connection closed by foreign host.
```

Repita el procedimiento, esta vez estableciendo conexión entre el cliente y el servidor a través de **IMAP**, como se ejemplificada a continuación.

```
Cliente:  $ telnet 127.0.0.1 143
Servidor: Trying 127.0.0.1...
          Connected to localhost.localdomain (127.0.0.1).
          Escape character is '^]'.
          * OK localhost.localdomain Cyrus IMAP4 v2.2.12-Invoca-RPM-2.2.12-3.RHEL4.1 server ready.
          +OK dovecot ready.
Cliente:  x LOGIN fulano clave de acceso
Servidor: x OK Logged in.
Cliente:  x SELECT inbox
Servidor: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
          * OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
          * 1 EXISTS
          * 0 RECENT
          * OK [UNSEEN 1] First unseen.
          * OK [UIDVALIDITY 1100569382] UIDs valid
          * OK [UIDNEXT 203] Predicted next UID
          x OK [READ-WRITE] Select completed.
Cliente:  x FETCH 1 (flags body[header.fields (subject)])
Servidor: * 1 FETCH (FLAGS (\Seen) BODY[HEADER.FIELDS (SUBJECT)] {30}
          Subject: Mensaje de prueba

          )
          x OK Fetch completed.
          .
Cliente:  x FETCH 1 (body[text])
Servidor: * 1 FETCH (BODY[TEXT] {45}
          Hola. Este es un mensaje de prueba.
          Adios.
          )
```

```
x OK Fetch completed.
Cliente: x LOGOUT
Servidor: * BYE Logging out
x OK Logout completed.
Connection closed by foreign host.
```

46. Instalación y configuración de SquirrelmMail (correo a través de interfaz HTTP)

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

46.1. Introducción

SquirrelMail es un interesante, extensible, funcional y robusto sustento lógico para correo y que permite acceder al usuario a su correo electrónico desde el navegador de su predilección.

SquirrelMail está escrito en PHP4 y cumple con los estándares como correo a través de interfaz HTTP. Incluye su propio soporte para los protocolos IMAP y SMTP. Además todas las páginas se muestran con HTML 4.0 sin la necesidad de JavaScript para una máxima compatibilidad con cualquier navegador.

SquirrelMail incluye toda la funcionalidad deseada para un cliente de correo como un robusto soporte MIME, libreta de direcciones y administración de carpetas.

46.2. Procedimientos

46.2.1. Instalación del sustento lógico necesario

```
yum -y install squirrelmail httpd
```

46.2.2. Configuración de SquirrelMail.

Cambie al directorio **/usr/share/squirrelmail/config/** y ejecute el guión de configuración que se encuentra en el interior:

```
cd /usr/share/squirrelmail/config/
./conf.pl
```

Lo anterior le devolverá una interfaz de texto muy simple de utilizar, como la mostrada a continuación:

```
SquirrelMail Configuration : Read: config.php (1.4.3)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books (LDAP)
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database


D.  Set pre-defined settings for specific IMAP servers

C.  Turn color on
S   Save data
Q   Quit

Command >>
```

Ingrese hacia las preferencias de la organización y defina el nombre de la empresa, el logotipo y sus dimensiones, El mensaje en la barra de título de la ventana del navegador, el idioma a utilizar, URL y el título de la página principal del servidor de red.

```
SquirrelMail Configuration : Read: config.php (1.4.3)
---------------------------------------------------------
Organization Preferences
1.  Organization Name      : Razón_Social_de_su_empresa
2.  Organization Logo      : ../images/sm_logo.png
3.  Org. Logo Width/Height : (308/111)
4.  Organization Title     : Bienvenido al Webmail de
Su_empresa.
5.  Signout Page           :
6.  Default Language       : es_ES
7.  Top Frame              : _top
8.  Provider link          : http://url_de_su_empresa/
9.  Provider name          : Nombre_de_su_emrpesa

R   Return to Main Menu
C.  Turn color on
S   Save data
Q   Quit
Command >>
```

En las opciones de servidores defina solamente el dominio a utilizar. Si el servidor de correo va a coexistir en el mismo sistema con el servidor HTTP, no hará falta modificar más en esta sección. Si lo desea, puede especificar otro servidor SMTP e IMAP localizados en otro equipo.

```
SquirrelMail Configuration : Read: config.php (1.4.3)
---------------------------------------------------------
Server Settings

General
-------
1.  Domain                 : su-máquina.su-dominio
2.  Invert Time            : false
3.  Sendmail or SMTP       : Sendmail

A.  Update IMAP Settings   : localhost:143 (uw)
B.  Change Sendmail Config : /usr/sbin/sendmail

R   Return to Main Menu
C.  Turn color on
S   Save data
Q   Quit

Command >>
```

En las opciones de las carpetas cambie Trash por Papelera, Sent por Enviados y Drafts por Borradores.

```
SquirrelMail Configuration : Read: config.php (1.4.3)
---------------------------------------------------------
Folder Defaults
1.  Default Folder Prefix         : mail/
2.  Show Folder Prefix Option     : true
3.  Trash Folder                  : Papelera
4.  Sent Folder                   : Enviados
5.  Drafts Folder                 : Borradores
6.  By default, move to trash     : true
7.  By default, move to sent      : true
8.  By default, save as draft     : true
9.  List Special Folders First    : true
10. Show Special Folders Color    : true
11. Auto Expunge                  : true
12. Default Sub. of INBOX         : true
13. Show 'Contain Sub.' Option    : false
14. Default Unseen Notify         : 2
15. Default Unseen Type           : 1
16. Auto Create Special Folders   : true
17. Folder Delete Bypasses Trash  : false
18. Enable /NoSelect folder fix   : false

R   Return to Main Menu
C.  Turn color on
S   Save data
Q   Quit

Command >>
```

Finalmente escoja y habilite las extensiones (plug-ins) que considere apropiados para sus necesidades:

```
SquirrelMail Configuration : Read: config.php (1.4.3)
---------------------------------------------------------
Plugins
  Installed Plugins
    1. delete_move_next
    2. squirrelspell
    3. newmail
    4. calendar
    5. filters
    6. mail_fetch
    7. translate
    8. abook_take
    9. message_details
    10. sent_subfolders

  Available Plugins:
    11. administrator
    12. bug_report
    13. info
    14. listcommands
    15. spamcop
    16. fortune

R   Return to Main Menu
C.  Turn color on
S   Save data
Q   Quit

Command >>
```

Guarde los cambios pulsando la tecla «S» y luego la tecla «Enter».

46.3. Finalizando configuración

Active, si no lo ha hecho aún, el servicio de IMAP. Si utiliza Red Hat™ Enterprise Linux 4, CentOS 4.0 o White Box Enterprise Linux 4. El paquete imap es reemplazado por dovecot, el cual funciona como otros servicios. Se debe modificar el fichero **/etc/dovecot.conf** y asegurarse que estén habilitados los servicios de imap (de modo predefinido sólo debe estar habilitado imap):

```
protocols = imap pop3
```

El servicio se agrega al arranque del sistema y se inicializa del siguiente modo:

```
chkconfig dovecot on
service dovecot start
```

Si utiliza Red Hat™ Enterprise Linux 3, CentOS 3.0 o White Box Enterprise Linux 3, el procedimiento utilizará el paquete imap, el cual sólo requiere un simple mandato para activar el servicio.

```
chkconfig imap on
```

Reinicie o inicie el servicio de apache:

```
service httpd start
```

Acceda con el navegador de su predilección hacia **http://127.0.0.1/webmail/**.

```
elinks http://127.0.0.1/webmail/
```

46.4. Ajustes en php.ini para optimizar el uso de Squirrelmail

A continuación algunos ajustes útiles para el fichero **/etc/php.ini** que pueden resolver algunos problemas comunes al utilizar Squirrelmail.

Un servidor de red combinado con servicio de correo y otras aplicaciones utiliza muchos recursos de sistema, y si se están ejecutando además varias aplicaciones PHP simultáneamente, es normal que se tengan problemas al exceder el límite de memoria para la ejecución de un guión.

Habrá que aumentar el RAM en algunos servidores en particular si modifica los límites actuales. Por defecto PHP sólo utilice 8 MB para la ejecución de guiones PHP:

```
memory_limit = 8M
post_max_size = 8M
```

Se pueden cambiar esos valores en el fichero **/etc/php.ini** por unos ligeramente mayores **(¡Por favor, NO ABUSAR!).** Utilice 9 o 10 MB.

```
memory_limit = 10M
post_max_size = 10M
```

Consultar http://www.squirrelmail.org/wiki/en_US/LowMemoryProblem para mayores detalles al respecto. Hay otro parámetro que seguramente algunos van a cuestionar a cuestionar: por defecto PHP que sólo permite subir un máximo de 2 MB. Por ende, Squirrelmail sólo permitirá subir no más de 2 MB en los adjuntos. Basta con modificar el fichero **/etc/php.ini** y cambiar:

```
upload_max_filesize = 2M
```

Por algo como:

```
upload_max_filesize = 4M
```

Adicionalmente **post_max_size** define el tamaño máximo para una publicación. Si se quiere subir objetos grandes, debe definirse con un valor ligeramente mayor que **upload_max_file**. El valor por defecto es 8M y puede ser más que suficiente, aunque 10 MB puede ser algo apropiado.

```
post_max_size = 10M
```

Más detalles en http://www.squirrelmail.org/wiki/en_US/AttachmentSize.

Respecto a las imágenes incluidas en los mensajes, desde las preferencias para cada cuenta en Squirrelmail se configuran las opciones para activarlas y poderlas ver. Si las imágenes **no están incluidas** en el mismo mensaje y se vinculan desde sitios externos, por defecto no se cargan **POR MOTIVOS SEGURIDAD**. Cargar una imagen externa puede servir a un spammer para confirmar

que alguien a ha leído su mensaje desde una cuenta activa o bien puede hacer que el usuario acceda hacia y ejecute código malicioso. Consultar http://www.squirrelmail.org/wiki/en_US/UnsafeImages antes de ingresar el complemento que permite ver imágenes inseguras: http://www.squirrelmail.org/plugin_view.php?id=98.

47. Apéndice: Enviar correo a todos los usuarios del sistema

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

47.1. Procedimientos

1. Lo primero será generar un fichero en el sistema, el cual tendrá como contenido una lista de los usuarios del sistema a los que se quiere enviar un mensaje. Éste puede localizarse en cualquier lugar del sistema, como por ejemplo /`etc/mail/allusers`. Puede editarse el fichero `/etc/mail/allusers` y añadir individualmente cada usuario que se desee conforme esa lista o bien, si se quiere añadir a todos los usuarios del sistema, ejecutar lo siguiente:

```
awk -F: '$3 > 500 { print $1 }' /etc/passwd > /etc/mail/allusers
```

2. A continuación, debe modificarse el fichero `/etc/aliases` y añadir al final del mismo:

```
allusers: :include:/etc/mail/allusers
```

1. Al terminar sólo debe ejecutarse el mandato `newaliases` o bien reiniciar el servicio de Sendmail (el guión de inicio se encarga de hacer todo lo necesario).

3. Para probar, bastará con enviar un mensaje de correo electrónico a la cuenta `allusers` del servidor.

47.2. Acerca de la seguridad

Evite a toda costa utilizar **allusers** o palabras muy obvias como alias de correo para enviar a todas las cuentas. Seguramente quienes se dedican a enviar correo masivo no solicitado o correo chatarra (*Spam*), tratarán de enviar correo a este alias en el servidor. No les facilite el trabajo a esas personas y trate de utilizar un alias ofuscado o en clave. Ejemplo: *8jj37sjei876*.

48. Configuración de MailScanner y ClamAV con Sendmail

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

48.1. Introducción.

48.1.1. Acerca de MailScanner.

MailScanner, un robusto servicio que se encarga de examinar el correo electrónico e identificar y etiquetar correo masivo no solicitado (**Spam**), así como también los fraudes electrónicos (**Phishing**). Combinado con ClamAV, un poderoso y versátil anti-virus libre para GNU/Linux y otros sabores de Unix, resultan una de las soluciones más robustas para la protección contra correo masivo no solicitado, fraudes electrónicos, virus, gusanos y troyanos desde el servidor de correo electrónico.

MailScanner tiene las siguiente características:

- Distribuido bajo los términos de la Licencia Publica General GNU versión 2.
- Revisa el correo electrónico en busca de virus utilizando cualquier combinación de entre más de una docena de distintos programas anti-virus.
- Automáticamente actualiza todo los anti-virus instalados cada hora.
- Identifica alrededor del 95% del correo masivo no solicitado (Spam) utilizando diferentes técnicas, incluyendo altamente avanzadas técnicas de heurística (capacidad de un sistema para realizar de forma inmediata innovaciones positivas para sus fines).
- El correo identificado como peligroso puede ser etiquetado, rechazado, descartado, archivado o reenviado hacia otras direcciones para su inspección por los administradores.
- Puede eliminar el contenido gráfico de correo masivo no solicitado (Spam) de tipo pornográfico protegiendo a los usuarios de contenido obsceno.
- Verifica el coreo electrónico en busca de conocidas vulnerabilidades para las más populares aplicaciones de correo electrónico y corrige automáticamente los mensajes durante el proceso cuando sea posible poniendo en cuarentena las secciones peligrosas de contenidas en los mensajes.
- Es altamente escalable. Un servidor puede procesar más de millón y medio de mensajes de correo por día.
- Es robusto. Se protege a si mismo contra ataques de Denegación de Servicio (**DoS**) y fuga de recursos del sistema operativo.
- Es altamente configurable, proporciona a los Proveedores de Servicios de Internet (**ISP** o **I**nternet **S**ervice **P**rovider y Proveedores de Servicios de

Aplicaciones (**ASP** o **A**pplication **S**ervice **P**rovider) la posibilidad de utilizar miles de diferentes reglas y configuraciones para cualquier combinación de usuarios y dominios.

- Es fácil de instalar y configurar puesto que sus opciones predefinidas permiten trabajar al servicio de correo sin complicaciones.

URL: http://www.mailscanner.info/.

48.1.2. Acerca de ClamAV.

ClamAV tiene las siguiente características:

- Distribuido bajo los términos de la Licencia Publica General GNU versión 2.
- Cumple con las especificaciones de familia de estándares **POSIX** (**P**ortable **O**perating **S**ystem **I**nterface for UNI**X** o interfaz portable de sistema operativo para Unix).
- Exploración rápida.
- Detecta más de 44 mil virus, gusanos y troyanos, incluyendo virus para MS Office.
- Capacidad para examinar contenido de ficheros ZIP, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM y MS SZDD.
- Soporte para explorar ficheros comprimidos con UPX, FSG y Petite.
- Avanzada herramienta de actualización con soporte para firmas digitales y consultas basadas sobre DNS.

URL: http://www.clamav.net/

48.1.3. Acerca de SpamAssassin.

SpamAssassin es un sustento lógico que utiliza un sistema de puntuación, basado sobre algoritmos de tipo genético, para identificar mensajes que pudieran ser sospechosos de ser correo masivo no solicitado, añadiendo cabeceras a los mensajes de modo que pueda ser filtrados por el cliente de correo electrónico o MUA (**M**ail **U**ser **A**gent).

URL: http://spamassassin.apache.org/

48.2. Procedimientos.

48.2.1. Equipamiento lógico necesario.

- mailscanner >= 4.50
- perl-Convert-BinHex
- perl-IO-stringy
- perl-Compress-Zlib
- tnef
- clamav >= 0.88
- perl-MailTools
- perl-TimeDate
- perl-Convert-ASN1
- spamAssassin >= 3.0.4
- perl-MIME-tools
- perl-Net-CIDR
- perl-Archive-Zip

Si dispone de un sistema con Red Hat™ Enterprise Linux 4, CentOS 4 o White Box Enterprise Linux 4, puede utilizar el siguiente depósito yum:

```
[mailscanner-lpt]
```

```
name=MailScanner Alcance Libre para Enterprise Linux 4
baseurl=http://www.linuxparatodos.net/lpt/whitebox/4.0/mailscanner/
gpgkey=http://www.linuxparatodos.net/lpt/LPT-RPM-KEY
```

Una vez configurado lo anterior, solo bastará utilizar:

```
yum -y install mailscanner clamav
```

Lo anterior instalará mailscanner y clamav junto con todas las dependencias que seas necesarias.

También podrá instalar MailScanner descargando la más reciente versión desde http://www.mailscanner.info/ en donde encontrará un paquete *.tar.gz en cuyo interior hay paquetes SRPM que podrá compilar e instalar en el orden indicado siguiendo las instrucciones del fichero README. De igual modo podrá proceder con clamav desde http://clamav.net/

48.2.2. Configuración de MailScanner.

Utilice el editor de texto de su predilección y disponga a modificar **/etc/MailScanner/MailScanner.conf** con la finalidad de configurar los siguiente parámetros:

48.2.2.1. Lenguaje de los mensajes de sistema.

Puede configurar MailScanner para que devuelva los mensajes de sistema en español. Localice lo siguiente:

```
%report-dir% = /etc/MailScanner/reports/en
```

Cambie por:

```
%report-dir% = /etc/MailScanner/reports/es
```

48.2.2.2. Identificación de la organización.

Solo es de carácter informativo y sirve para identificar si un mensaje infectado pertenece a un servidor u otro. Localice lo siguiente:

```
%org-name% = yoursite
```

Cambie por:

```
%org-name% = empresa
```

El parámetro **%org-long-name%** es utilizado para definir que mostrar en la firma localizada al final de los reportes enviados por MailScanner. Puede incluir cuanto texto sea necesario, e incluso definir varias líneas utilizando secuencias \n.

```
%org-long-name% = Empresa Imaginaria S.A. de C.V.
```

El parámetro **%web-site%** se utiliza para definir el URL de la empresa, mismo que también se incluye en la firma al final de los reportes que envía MailScannmer. Se recomienda se utilice una

URL hacia un documento que explique el porque se han rechazado/filtrado mensajes o bien información de contacto.

```
%web-site% = http://www.empresa-imaginaria.com.mx/info-correo.html
```

48.2.2.3. Adjuntos en formato de texto enriquecido.

Algunas versiones de Microsoft Outlook generan adjuntos en formato de Texto Enriquecido (**R**ich **T**ext **F**ormat) que no pueden ser examinados. El valor predefinido es **no** ya que de otro modo habría un alto riesgo de permitir la entrada de virus a través de este tipo de mensajes. Sin embargo muchos usuarios de Outlook pueden protestar al respecto por carecer una enfoque apropiado acerca de la seguridad. ¿Realmente vale la pena el riesgo? Si los usuarios están de acuerdo en que recibir un mensaje con colores y letras bonitos es más importante que la seguridad, puede cambiarse el valor a **yes**.

```
Deliver Unparsable TNEF = no
```

Adicionalmente puede, aunque no se recomienda, cambiar el valor de **deny** por **allow**en la línea de configuración correspondiente para adjuntos con extensión ***.dat** en el fichero **/etc/MailScanner/filename.rules.conf**. En este fichero se define lo que se quiera denegar si los mensajes incluyen ciertos tipos de ficheros adjuntos **que se consideran de alto riesgo**. El formato de este fichero consiste en definir una regla (que puede ser **allow**, **deny** o **deny+delete**), una expresión regular a filtrar, texto a incluir en la bitácora del sistema y el texto a utilizar en el reporte para el usuario, todo separado por tabuladores y en una sola línea por cada regla.

```
deny     winmail\.dat$     Windows security vulnerability     No Outlook Rich Text Format
messages due to security hole, use HTML instead
```

Lo anterior rechaza los mensajes que incluyan adjuntos *.dat, es decir mensajes de Outlook en Formato de Texto Enriquecido (Outlook **R**ich **T**ext **F**ormat), devolviendo un mensaje de error en inglés que diría: *«No Outlook **R**ich **T**ext **F**ormat messages due to security hole, use HTML instead»*. Se puede poner el mensaje al español:

```
deny     winmail\.dat$     Windows security vulnerability     No aceptamos mensajes en
Formato de Texto Enriquecido de Outlook, por favor utilice HTML.
```

Lo anterior rechaza los mensajes que incluyan adjuntos *.dat, es decir mensajes de Outlook en Formato de Texto Enriquecido (Outlook **R**ich **T**ext **F**ormat), devolviendo un mensaje de error en inglés que diría: *«No aceptamos mensajes en Formato de Texto Enriquecido de Outlook, por favor utilice HTML.»*.

48.2.2.4. Definir anti-virus a utilizar.

MailScanner puede detectar automáticamente los anti-virus a utilizar dejando el valor **auto** en el parámetro **Virus Scanners**, de modo que detectará cualquiera de los siguientes:

- Sophos.
- Bitdefender.
- eTrust.
- Nod32.
- Panda.
- ClamAV.
- Css.
- Mcafee.
- DRweb.
- Inoculate.
- F-Secure.
- Rav.
- Trend.
- AVG.
- Command.
- Kaspersky.
- Inoculan.
- F-Prot.
- Antivir.
- Norman.
- Vexira.

Para agilizar el inicio de MailScanner se pueden definir los anti-virus necesarios. **ClamAV** es el anti-virus recomendado por tratarse de un sustento lógico libre.

Localice lo siguiente en el fichero **/etc/MailScanner/MailScanner.conf**:

```
Virus Scanners = none
```

Cambie por:

```
Virus Scanners = clamav
```

Puede utilizar más de un anti-virus si así lo considera conveniente. Solo necesitará instalar las versiones apropiadas para el sistema operativo que utilice y añadirlos en MailScanner como lista horizontal separada por espacios. Ejemplo:

```
Virus Scanners = clamav mcafee sophos trend
```

48.2.2.5. ¿Poner en cuarentena los mensajes infectados o no?

Si decide no poner en cuarentena los elementos adjuntos infectados en los mensajes de correo electrónico y prefiere **eliminar estos adjuntos inmediatamente** después de ser procesados, localice lo siguiente:

```
Quarantine Infections = yes
```

Cambie por:

```
Quarantine Infections = no
```

48.2.2.6. Permitir mensajes con etiqueta *Iframe*, *Form* y *Script*.

Las etiquetas **iframe** se utilizan para cargar una página empotrada dentro de un marco. Lamentablemente esto representa un riesgo muy alto e innecesario debido a que un mensaje de correo electrónico podría no contener material dañino, pero tal vez el la página que cargue el marco que si lo contenga. Actualmente se considera el enviar correo electrónico utilizando etiquetas **iframe** como poco ético por todos los riesgos que conlleva.

Las opciones permitidas son:

- **yes**: Permite la etiqueta en el mensaje.
- **no**: elimina los mensajes que contengan la etiqueta.
- **disarm**: Permite las etiquetas pero impide que éstas funcionen.

El valor predeterminado es **disarm**.

```
Allow IFrame Tags = disarm
```

Lo mismo aplica para las etiquetas **form**, que pueden permitir la recolección de datos desde el mensaje de correo electrónico con ayuda de la ingenuidad del usuario, o bien la ejecución de código peligroso a través de guiones escritos en **JavaScript** a través de la etiqueta **script**.

```
Allow Form Tags = disarm
Allow Script Tags = disarm
```

48.2.3. Control de Spam.

De modo predefinido está activo el soporte de exploración de correo en búsqueda de correo masivo no solicitado (Spam).

```
Spam Checks = yes
```

Quienes se dedican al envío de correo masivo no solicitado han aprendido que pueden hacer que su mensaje pase los filtros enviando un mensaje con muchos destinatarios, uno de los cuales podría tener configurado tener todo en lista blanca en las opciones de SpamAssassin en el directorio de inicio del usuario. De este modo, si un mensaje llega con más de un número determinado de destinatarios (20 de modo predefinido), éste se será tratado como cualquier otro mensaje sin aún si el destinatario ha decidido poner todo en lista blanca o si el remitente está en la lista blanca en el fichero **/etc/MailScanner/rules/spam.whitelist.rules**.

```
Ignore Spam Whitelist If Recipients Exceed = 20
```

48.2.3.1. A través de DNSBL o listas negras.

MailScanner permite también realizar filtrado de correo contra listas negras como **SpamCop** y **Spamhaus**. **Si ya utiliza los DNSBL o listas negras desde Sendmail, no active esta funcionalidad en MailScanner para no duplicar las consultas hacia los DNSBL**.

Modifique el fichero **/etc/MailScanner/spam.lists.conf** y defina o confirme las listas negras a utilizar

```
ORDB-RBL relays.ordb.org.
#
# spamhaus.org sbl.spamhaus.org.
# spamhaus-XBL xbl.spamhaus.org.
# combinación de las dos anteriores:
SBL+XBL sbl-xbl.spamhaus.org.
#
spamcop.net bl.spamcop.net.
NJABL dnsbl.njabl.org.
SORBS dnsbl.sorbs.net.
```

Localice en el fichero **/etc/MailScanner/MailScanner.conf** lo siguiente:

```
Spam List = ORDB-RBL SBL+XBL # MAPS-RBL+ costs money (except .ac.uk)
```

Cambie por:

```
Spam List = ORDB-RBL SBL+XBL spamcop.net NJABL SORBS
```

48.2.3.2. A través de SpamAssassin.

MailScanner puede echar mano de SpamAssassin para una más eficiente detección de correo masivo no solicitado. Puede activarse o desactivarse esta funcionalidad a través del parámetro **Use**

SpamAssassin asignando **yes** o **no**.

```
Use SpamAssassin = yes
```

SpamAssassin utiliza un sistema de calificación para etiquetar o no como correo masivo no solicitado. Se asigna un valor numérico a partir de 1 (valor recomendado es 6), con o sin decimales, para el parámetro **Required SpamAssassin Score**. Cada vez que se identifica en un mensaje contiene alguna característica que pudiera clasificarlo como correo masivo no solicitado, se asignan fracciones de punto que se van sumando. Cuando un mensaje rebasa el valor asignado para **Required SpamAssassin Score** éste es etiquetado de inmediato como correo masivo no solicitado.

```
Required SpamAssassin Score = 6
```

Puede especificarse también a través del parámetro **High SpamAssassin Score** que los mensajes que rebasen la puntuación establecido como valor de este se eliminen directamente en lugar de solo etiquetarlos como correo masivo no solicitado. El valor prefinido (y recomendado) es 10.

```
High SpamAssassin Score = 10
```

El parámetro **Spam Actions** define que política a aplicar para el correo electrónico que se clasifica como Spam, calificado a partir del valor definido en **Required SpamAssassin Score**, pero inferior al valor definido a **High SpamAssassin Score**. El parámetro **High Scoring Spam Actions** se utiliza para definir la política a aplicar para el correo electrónico que se clasifica como Spam, calificado a partir del valor definido en **High SpamAssassin Score**. Pueden utilizarse combinaciones de los siguientes valores:

deliver	Entrega del mensaje de modo normal.
delete	Eliminar el Mensaje.
bounce	Envía un masaje de rechazo al remitente. Este valor solo puede utilizarse con el parámetro **Spam Actions**, no puede utilizarse con el parámetro **High Scoring Spam Actions**.
store	Almacenar el mensaje en el directorio de cuarentena.
forward usuario@dominio.com	Reenviar copia del mensaje a usuario@dominio.com
striphtml	Convierte el contenido HTML a texto simple. Se requiere especificar el valor **deliver** para que tenga efecto.
attachment	Convierte el mensaje a adjunto, de modo que el usuario tendrá que realizar un paso adicional para mirar el contenido.
notify	Se envía una breve notificación al usuario que le indica que no le fue entregado un mensaje por haber sido clasificado como correo masivo no solicitado, permitiendo solicitar recuperar el mensaje si acaso éste fuese un mensaje esperado.
header "nombre: valor"	Añade la cabecera con cualquier nombre (sin

	espacios) con el valor especificado.

Suponiendo se aplicarán las siguientes políticas:

• Si el mensaje es calificado al menos el valor definido en **Required SpamAssassin Score**, pero inferior al valor definido en **High SpamAssassin Score**, se **entregará** al usuario como **mensaje adjunto** y añadirá la cabecera **"X-Spam-Status: Yes"**.
• Si el mensaje es calificado al menos con el valor definido en **High SpamAssassin Score**, se **eliminará** automáticamente.

Los valores para **Required SpamAssassin Score** y **High SpamAssassin Score** coresponderían del siguiente modo:

```
Spam Actions = deliver attachment header "X-Spam-Status: Yes"
High Scoring Spam Actions = delete
```

48.2.3.3. Listas Blancas.

Pueden especificarse listas blancas de direcciones o nombres de dominio que no se desee etiqueten como correo masivo no solicitado (Spam) en el fichero **/etc/MailScanner/rules/spam.whitelist.rules** del siguiente modo, donde **yes** signficará que el correo proveniente de dichas direcciones nunca se etiquetará como correo masivo no solicitado (Spam):

```
# This is where you can build a Spam WhiteList
# Addresses matching in here, with the value
# "yes" will never be marked as spam.
#From:          152.78.         yes
#From:          130.246.        yes
FromOrTo:       default         no
From:           200.76.185.250  yes
From:           192.168.0.      yes
```

En el ejemplo anterior, todo el correo proveniente de 200.76.185.250 y cualquier dirección IP de la red 192.168.0.0/24 quedará exento de etiquetarse como correo masivo no solicitado (Spam).

48.2.4. Configuración de servicios.

Necesitará inicializar los servicios **clamd** y **freshclam**. El segundo, particularmente, se encarga de contactar los servidores que hospedan las bases de datos actualizadas con las más recientes firmas de los más recientes virus, gusanos, troyanos y otros tipos de sustento lógico maligno.

```
chkconfig clamd on
chkconfig freshclam on
service clamd start
service freshclam start
```

De ser necesario puede actualizar manualmente y de manera inmediata la base de datos de firmas ejecutando simplemente freshclam desde cualquier terminal como **root**.

Se debe desactivar y detener el servicio de sendmail, el cual será controlado en adelante por el servicio MailScanner:

```
chkconfig sendmail off
chkconfig MailScanner on
service sendmail stop
service MailScanner start
```

48.3. Comprobaciones.

Utilice cualquier cliente de correo electrónico y envíe éste como adjunto hacia una cuenta de correo loca el fichero **test2.zip**, incluido en el directorio de MailScanner del **disco de extras de curso** de Alcance Libre. El procedimiento deberá entregar el mensaje al destinatario con el título alterado indicando que el mensaje contenía un virus y en el interior un texto que indica que el adjunto fue removido y eliminado.

Si quiere hacer una prueba rápida, utilice **mutt** para enviar un mensaje de prueba ejecutando lo siguiente, suponiendo que hay un usuario denominado como «fulano» en el sistema:

```
echo "Prueba Anti-virus" | mutt -a test2.zip -s "Prueba Anti-virus" fulano
```

Lo anterior deberá devolver al destinatario el siguiente mensaje de correo electrónico:

```
Asunto:  Prueba Anti-virus
De: "Fulano" <fulano@localhost.localdomain >
Fecha: Mie, 18 de Agosto de 2004, 10:31 pm
Para: "Fulano" <fulano@localhost.localdomain >
Atención: Este mensaje contenía uno o más anexos
que han sido eliminados
Atención: (test2.zip, clamtest).
Atención: Por favor, lea el(los) anexo(s) "empresa-Attachment-Warning.txt"
para más información.
Prueba Anti-virus
```

El administrador del servidor de correo recibirá en cambio lo siguiente:

```
Asunto: Virus Detected
De: "MailScanner" <postmaster@localhost.localdomain>
Fecha: Mie, 18 de Agosto de 2004, 10:31 pm
Para: postmaster@localhost.localdomain

The following e-mails were found to have:Virus Detected
Sender: root@localhost.localdomain
IP Address: 127.0.0.1
 Recipient: fulano@localhost.localdomain
 Subject: Prueba Anti-virus
 MessageID: i7J3VTXF004487
 Informe: ClamAV: clamtest contains ClamAV-Test-Signature
 Informe: ClamAV: test2.zip contains ClamAV-Test-Signature
 ClamAV: clamtest contains ClamAV-Test-Signature --
MailScanner
Email Virus Scanner
www.mailscanner.info
```

Si todos los procedimientos de comprobación por algún motivo no funcionan, por favor verifique la sintaxis en todas las líneas modificadas en el fichero **/etc/MailScanner/MailScanner.conf**, como seguramente podrá leer se indica en la bitácora localizada en el fichero **/var/log/maillog**.y que

también puede mostrar información de utilidad.

```
tail -f /var/log/maillog
```

48.4. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es importante que MailScanner pueda realizar conexiones hacia el exterior hacia los siguientes servicios:

- **SMTP**, puerto 25 a través de TCP (entrada y salida).
- **DNS**, puerto 53 a través de TCP y UDP (salida).
- **Razor23**, puerto 2703 a través de TCP y puerto 7 a través de UDP (salida).
- **DCC**, puerto 6277 a través de UDP (salida).
- **Pyzor**, puerto 24441 a través de UDP (salida).

ClamAV necesita además poder realizar conexiones hacia **HTTP** (puerto 80) en el exterior para sincronizar la base de datos de firmas.

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a esto:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)
ACCEPT  fw      net     tcp     25,53,80,2703
ACCEPT  fw      net     udp     7,53,6277,24441
ACCEPT  net     fw      tcp     25
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

49. Cómo configurar clamav-milter.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

49.1. Introducción.

49.1.1. Acerca de clamav-milter.

Clamav-milter es un componente para añadir (**Plug-in**) para la biblioteca de filtros de correo (**libmilter**) de **Sendmail**, que se encarga de hacer pasar todo el correo entrante, incluyendo todo lo que se reciba a través de **rmail/UUCP**, a través del **ClamAV**, que a su vez es un poderoso y robusto motor, con licenciamiento libre, para la detección de gusanos, troyanos y virus. Verifica el correo electrónico durante la conexión con el servidor de correo que remite éste ultimo, y lo rechaza automáticamente si éste incluye algún gusanos, troyanos o virus.

Al igual que clamav-milter, el cual es utilizado para la filtración de Spam, representa una excelente alternativa pues tiene un bajo consumo de recursos de sistema, haciéndolo idóneo para servidores con sustento físico obsoleto, o donde otras aplicaciones tiene mayor prioridad en la utilización de recursos de sistema.

URL: http://www.clamav.net/

49.1.2. Acerca de ClamAV.

ClamAV tiene las siguiente características:

- Distribuido bajo los términos de la Licencia Publica General GNU versión 2.
- Cumple con las especificaciones de familia de estándares **POSIX** (**P**ortable **O**perating **S**ystem **I**nterface for UNI**X** o interfaz portable de sistema operativo para Unix).
- Exploración rápida.
- Detecta más de 44 mil virus, gusanos y troyanos, incluyendo virus para MS Office.
- Capacidad para examinar contenido de ficheros ZIP, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM y MS SZDD.
- Soporte para explorar ficheros comprimidos con UPX, FSG y Petite.
- Avanzada herramienta de actualización con soporte para firmas digitales y consultas basadas sobre DNS.

URL: http://www.clamav.net/

49.2. Equipamiento lógico necesario.

- sendmail (previamente configurado)
- make
- clamav
- sendmail-cf
- m4
- clamav-milter

49.2.1. Instalación a través de yum.

Si dispone de un servidor con **CentOS 4**, **Red Hat™ Enterprise Linux 4** o **White Box Enterprise Linux 4**, puede utilizar el el depósito yum de **Alcance Libre** para servidores en producción:

```
[alcance-libre]
name=Alcance Libre para Enterprise Linux 4
baseurl=http://www.alcancelibre.org/al/el/4/
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

Si dispone de un servidor con **CentOS 5**, **Red Hat™ Enterprise Linux 5** o **White Box Enterprise Linux 5**, puede utilizar el el depósito yum de **Alcance Libre** para servidores en producción:

```
[alcance-libre]
name=Alcance Libre para Enterprise Linux 5
baseurl=http://www.alcancelibre.org/al/el/5/
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

La instalación solo requiere utilizar lo siguiente:

```
yum -y install clamav-milter clamav-milter-sysv clamav-data-empty clamav-update
```

49.3. Procedimientos.

49.3.1. Requisitos previos.

Se requiere un servidor de correo con **Sendmail**, previamente configurado y funcionando para enviar y recibir correo electrónico. Para más detalles al respecto, consultar el documento titulado *«Configuración básica de Sendmail (Parte I).»*.

49.3.2. Fichero /etc/mail/sendmail.mc.

Es necesario agregar el siguiente contenido en el fichero **/etc/mail/sendmail.mc**, justo arriba de **MAILER(smtp)dnl**.

```
INPUT_MAIL_FILTER(`clamav',        `S=local:/var/run/clamav-milter/clamav.sock,        F=,
T=S:4m;R:4m')dnl
define(`confINPUT_MAIL_FILTERS', `clamav')dnl
```

Si se combina con **Spamassassin Milter**, quedaría del siguiente modo:

```
INPUT_MAIL_FILTER(`clamav',        `S=local:/var/run/clamav-milter/clamav.sock,        F=,
T=S:4m;R:4m')dnl
INPUT_MAIL_FILTER(`spamassassin',     `S=unix:/var/run/spamass-milter/spamass-milter.sock,
F=, T=C:15m;S:4m;R:4m;E:10m')dnl
define(`confMILTER_MACROS_CONNECT',`t, b, j, _, {daemon_name}, {if_name}, {if_addr}')dnl
```

```
define(`confMILTER_MACROS_HELO',`s,      {tls_version},      {cipher},      {cipher_bits},
{cert_subject}, {cert_issuer}')dnl
define(`confINPUT_MAIL_FILTERS', `spamassassin,clamav')dnl
```

49.3.3. Configuración.

Clamav-milter depende totalmente de la base de datos de **ClamAV**. No requiere parámetros para modificar para el funcionamiento estándar, que consiste en rechazar correo electrónico. Las banderas de inicio para clamav-milter están definidas en el fichero **/etc/sysconfig/clamav-milter**, mismo que no requiere modificarse, a menos que se necesite especificar alguna opción avanzada definida en la página de manual de clamav-milter.

```
man clamav-milter
```

49.3.4. Iniciar, detener y reiniciar el servicio clamav-milter.

Se agrega al arranque del sistema y se inicia el servicio **clamav-milter** del siguiente modo:

```
chkconfig clamav-milter on
service clamav-milter start
```

A fin de mantener actualizada la base de datos de firmas digitales, es necesario editar el fichero **/etc/sysconfig/freshclam** y comentar la línea que desactiva la actualización automática a través del servicio **crond**:

```
### !!!!! REMOVE ME !!!!!!
### REMOVE ME: By default, the freshclam update is disabled to avoid
### REMOVE ME: network access without prior activation
# FRESHCLAM_DELAY=disabled-warn # REMOVE ME
```

De ser necesario, puede actualizar manualmente, y de manera inmediata, la base de datos de firmas utilizando el mandato **freshclam**, desde cualquier terminal como **root**.

Al terminar, considerando que está instalado el paquete **sendmail-mc**, el cual permite reconfigurar **Sendmail** a partir del fichero **/etc/mail/sendmail.mc**, se debe reiniciar el servicio **sendmail** para que surtan efectos los cambios.

```
service sendmail restart
```

50. Cómo configurar spamass-milter.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

50.1. Introducción.

50.1.1. Acerca de spamass-milter.

Spamass-milter es un componente adicional (**Plug-in**) para la biblioteca de filtros de correo (**libmilter**) de **Sendmail**, que se encarga de hacer pasar todo el correo entrante, incluyendo todo lo que se reciba a través de **rmail/UUCP**, a través de **SpamAssassin**, que a su vez es un poderoso y robusto componente de filtrado de correo.

Representa una excelente alternativa pues tiene un bajo consumo de recursos de sistema, haciéndolo idóneo para servidores con sustento físico obsoleto, o donde otras aplicaciones tiene mayor prioridad en la utilización de recursos de sistema.

URL: http://savannah.nongnu.org/projects/spamass-milt/

50.1.2. Acerca de SpamAssassin.

SpamAssassin es un equipamiento lógico que utiliza un sistema de puntuación, basado sobre algoritmos de tipo genético, para identificar mensajes que pudieran ser sospechosos de ser correo masivo no solicitado, añadiendo cabeceras a los mensajes de modo que pueda ser filtrados por el cliente de correo electrónico o **MUA** (**M**ail **U**ser **A**gent).

URL: http://spamassassin.apache.org/

50.2. Equipamiento lógico necesario.

- sendmail (previamente configurado)
- make
- spamassassin
- sendmail-cf
- m4
- spamass-milter

50.2.1. Instalación a través de yum.

Si dispone de un servidor con **CentOS 4**, **Red Hat™ Enterprise Linux 4** o **White Box Enterprise Linux 4**, puede utilizar el el depósito yum de **Alcance Libre** para servidores en producción:

```
[alcance-libre]
name=Alcance Libre para Enterprise Linux 4
baseurl=http://www.alcancelibre.org/al/el/4/
```

```
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

La instalación solo requiere utilizar lo siguiente:

```
yum -y install spamass-milter
```

50.3. Procedimientos.

50.3.1. Requisitos previos.

Se requiere un servidor de correo con **Sendmail**, previamente configurado y funcionando para enviar y recibir correo electrónico. Para más detalles al respecto, consultar el documento titulado *«Configuración básica de Sendmail (Parte I).»*.

50.3.2. Fichero /etc/mail/sendmail.mc.

Es necesario agregar el siguiente contenido en el fichero **/etc/mail/sendmail.mc**, justo arriba de **MAILER(smtp)dnl**.

```
INPUT_MAIL_FILTER(`spamassassin',     `S=unix:/var/run/spamass-milter/spamass-milter.sock,
F=, T=C:15m;S:4m;R:4m;E:10m')dnl
define(`confMILTER_MACROS_CONNECT',`t, b, j, _, , , ')dnl
define(`confMILTER_MACROS_HELO',`s, , , , , ')dnl
```

50.3.3. Configuración.

Spamass-milter depende totalmente de **SpamAssassin**. por lo que toda la configuración de se hace a través de éste último, configurando y añadiendo parámetros y valores en el fichero **/etc/mail/spamassassin/local.cf**, donde, entre muchos otros, se pueden establecer los siguientes parámetros:

required_hits	Se utiliza para establecer la cantidad de puntos acumulados, y asignados por **SpamAssassin**, en un mensaje para considerar el éste como Spam. El valor predeterminado es **5**, acepta decimales y se puede ajustar con un valor inferior o mayor de acuerdo al criterio del administrador. Ejemplo: 4.5
report_safe	Determina si el mensaje, si es calificado como spam, se incluye en un adjunto, con el valor 1, o se deja el mensaje tal y como está, con el valor 0. El valor predeterminado es **0**.
rewrite_header	Define con que cadena de caracteres se añadirá al mensaje para identificarlo como Spam. El valor predeterminado es **[SPAM]**, y puede cambiarse por lo que considere apropiado el administrador. Ejemplo:
whitelist_from	Se utiliza para definir que jamás se considere como Spam los mensajes de correo electrónico cuyo remitente sea un dominio o cuenta de correo electrónico en particular. Se pueden definir varias líneas. Ejemplo: whitelist_from *@midominio.algo whitelist_from *@alcancelibre.org whitelist_from *@hsbc.com.mx whitelist_from *@bancomer.com.mx whitelist_from *@banamex.com

whitelist_to	Si utiliza una lista de correo electrónico (**majordomo** o **mailman**), y se desea evitar que accidentalmente se considere Spam un mensaje de correo electrónico emitido por una de estas listas, se puede definir que nunca se considere Spam el correo emitido por dicha lista. Ejemplo: whitelist_to mailman-users@algo.algo
blacklist_from	Se puede definir que todo el correo electrónico proveniente de un dominio o cuenta de correo electrónico en particular siempre sea considerado como Spam. Ejemplo: blacklist_from alguien@spammer.com
ok_languages	Permite definir los códigos de los países cuyos lenguajes no serán considerados Spam. En el ejemplo a continuación, se establece que los idiomas español y portugués no se considerará como Spam: ok_languages pt es

Hay una herramienta de configuración de SpamAssassin, que permite generar el fichero **/etc/mail/spanassassin/local.cf**, en http://www.yrex.com/spam/spamconfig.php.

50.3.4. Fichero /etc/sysconfig/spamass-milter.

El fichero **/etc/sysconfig/spamassassin** incluye el siguiente contenido:

```
### Override for your different local config
#SOCKET=/var/run/spamass-milter/spamass-milter.sock

### Standard parameters for spamass-milter are:
### -P /var/run/spamass-milter.pid (PID file)
###
### Note that the -f parameter for running the milter in the background
### is not required because the milter runs in a wrapper script that
### backgrounds itself
###
### You may add another parameters here, see spamass-milter(1)
#EXTRA_FLAGS="-m -r 15"
```

De forma predeterminada, a través del parámetro **-m**, **spmass-milter** desactiva la modificación de el asunto del mensaje (**Subject:**) y la cabecera **Content-Type:**, lo cual es conveniente para añadir cabeceras y se procesado posteriormente, y, a través del parámetro **-r 15**, rechaza los mensajes de correo electrónico cuando éstos tienen asignados 15 puntos o más. Se pueden modificar el número de puntos mínimos para rechazar directamente el correo electrónico sospechoso de ser spam incremenatando el valor para el parámetro **-r**. La recomendación es asignar un valor mayor al definido en el fichero **/etc/mail/spamassassin/local.cf**. Si, por ejemplo, se establece en éste último **required_hits 4.5** y **rewrite_header Subject** y en el fichero **/etc/sysconfig/spamass-milter** se establece **EXTRA_FLAGS="-m -r 6"**, ocurrirá lo siguiente:

1. Todos los mensajes maracdos con 4.4 puntos o menos, se entregarán inmediatamente al usuario sin modificaciones visibles.

2. Todos los mensajes marcados desde 4.5 hasta 5.9 puntos se entregarán al usuario con el asunto modificado añadiendo a éste al inicio.

3. Todos los mensajes que estén marcados con 6.0 puntos o más serán rechazados automáticamente.

Basado sobre el ejemplo mencionado, el contenido del fichero **/etc/sysconfig/spamass-milter** quedaría del siguiente modo:

```
### Override for your different local config
#SOCKET=/var/run/spamass-milter/spamass-milter.sock

### Standard parameters for spamass-milter are:
### -P /var/run/spamass-milter.pid (PID file)
###
### Note that the -f parameter for running the milter in the background
### is not required because the milter runs in a wrapper script that
### backgrounds itself
###
### You may add another parameters here, see spamass-milter(1)
EXTRA_FLAGS="-m -r 6"
```

50.3.5. Fichero /etc/sysconfig/spamassassin.

A fin de que **spamass-milter** y **spamasssin** trabajen juntos, es necesario crear un directorio virtual de configuración para el usuario **sa-milt** que se utilizará para iniciar **spamd**, el cual corresponde al servicio **spamassassin**.

```
mkdir /var/lib/spamassassin
```

Este directorio debe pertenecer al usuario **sa-milt** y grupo **sa-milt**.

```
chown sa-milt.sa-milt /var/lib/spamassassin
```

Se edita el fichero **/etc/sysconfig/spamassassin**, y se añaden las opciones **-u sa-milt -x --virtual-config-dir=/var/lib/spamassassin**, las cuales especifican que se iniciará como el usuario **sa-milt**, que se deactivará la configuración por usuario y que se utilizará **/var/lib/spamassassin** como directorio virtual de configuración. De tal modo, el fichero debe quedar de la siguiente forma:

```
# Options to spamd
SPAMDOPTIONS="-d -c -m5 -H -u sa-milt -x --virtual-config-dir=/var/lib/spamassassin"
```

50.3.6. Iniciar, detener y reiniciar el servicio spamass-milter.

Se agrega al arranque del sistema y se inicia el servicio **spamassasin** del siguiente modo:

```
chkconfig spamassassin on
service spamassassin start
```

El servicio **spamass-milter** se agrega al arranque del sistema y se inicia del siguiente modo:

```
chkconfig spamass-milter on
service spamass-milter start
```

Al terminar, considerando que está instalado el paquete **sendmail-mc**, el cual permite reconfigurar **Sendmail** a partir del fichero **/etc/mail/sendmail.mc**, se debe reiniciar el servicio **sendmail** para que surtan efectos los cambios realizado en el fichero mencionado.

```
service sendmail restart
```

51. Cómo configurar un servidor NIS

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

51.1. Introducción.

Anteriormente conocido como **Sun Yellow Pages** (**YP** o Páginas Amarillas), **NIS** (**N**etwork **I**nformation **S**ervice o Sistema de Información de Red) es un protocolo para servicio de directorios cliente/servidor para la distribución de datos, como pueden ser nombres de usuarios, claves de acceso, directorios de usuario y nombres de anfitriones, utilizados por sistemas comunicados en una red. Originalmente fue desarrollado por **Sun Microsystems** y está está basado sobre **ONC RPC**. Consta de un servidor, una biblioteca para los clientes y herramientas de administración. Actualmente NIS está incluido como implementación libre en todas las distribuciones de Linux y variantes de Unix, e incluso existen implementaciones libres.

51.2. Procedimientos.

Este documento considera las siguientes variables que deberán ser reemplazadas por valores reales:

- dominio.net: sustituya por el dominio que se desee configurar.
- servidor.dominio.net: sustituya por el nombre de anfitrión del servidor NIS.
- 192.168.0.254: Dirección IP del servidor NIS
- 192.168.0.0: Dirección de red
- 255.255.255.0: Máscara de subred.

Instalación del equipamiento lógico necesario en el servidor NIS.

51.2.1.1. Instalación a través de yum.

Si utiliza **CentOS 4 y 5**, **White Box Enterprise Linux 4 y 5** o **Red Hat Enterprise Linux 5**, y versiones posteriores, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install ypbind yp-tools ypserv
```

51.2.1.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date -i install ypbind yp-tools ypserv
```

51.2.2. Configuración del servidor NIS.

51.2.2.1. Configuración del fichero /etc/yp.conf

Edite el fichero /etc/yp.conf:

```
vi /etc/yp.conf
```

Añada la siguiente línea:

```
domain dominio.net server 192.168.0.254
```

51.2.2.2. Configuración del fichero /etc/ypserv.conf

Edite el fichero /etc/ypserv.conf

```
vi /etc/ypserv.conf
```

Añada o verifique que esté presente el siguiente contenido:

```
dns: no
files: 30
xfr_check_port: yes
* : * : shadow.byname : port
* : * : passwd.adjunct.byname : port
```

51.2.2.3. Configuración del fichero /etc/sysconfig/network

Edite el fichero /etc/sysconfig/network

```
vi /etc/sysconfig/network
```

Añada el siguiente contenido:

```
NISDOMAIN="dominio.net"
```

Para integrarse al dominio recién configurado, es necesario utilizar los siguiente mandatos.

```
domainname dominio.net
ypdomainname dominio.net
```

51.2.2.4. Creación y contenido del fichero /var/yp/securenets.

Edite el fichero /var/yp/securenets:

```
vi /var/yp/securenets
```

Definir la dirección IP del retorno del sistema y la máscara de subred y dirección IP de red correspondiente a la red con la que se está trabajando. El el ejemplo a continuación, se está utilizando una red **192.168.0.0** con máscara de subred **255.255.255.0** (24 bits):

```
host 127.0.0.1
255.255.255.0 192.168.0.0
```

51.2.2.5. Inicio y reinicio de servicios portmap y ypserv.

El servicio de **portmap** se debe reiniciar para reconozca al servicio **ypserv** recién instalado.

```
service portmap restart
```

El servicio **ypserv** es iniciado (o reiniciado si ya estuviera ejecutándose) y agregado al arranque del sistema.

```
service ypserv start
chkconfig ypserv on
```

Para hacer comprobar que el servicio está funcionado **ypserv** correctamente, utilice:

```
rpcinfo -u localhost ypserv
```

Lo anterior debe devolver una salida similar a la siguiente:

```
el programa 100004 versión 1 está listo y a la espera
el programa 100004 versión 2 está listo y a la espera
```

51.2.2.6. Creación de mapas NIS.

Deben crearse los mapas NIS donde se almacenará la información del servicio.

```
/usr/lib/yp/ypinit -m
```

Lo anterior deberá devolver una salida similar a lo siguiente, donde solo deberá agregarse el nombre de anfitrión del sistema:

```
At this point, we have to construct a list of the hosts which will run NIS
servers. servidor00.cch-naucalpan.mx is in the list of NIS server hosts. Please continue to
add
the names for the other hosts, one per line. When you are done with the
list, type a <control D>.
 next host to add: locahost.localdomain
 next host to add:
```

El el último campo ingrese el nombre de anfitrión del sistema y pulse CTRL-D al terminar:

```
At this point, we have to construct a list of the hosts which will run NIS
servers. servidor00.cch-naucalpan.mx is in the list of NIS server hosts. Please continue to
add
the names for the other hosts, one per line. When you are done with the
list, type a <control D>.
 next host to add: localhost.localdomain
 next host to add: servidor.dominio.net
```

51.2.2.7. Arranque de servicios ypbind, yppasswdd y ypxffrd

Inicie los servicios ypbind, yppasswdd y ypxffrd.

```
service ypbind start
service yppasswdd start
service ypxfrd start
```

Añada éstos servicios al arranque del sistema

```
chkconfig ypbind on
chkconfig yppasswdd on
chkconfig ypxfrd on
```

51.2.3. Instalación del equipamiento lógico necesario en el cliente NIS.

51.2.3.1. Instalación a través de yum.

Si utiliza **CentOS 4 y 5**, **White Box Enterprise Linux 4 y 5** o **Red Hat Enterprise Linux 5**, y versiones posteriores, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install ypbind yp-tools
```

51.2.3.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date -i install ypbind yp-tools
```

51.2.4. Configuración del cliente NIS.

51.2.4.1. Configuración de ficheros /etc/sysconfig/network, /etc/yp.conf y /etc/hosts.

Edite el fichero /etc/sysconfig/network:

```
vi /etc/sysconfig/network
```

Añada la siguiente línea:

```
NISDOMAIN=internal
```

Edite el fichero /etc/yp.conf:

```
vi /etc/yp.conf
```

Considerando que el dominio a utilizar es **dominio.net** y que la dirección IP del servidor es **192.168.0.254**, añada la siguiente línea:

```
domain dominio.net server 192.168.0.54
```

Edite el fichero /etc/hosts:

```
vi /etc/hosts
```

Asegúrese que esté definido un registro que asocie la dirección IP principal del sistema con el nombre de anfitrión del sistema. Considerando que la IP del servidor es **192.168.0.254**, y que el nombre de anfitrión es **servidor.dominio.net**, deberá encontrar o añadir un registro similar al siguiente:

```
192.168.0.254   servidor.dominio.net    servidor
```

51.2.4.2. Establecer el domino NIS.

Es necesario integrar el sistema al dominio NIS. Utilice los siguientes dos mandatos para lograr ésto:

```
domainname dominio.net
ypdomainname dominio.net
```

51.2.4.3. Ajustes en los ficheros /etc/nsswitch.conf, /etc/hosts.allow y /etc/hosts.deny.

Edite el fichero /etc/nsswitch.conf:

```
vi /etc/nsswitch.conf
```

Añada las siguientes líneas al final de este fichero:

```
passwd: files nis
shadow: files nis
group: files nis
```

A fin de establecer una seguridad apropiada, es necesario denegar el acceso a todo en el fichero /etc/hosts.deny. Edite éste fichero:

```
vi /etc/hosts.deny
```

Añada la siguiente línea:

```
portmap:ALL
```

Edite el fichero /etc/hosts.allow:

vi /etc/hosts.allow

Defina los anfitriones y redes que tendrán permitido acceder a los servicios configurados:

```
portmap:127.0.0.1
portmap:192.168.0.0/255.255.255.0
```

51.2.4.4. Iniciar servicio ypbind.

Inicie y añada al arranque del sistema el servicio ypbind:

```
service ypbind start
chkconfig ypbind on
```

51.2.4.5. Comprobaciones.

Para asegurarse de que todo funciona correctamente, utilice el siguiente mandato que realizará una solicitud RPC para solicitar información del servicio ypbind:

```
rpcinfo -u localhost ypbind
```

El mandato anterior deberá regresar una salida similar a la siguiente. Si acaso regresa algo distinto o conexión rehusada, deben revisarse todos los procedimiejntos realizados hasta este punto.

```
el programa 100007 versión 1 está listo y a la espera
el programa 100007 versión 2 está listo y a la espera
```

Utilice el siguiente mandato para consultar todos los datos que están siendo distribuídos por el servicio ypserv del servidor NIS.

```
ypcat passwd
```

Lo anterior debe devolver una salida similar a la siguiente, que consiste en todo el contenido de /etc/passwd.

```
usuario1:$1$nieMHnA/$ScODTDw8lpog62ql03Jh00:541:48::/home/usuario1:/bin/bash
usuario2:$1$nieMHnA/$ScODTDw8lpog62ql03Jh00:510:48::/home/usuario2:/bin/bash
vusuario3:$1$nieMHnA/$ScODTDw8lpog62ql03Jh00:546:48::/home/usuario3:/bin/bash
```

52. Cómo configurar OpenLDAP como servidor de autenticación

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

52.1. Introducción.

LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) es un protocolo para consulta y modificación de servicios de directorio que se desempeñan sobre TCP/IP. **LDAP** utiliza el modelo X.500 para su estructura, es decir, se estructura árbol de entradas, cada una de las cuales consiste de un conjunto de atributos con nombre y que a su vez almacenan valores.

URL: http://en.wikipedia.org/wiki/LDAP

52.2. Equipamiento lógico requerido.

- openldap-2.2.13
- openldap-clients-2.2.13
- openldap-servers-2.2.
- authconfig-4.6.10
- authconfig-gtk-4.6.10 (opcional)

52.2.1. Instalación a través de yum.

```
yum -y install openldap openldap-clients openldap-servers authconfig authconfig-gtk
```

52.2.2. Instalación a través de up2date.

```
up2date -i openldap openldap-clients openldap-servers authconfig authconfig-gtk
```

52.3. Procedimientos.

Con fines de organización se creará un directorio específico para este directorio y se configurará con permisos de acceso exclusivamente al usuario y grupo ldap.

```
mkdir /var/lib/ldap/autenticar
chmod 700 /var/lib/ldap/autenticar
chown ldap.ldap /var/lib/ldap/autenticar
```

Crear la clave de acceso que se asignará en LDAP para el usuario administrador del directorio. Basta ejecutar desde una terminal:

```
slappasswd
```

Lo anterior debe dar como salida un criptograma como lo mostrado a continuación:

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

El texto de la salida será utilizado más adelante en el fichero **/etc/openldap/slapd.conf** y se definirá al usuario *Administrador* para como el utilizado para acceder con todos los privilegios al directorio.

Se edita el fichero **/etc/openldap/slapd.conf** y se verifica que los ficheros de esquema mínimos requeridos estén presentes. De tal modo, debe quedar algo así:

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
```

Independientemente de lo que ya se tenga configurado, y que no será tocado, se añade al final del fichero `/etc/openldap/slapd.conf` lo siguiente con el fin de definir el nuevo directorio que en adelante se utilizará para autenticar a toda al red local:

```
database        bdb
suffix          "dc=su-red-local,dc=com"
rootdn          "cn=Administrador,dc=su-red-local,dc=com"
rootpw          XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
directory       /var/lib/ldap/autenticar

# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
```

Inicie el servicio de **LDAP** y añada éste al resto de los servicios que arrancan junto con el sistema:

```
service ldap start
chkconfig ldap on
```

Edite el fichero **/usr/share/openldap/migration/migrate_common.ph** y modifique los los valores de las variables **$DEFAULT_MAIL_DOMAIN** y `$DEFAULT_BASE a fin de que queden del siguiente modo:`

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "su-red-local.com";
```

```
# Default base
$DEFAULT_BASE = "dc=su-red-local,dc=com";
```

A continuación hay que crear el objeto que a su vez contendrá el resto de los datos en el directorio. Genere un fichero base.ldif del siguiente modo:

```
/usr/share/openldap/migration/migrate_base.pl > base.ldif
```

Se utilizará **ldapadd** para insertar los datos necesarios. Las opciones utilizadas con este mandato son las siguientes:

```
-x              autenticación simple
-W              solicitar clave de acceso
-D binddn       Nombre Distinguido (dn) a utilizar
-h anfitrión    Servidor LDAP a acceder
-f fichero      fichero a utilizar
```

Una vez entendido lo anterior, se procede a insertar la información generada en el directorio utilizando lo siguiente:

```
ldapadd -x -W -D 'cn=Administrador, dc=su-red-local, dc=com' -h 127.0.0.1 -f base.ldif
```

Una vez hecho lo anterior, se podrá comenzar a poblar el directorio con datos. Lo primero será importar los grupos y usuarios existentes en el sistema. Realice la importación de usuarios utilizando los guiones correspondientes del siguiente modo:

```
/usr/share/openldap/migration/migrate_group.pl /etc/group group.ldif
/usr/share/openldap/migration/migrate_passwd.pl /etc/passwd passwd.ldif
```

Lo anterior creará los ficheros **group.ldif** y **passwd.ldif**, los cuales incluirán la información de los grupos y cuentas en el sistema, incluyendo las claves de acceso. Los datos se podrán insertar en el directorio LDAP utilizando lo siguiente:

```
ldapadd -x -W -D 'cn=Administrador, dc=su-red-local, dc=com' -h 127.0.0.1 -f group.ldif
ldapadd -x -W -D 'cn=Administrador, dc=su-red-local, dc=com' -h 127.0.0.1 -f passwd.ldif
```

52.4. Comprobaciones.

Antes de configurar el sistema para utilizar LDAP para autenticar, es conveniente verificar que todo funciona correctamente.

El siguiente mandato verifica que directorios disponibles existen en el servidor 127.0.0.1.

```
ldapsearch -h 127.0.0.1 -x -b '' -s base '(objectclass=*)' namingContexts
```

Lo anterior debe devolver una salida similar a lo siguiente:

```
# extended LDIF
#
```

```
# LDAPv3
# base <> with scope base
# filter: (objectclass=*)
# requesting: namingContexts
#

#
dn:
namingContexts: dc=su-red-local,dc=com

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

El siguiente mandato debe devolver toda la información de todo el directorio solicitado (dc=su-red-local,dc=com).

```
ldapsearch -x -b 'dc=su-red-local,dc=com' '(objectclass=*)'
```

Otro ejemplo es realizar una búsqueda específica para un usuario en particular. Suponiendo que en el sistema se tiene un usuario denominado *fulano*, puede ejecutarse lo siguiente:

```
ldapsearch -x -b 'uid=fulano,ou=People,dc=su-red-local,dc=com'
```

Lo anterior debe regresar algo como lo siguiente:

```
# extended LDIF
#
# LDAPv3
# base  with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# fulano, People, linuxparatodos.net
dn: uid=fulano,ou=People,dc=su-red-local,dc=com
uid: fulano
cn: fulano
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: xxxxxxxxxxxx
shadowLastChange: 12594
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 505
gidNumber: 505
homeDirectory: /home/fulano
```

```
# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

52.5. Configuración de clientes.

Defina los valores para los parámetros **host** y **base** a fin de establecer hacia que servidor y a que directorio conectarse. Para fines prácticos, el valor del parámetros **base** debe ser el mismo que se especificó en el fichero **/etc/openldap/slapd.conf** para el parámetro **suffix**.

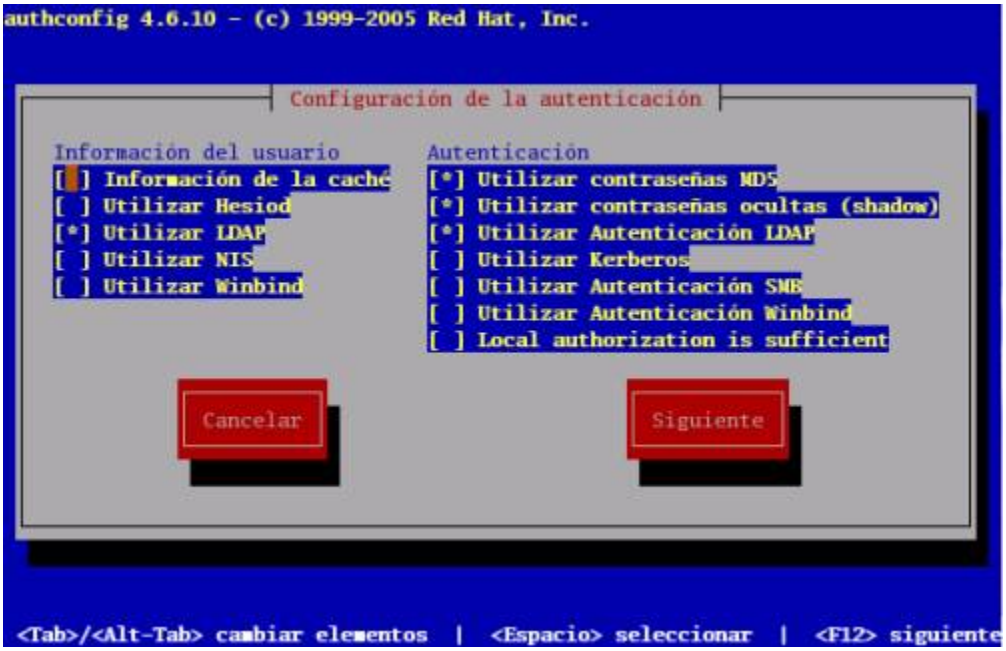
```
# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
host 192.168.0.1

# The distinguished name of the search base.
base dc=su-red-local,dc=com
```

Lo que sigue es utilizar ya sea **authconfig** o **authconfig-gtk** para configurar el sistema a fin de que se utilice el servidor LDAP para autenticar.

52.5.1. authconfig (modo texto)

Habilite las casillas **Utilizar LDAP** y **Utilizar Autenticación LDAP** y pulse la tecla **Tab** hasta **Siguiente** y pulse la tecla **Enter** y verifique que los datos del servidor y el directorio a utilizar sean los correctos.



uthconfig, pantalla principal.

authconfig, pantalla configuración ldap.

52.5.2. authconfig-gtk (modo gráfico)

Si se utiliza authconfig-gtk se deben habilitar las casillas de Soporte LDAP. Antes de cerrar la ventana en la pestañas de Información del usuario y Autenticación. Antes de dar clic en **Aceptar**, haga clic en **Configurar LDAP** y verifique que los datos del servidor y el directorio a utilizar sean los correctos.

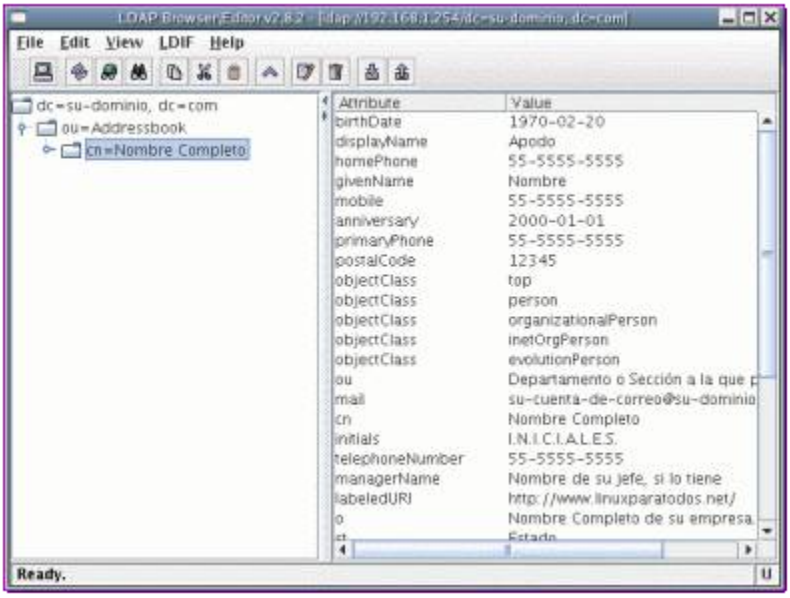
authconfig-gtk, pestaña de Información del usuario.

authconfig-gtk, pestaña de Autenticación.

authconfig-gtk, ventana Configurar LDAP.

52.6. Administración.

Hay una gran cantidad de programas para acceder y administrar servidores LDAP, pero la mayoría solo sirven para administrar usuarios y grupos del sistema como diradmin y el módulo de LDAP de Webmin. La mejor herramienta de administración de directorios LDAP que podemos recomendar es LDAP Browser/Editor (requiere Java).



LDAP Browser/Editor 2.8.1.

52.7. Respaldo de datos.

Debe detenerse el servicio de LDAP antes de proceder con el respaldo de datos.

```
service ldap stop
```

A continuación, se utiliza la herramienta **slapcat**, utilizando el fichero de configuración **/etc/openldap/slapd.conf**.

```
slapcat -v -f /etc/openldap/slapd.conf -l respaldo-$(date +%Y%m%d).ldif
```

Concluido el proceso de respaldo de datos, puede iniciarse de nuevo el servicio de **ldap**.

```
service ldap start
```

52.8. Restauración de datos.

El procedimiento requiere detener el servicio.

```
service ldap stop
```

Debe eliminarse los datos del directorio a restaurar.

```
rm -f /var/lib/ldap/autenticar/*
```

A continuación, se utiliza la herramienta **slapadd** para cargar los datos desde un fichero *.dif de respaldo.

```
slapadd -v -c -l respaldo-20061003.ldif -f /etc/openldap/slapd.conf
```

Se debe ejecutar la herramienta **slapindex**, que se utiliza para regenerar los índices LDAP.

```
slapindex
```

Concluido el proceso de restauración de datos, puede iniciarse de nuevo el servicio de **ldap**.

```
service ldap start
```

52.9. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir el puerto 389 por TCP (**LDAP**).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     389
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

53. Cómo configurar OpenLDAP como libreta de direcciones.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

53.1. Introducción.

LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) es un protocolo para consulta y modificación de servicios de directorio que se desempeñan sobre TCP/IP. **LDAP** utiliza el modelo X.500 para su estructura, es decir, se estructura árbol de entradas, cada una de las cuales consiste de un conjunto de atributos con nombre y que a su vez almacenan valores.

URL: http://en.wikipedia.org/wiki/LDAP

53.2. Equipamiento lógico requerido.

- openldap-2.2.13
- openldap-clients-2.2.13
- openldap-servers-2.2.13
- evolution-data-server-1.x (o bien simplemente del fichero evolutionperson.schema que incluye dicho paquete)

53.2.1. Instalación a través de yum.

```
yum -y install openldap openldap-clients openldap-servers evolution-data-server
```

53.2.2. Instalación a través de up2date.

```
up2date -i openldap openldap-clients openldap-servers evolution-data-server
```

53.3. Procedimientos.

Con fines de organización se creará un directorio específico para este directorio y se configurará con permisos de acceso exclusivamente al usuario y grupo **ldap**.

```
mkdir /var/lib/ldap/addressbook
chmod 700 /var/lib/ldap/addressbook
chown ldap.ldap /var/lib/ldap/addressbook
```

Crear la clave de acceso que se asignará en LDAP para el usuario administrador del directorio. Basta

ejecutar desde una terminal:

```
slappasswd
```

Lo anterior debe dar como salida un criptograma como lo mostrado a continuación:

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

El texto de la salida será utilizado más adelante en el fichero **/etc/openldap/slapd.conf** y se definirá al usuario **Administrador** para como el utilizado para acceder con todos los privilegios al directorio.

Se copia el fichero de esquema de evolution-data-server dentro del directorio **/etc/openldap/schema/**:

```
cp /usr/share/evolution-data-server-*/evolutionperson.schema \
/etc/openldap/schema/
```

Se edita el fichero **/etc/openldap/slapd.conf** y se agrega el esquema de datos incluido con evolution-data-server:

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/evolutionperson.schema
```

Independientemente de lo que ya se tenga configurado, y que no será tocado, se añade al final del fichero **/etc/openldap/slapd.conf** lo siguiente con el fin de definir el nuevo directorio que en adelante se utilizará como libreta de direcciones:

```
database        bdb
suffix          "dc=su-dominio,dc=com"
rootdn          "cn=Administrador,dc=su-dominio,dc=com"
rootpw          XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
directory       /var/lib/ldap/addressbook

# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
```

Inicie el servicio de LDAP y añada éste al resto de los servicios que arrancan junto con el sistema:

```
service ldap start
chkconfig ldap on
```

A continuación hay que crear el objeto que a su vez contendrá el resto de los datos en el directorio. Genere un fichero **addressbook.ldif** al cual agregará el siguiente contenido:

```
dn: dc=su-dominio, dc=com
objectclass: top
objectclass: dcObject
objectclass: organization
o: Nombre completo de su empresa
dc: su-dominio

dn: ou=Addressbook, dc=su-dominio, dc=com
ou: Addressbook
objectClass: top
objectClass: organizationalUnit
```

Se utilizará **ldapadd** para insertar los datos necesarios. Las opciones utilizadas con este mandato son las siguientes:

```
-x              autenticación simple
-W              solicitar clave de acceso
-D binddn       Nombre Distinguido (dn) a utilizar
-h anfitrión    Servidor LDAP a acceder
-f fichero      fichero a utilizar
```

Una vez entendido lo anterior, se procede a insertar la información generada en el directorio utilizando lo siguiente:

```
ldapadd -x -W -D 'cn=Administrador, dc=su-dominio, dc=com' -h 127.0.0.1 -f
addressbook.ldif
```

Una vez hecho lo anterior, se podrá comenzar a poblar el directorio con datos. Genere el fichero su-usuario.ldif con los siguientes datos, donde reemplazará los valores por reales. **Elimine los campos que queden vacíos o no le sean de utilidad, porque de otra forma LDAP no le dejará insertar éstos**. Es importante destacar que deben estar incluidas las clases **top**, **person**, **organizationalPerson**, **inetOrgPerson** y **evolutionPerson**, ya que de otro modo no será posible utilizar los campos de información necesarios para que el directorio funcione como libreta de direcciones.

```
dn: cn=Nombre Completo, ou=Addressbook, dc=su-dominio, dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: evolutionPerson
cn: Nombre Completo
givenName: Nombre
sn: Apellidos
displayName: Apodo
title: Sr.
mail: su-cuenta-de-correo@su-dominio.com
initials: I.N.I.C.I.A.L.E.S.
o: Nombre Completo de su empresa.
ou: Departamento o Sección a la que pertenece
businessRole: Puesto que desempeña en su empresa
```

```
homePostalAddress: Domicilio de su hogar.
postalAddress: Domicilio de su empresa.
l: Ciudad
st: Estado
# Código postal
postalCode: 12345
# Telefono empresa
telephoneNumber: 55-5555-5555
# Teléfono principal
primaryPhone: 55-5555-5555
# Teléfono móvil
mobile: 55-5555-5555
# Telefono hogar
homePhone: 55-5555-5555
# Otro teléfono
otherPhone: 55-5555-5555
labeledURI: http://www.linuxparatodos.net/
# Su fecha de nacimiento
birthDate: 1970-02-20
fileAs: Apellidos, Nombre
category: Cualquier-categoría-que-queira-crear
managerName: Nombre de su jefe, si lo tiene
assistantName: Nombre de su asistente, si lo tiene.
# Telefono de su asistente, si lo tiene
assistantPhone: 55-5555-5555
spouseName: Nombre de su esposa(o), si lo tiene.
# fecha en que celebra su aniversario de bodas, si aplica
anniversary: 2000-01-01
```

Los datos se podrán insertar utilizando lo siguiente:

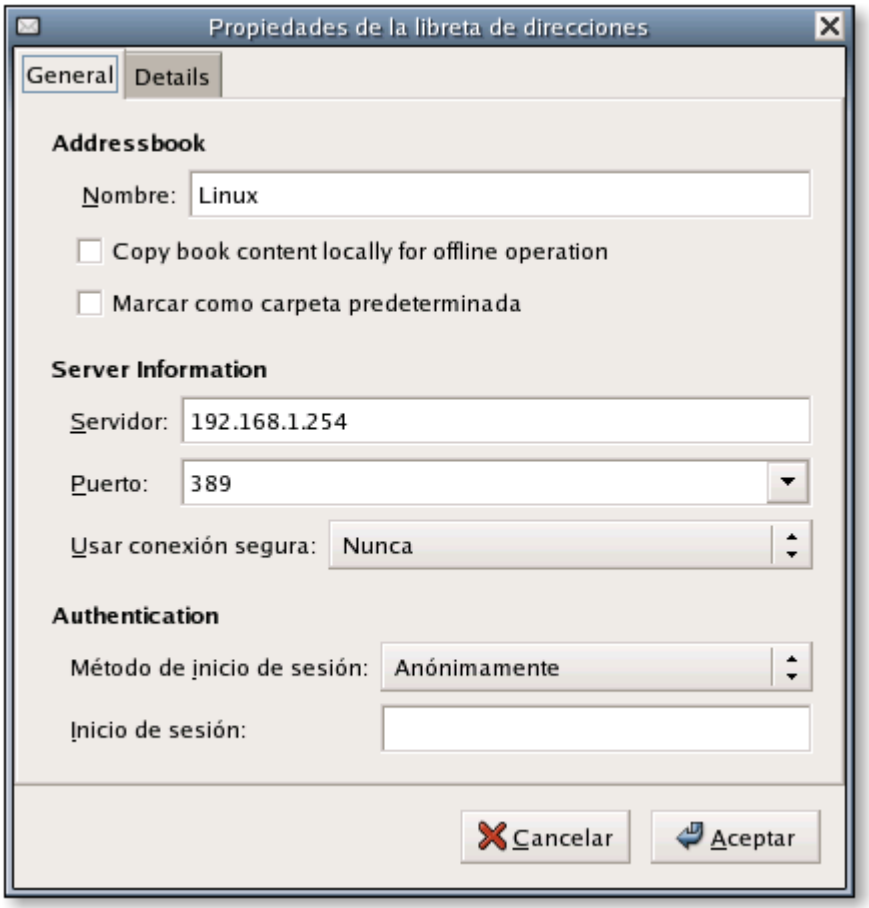
```
ldapadd -x -W -D 'cn=Administrador, dc=su-dominio, dc=com' -h 127.0.0.1 -f su-usuario.ldif
```

53.4. Configuración de clientes.

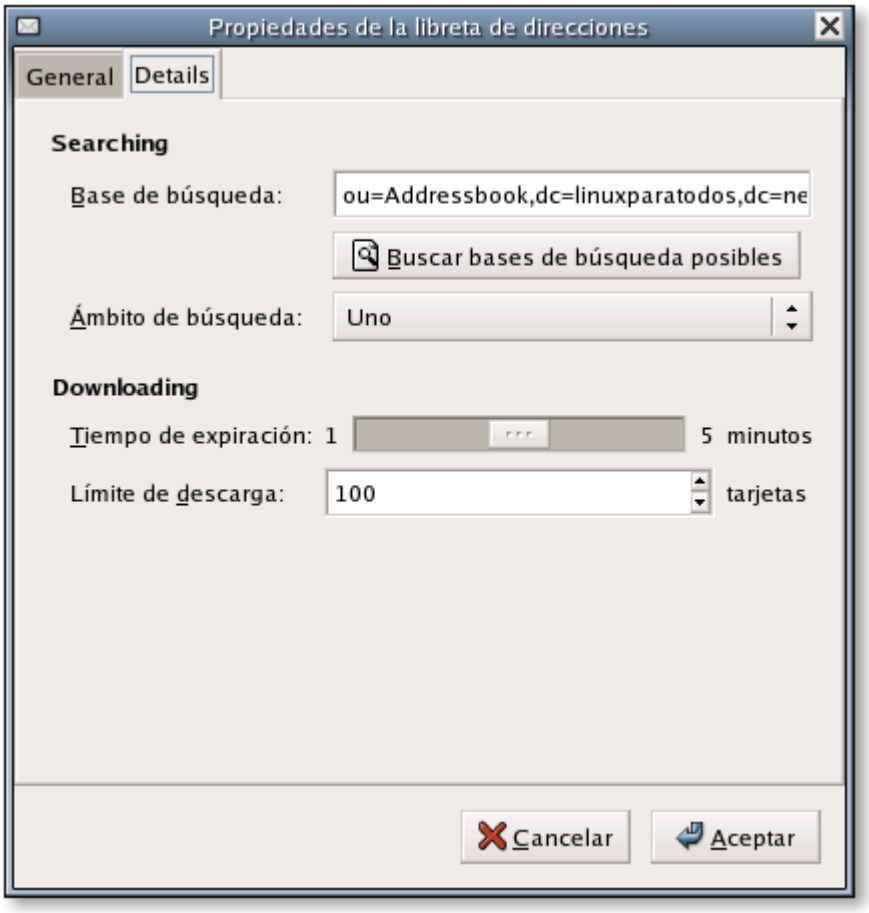
Acceda hacia el directorio con cualquier cliente que tenga soporte para acceder hacia directorios LDAP.

53.4.1. Novell Evolution.

Hacer clic en Archivo → Nuevo → Libreta de direcciones.



Propiedades de la libreta de direcciones, pestaña General.

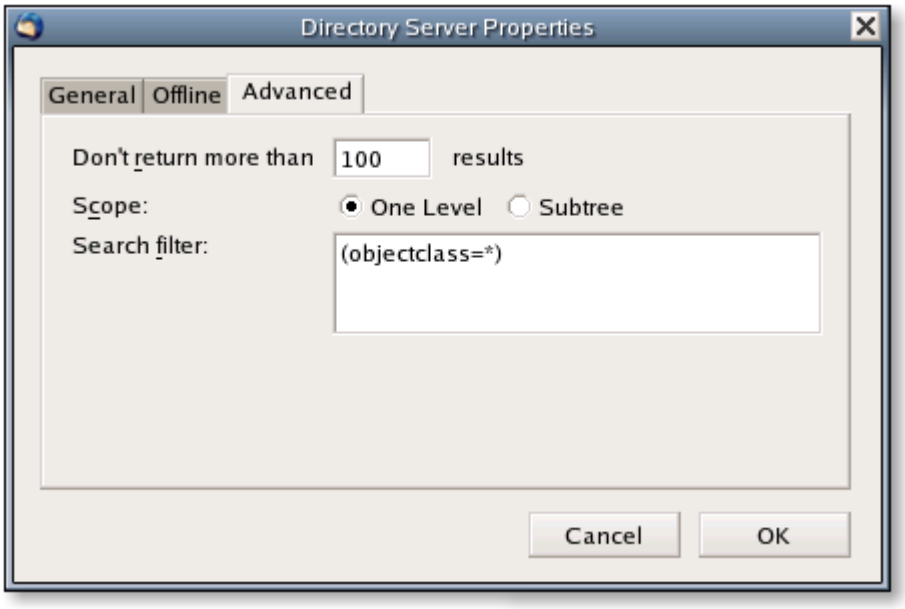


Propiedades de la libreta de direcciones, pestaña Detalles.

53.4.2. Mozilla Thunderbird.

Hacer clic en Archivo → Nuevo → Directorio LDAP

Propiedades de servidor de directorio, pestaña General.



Propiedades de servidor de directorio, pestaña Avanzado.

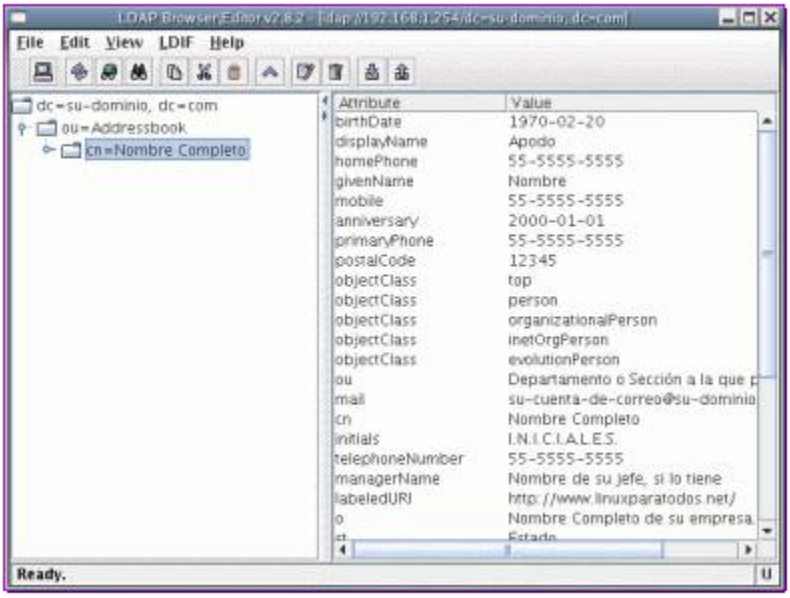
53.4.3. Squirrelmail.

Hay que editar el fichero **/etc/squirrelmail/config.php** y añadir/editar:

```
$ldap_server[0] = array(
    'host' => '127.0.0.1',
    'base' => 'ou=Addressbook,dc=su-dominio,dc=com',
    'name' >= 'Addressbook'
);
```

53.5. Administración.

Hay una gran cantidad de programas para acceder y administrar servidores LDAP, pero la mayoría solo sirven para administrar usuarios y grupos del sistema. La mejor herramienta de administración de directorios LDAP que podemos recomendar es LDAP Browser/Editor (requiere Java).



LDAP Browser/Editor 2.8.1.

53.6. Respaldo de datos.

Debe detenerse el servicio de LDAP antes de proceder con el respaldo de datos.

```
service ldap stop
```

A continuación, se utiliza la herramienta **slapcat**, utilizando el fichero de configuración **/etc/openldap/slapd.conf**.

```
slapcat -v -f /etc/openldap/slapd.conf -l respaldo-$(date +%Y%m%d).ldif
```

Concluido el proceso de respaldo de datos, puede iniciarse de nuevo el servicio de **ldap**.

```
service ldap start
```

53.7. Restauración de datos.

El procedimiento requiere detener el servicio.

```
service ldap stop
```

Debe eliminarse los datos del directorio a restaurar.

```
rm -f /var/lib/ldap/addressbook/*
```

A continuación, se utiliza la herramienta **slapadd** para cargar los datos desde un fichero *.dif de respaldo.

```
slapadd -v -c -l respaldo-20061003.ldif -f /etc/openldap/slapd.conf
```

Se debe ejecutar la herramienta **slapindex**, que se utiliza para regenerar los índices LDAP.

```
slapindex
```

Concluido el proceso de restauración de datos, puede iniciarse de nuevo el servicio de **ldap**.

```
service ldap start
```

53.8. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir el puerto 389 por TCP (**LDAP**).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     389
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

54. Cómo configurar OpenLDAP con soporte SSL/TLS.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

54.1. Introducción.

Este documento requiere la lectura y comprensión previa de cualquiera de los siguientes temas:

- Cómo configurar OpenLDAP como libreta de direcciones.
- Cómo configurar OpenLDAP como servidor de autenticación.

54.1.1. Acerca de LDAP en modo SSL/TLS.

El inicio de la operación StartTLS en un servidor LDAP, establece la comunicación **TLS** (**T**ransport **L**ayer **S**ecurity, o Seguridad para Nivel de Transporte) a través del mismo puerto 389 por TCP. Provee confidencialidad en el transporte de datos e protección de la integridad de datos. Durante la negociación, el servidor envía su certificado con estructura X.509 para verificar su identidad. Opcionalmente puede establecerse la comunicación. La conexión a través del puerto 389 y 636 difiere en lo siguiente:

1. Al realizar la conexión por puerto 636, tanto el cliente como el servidor establecen TLS antes de que se transfiera cualquier otro dato, sin utilizar la operación **StatTLS**.

2. La conexión a través de puerto 636 debe cerrarse al terminar TLS.

URL: http://en.wikipedia.org/wiki/LDAP

54.1.2. Acerca de RSA.

RSA, acrónimo de los apellidos de sus autores, Ron **R**ivest, Adi **S**hamir y Len **A**dleman, es un algoritmo para el cifrado de claves públicas que fue publicado en 1977, patentado en EE.UU. en 1983 por el el Instituto Tecnológico de Michigan (**MIT**). **RSA** es utilizado ampliamente en todo el mundo para los protocolos destinados para el comercio electrónico.

URL: http://es.wikipedia.org/wiki/RSA

54.1.3. Acerca de X.509.

X.509 es un estándar **ITU-T** (estandarización de **T**elecomunicaciones de la **I**nternational **T**elecommunication **U**nion) para infraestructura de claves públicas (**PKI**, o **P**ublic **K**ey **I**nfrastructure). Entre otras cosas, establece los estándares para certificados de claves públicas y un

algoritmo para validación de ruta de certificación. Este último se encarga de verificar que la ruta de un certificado sea válida bajo una infraestructura de clave pública determinada. Es decir, desde el certificado inicial, pasando por certificados intermedios, hasta el certificado de confianza emitido por una Autoridad Certificadora (**CA**, o **C**ertification **A**uthority).

URL: http://es.wikipedia.org/wiki/X.509

54.1.4. Acerca de OpenSSL.

OpenSSL es una implementación libre, de código abierto, de los protocolos **SSL** (**S**ecure **S**ockets **L**ayer o Nivel de Zócalo Seguro) y **TLS** (**T**ransport **L**ayer **S**ecurity, o Seguridad para Nivel de Transporte). Está basado sobre el extinto proyecto **SSLeay**, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation.

URL: http://www.openssl.org/

54.2. Procedimientos.

54.2.1. Generando clave y certificado.

```
cd /etc/openldap/cacerts
```

La creación de la llave y certificado para **OpenLDAP** requiere utilizar una clave con algoritmo **RSA** de 1024 octetos y estructura **x509**. En el ejemplo a continuación, se establece una validez por 730 días (dos años) para el certificado creado.

```
openssl req -x509 -nodes -newkey rsa:1024 \
-days 730 -out slapd.crt -keyout slapd.key
```

Lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o razón social.
- Unidad o sección.
- Nombre del anfitrión.
- Dirección de correo.

La salida devuelta sería similar a la siguiente:

```
Generating a 1024 bit RSA private key
................++++++
.++++++
writing new private key to 'dovecot.key'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
```

```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:Mexico
Organization Name (eg, company) [My Company Ltd]:
Mi empresa, S.A. de C.V.
Organizational Unit Name (eg, section) []:Direccion Comercial
Common Name (eg, your name or your server's hostname) []:
midominio.org
Email Address []:webmaster@midominio.org
```

El certificado solo será válido cuando el servidor **LDAP** sea invocado con el nombre definido en el campo **Common Name**. Es decir, solo podrá utilizarlo cuando se defina **midominio.org** como servidor **LDAP** con soporte **SSL/TLS**. No funcionará si se invoca al servidor como, por mencionar un ejemplo, **directorio.midominio.org**.

Es indispensable que todos los ficheros de claves y certificados tengan permisos de acceso de solo lectura para el usuario **ldap**:

```
chown ldap.ldap /etc/openldap/cacerts/slapd.*
chmod 400 /etc/openldap/cacerts/slapd.*
```

54.2.2. Parámetros de /etc/openldap/slapd.conf.

Se deben descomentar los parámetros **TLSCACertificateFile**, **TLSCertificateFile** y **TLSCertificateKeyFile** establecendo las rutas hacia el certificado y clave. Opcionalmente se puede descomentar la directiva **referral** para indicar el **URI** (**U**niform **R**esource **I**dentifier o Identificador Uniforme de Recursos) del servicio de directorio superior como **ldaps** en lugar de **ldap**.

```
TLSCACertificateFile /etc/openldap/cacerts/slapd.crt
TLSCertificateFile /etc/openldap/cacerts/slapd.crt
TLSCertificateKeyFile /etc/openldap/cacerts/slapd.key
referral        ldaps://midominio.org
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **ldap**.

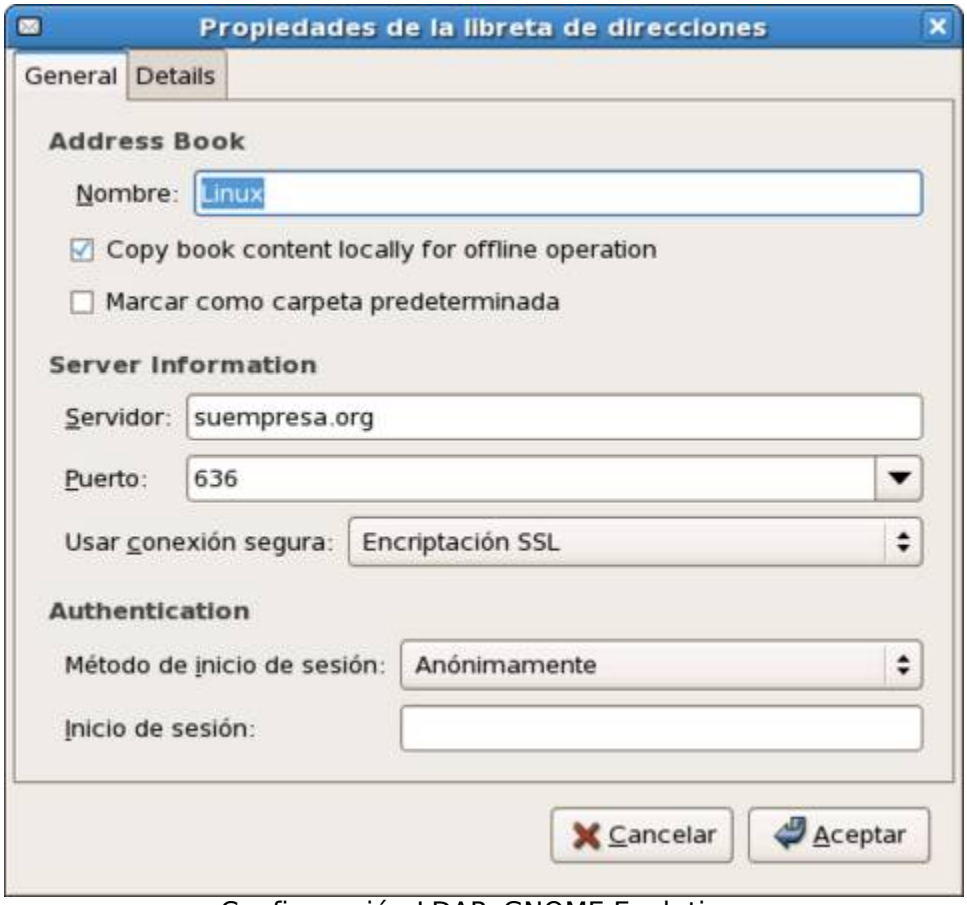
```
service ldap restart
```

54.2.3. Comprobación.

Configure cualquier cliente LDAP para utilizar SSL en el puerto 636. Tras aceptar el certificado, en el caso de que éste no haya sido firmado por un **RA** (**R**egistration **A**uthority o Autoridad de Registro), servidor LDAP deberá permitir completar la conexión y realizar cualquier tipo de consulta y/o manipulación de registros.

54.2.4. Configuración de GNOME Evolution.

Se debe establecer el mismo nombre del servidor utilizado para crear el certificado, y conexión por SSL.



Configuración LDAP, GNOME Evolution.

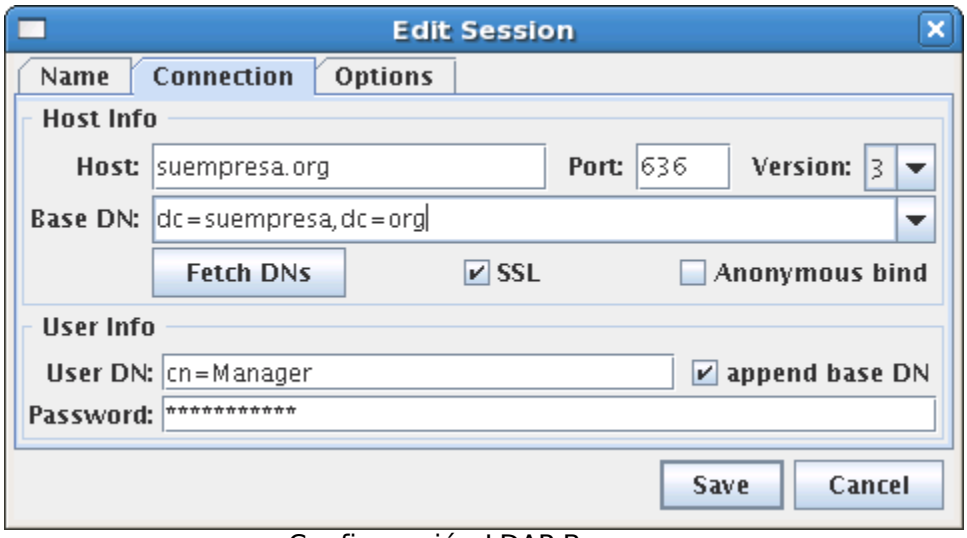
54.2.5. Configuración de Mozilla Thunderbird.

Se debe establecer el mismo nombre del servidor utilizado para crear el certificado, y conexión por SSL.

Configuración LDAP, Mozilla Thunderbird.

54.2.6. Configuración LDAP Browser.

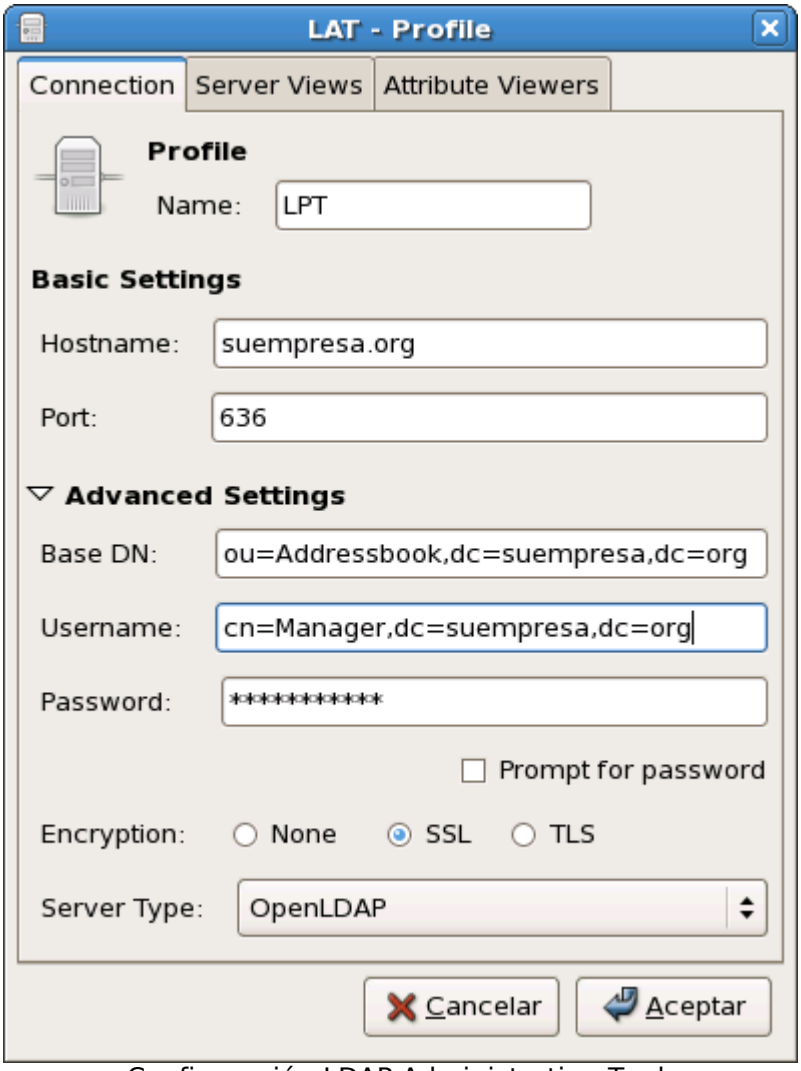
Se debe establecer el mismo nombre del servidor utilizado para crear el certificado, y conexión por SSL.



Configuración LDAP Browser.

54.2.7. Configuración LDAP Administration Tool.

Se debe establecer el mismo nombre del servidor utilizado para crear el certificado, y conexión por SSL.



Configuración LDAP Administration Tool.

54.3. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, además del puerto 389 por TCP, es necesario abrir el puerto 636 por TCP (**LDAPS**).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     389,636
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

55. Configuración básica de Freeradius con soporte de LDAP.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

55.1. Introducción.

55.1.1. Acerca de RADIUS.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) es un protocolo de autenticación, autorización y manejo de cuentas de usuario originalmente desarrollado por Livingston Enterprises y publicado en 1997 como los RFC 2058 y 2059. Es utilizado para administrar el acceso remoto y la movilidad IP, como ocurre en servicios de acceso por modem, DSL, servicios inalámbricos 802.11 o servicios de **VoIP** (**V**oice **o**ver **IP** o Voz sobre IP). Este protocolo trabaja a través del puerto 1812 por UDP.

La autenticación gestionada por este protocolo se realiza a través del ingreso de un nombre de usuario y una clave de acceso. Esta información es procesada por un dispositivo **NAS** (**N**etwork **A**ccess **S**erver) a través de **PPP** (**P**oint-to-**P**oint **P**rotocol o Protocolo Punto-a-Punto) siendo posteriormente validada por un servidor **RADIUS** a través del protocolo correspondiente valiéndose de diversos esquemas de autenticación, como **PAP** (**P**assword **A**uthentication **P**rotocol o Protocolo de Autenticación de Clave de acceso), CHAP (**C**hallenge-**H**andshake **A**uthentication **P**rotocol) o **EAP** (**E**xtensible **A**uthentication **P**rotocol), y permitiendo el acceso al sistema.

URL: http://tools.ietf.org/html/rfc2058 y http://tools.ietf.org/html/rfc2059

55.1.2. Acerca de Freeradius.

Freeradius, proyecto iniciado en 1999 por Alan DeKok y Miquel van Smoorenburg (quien colaboró anteriormente en el desarrollo de Cistron RADIUS), es una alternativa libre hacia otros servidores RADIUS, siendo uno de los más completos y versátiles gracias a la variedad de módulos que le componenen. Puede operar tanto en sistemas con recursos limitados así como sistemas atendiendo millones de usuarios.

Freeradius inició como un proyecto de servidor RADIUS que permitiera una mayor colaboración de la comunidad y que pudiera cubrir las necesidades que otros servidores RADIUS no podían. Actualmente incluye soporte para LDAP, SQL y otras bases de datos, así como EAP, EAP-TTLS y PEAP. Actualmente incluye soporte para todos los protocolos comunes de autenticación y bases de datos.

URL: http://www.freeradius.org/

55.2. Equipamiento lógico necesario.

55.2.1. Instalación a través de yum.

Si se utiliza de CentOS 4 o White Box Enterprise Linux 4, solo basta utilizar lo siguiente:

```
yum -y install freeradius
```

55.2.2. Instalación a través de Up2date

Si se utiliza de Red Hat™ Enterprise Linux 4, solo basta utilizar lo siguiente:

```
up2date -i freeradius
```

55.3. Procedimientos.

Editar /etc/raddb/radiusd.conf y habilitar la línea que activa el módulo de LDAP:

```
Authorize {

        #
        #  The ldap module will set Auth-Type to LDAP if it has not
        #  already been set
        ldap
```

En este mismo fichero se configura el directorio LDAP a utilizar:

```
ldap {
                server = "tu-servidor-ldap"
                # identity = "cn=admin,o=My Org,c=UA"
                # password = mypass
                basedn = "ou=People,dc=dominio,dc=com"
                password_attribute = "userPassword"
                filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
```

Si no se va a utilizar el acceso Dial-Up, se puede desactivar la función o de otro modo no permitirá autenticar o realizar las pruebas de verificación.

```
# access_attr = "dialupAccess"
```

Se añade el método de autenticación LDAP en el fichero **/etc/raddb/users** del siguiente modo:

```
#
# First setup all accounts to be checked against the UNIX /etc/passwd.
# (Unless a password was already given earlier in this file).
#
DEFAULT Auth-Type = System
    Fall-Through = 1
#
```

```
# Defaults for LDAP
#
DEFAULT Auth-Type := LDAP
    Fall-Through = 1
```

Finalmente se define en el fichero **/etc/raddb/clients.conf** a la red o redes que se permitirá autenticar:

```
client 192.168.0.0/24 {
    secret          = clave-acceso-red
    shortname       = Nombre de la red privada
}
```

55.3.1. Agregar el servicio al arranque del sistema.

Para hacer que el servicio de **RADIUS** esté activo con el siguiente inicio del sistema, en todos los niveles de corrida (2, 3, 4, y 5) se utiliza lo siguiente

```
chkconfig radiusd on
```

55.3.2. Iniciar, detener y reiniciar el servicio.

Para ejecutar por primera vez el servicio, utilice:

```
service radiusd start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service radiusd restart
```

Para detener el servicio, utilice:

```
service radiusd stop
```

55.4. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir el puerto 1812 por UDP.

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      udp     1812
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

55.5. Comprobaciones.

Freeradius incluye una herramienta para realizar pruebas. A fin de verificar que funcione

correctamente la autenticación, se utiliza el mandato radtest del siguiente modo:

```
radtest usuario-ldap "clave-de-acceso-en-ldap" \
192.168.0.1 2 clave-acceso-red
```

Lo anterior debe devolver algo como lo siguiente:

```
Sending Access-Request of id 191 to 192.168.0.1:1812
         User-Name = "usuario-ldap"
         User-Password = "clave-de-acceso-en-ldap"
         NAS-IP-Address = nombre-servidor
         NAS-Port = 2
rad_recv: Access-Accept packet from host 192.168.0.1:1812, id=191,
length=20
```

56. Cómo instalar y configurar MySQL™.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

56.1. Introducción.

56.1.1. Acerca de MySQL™.

MySQL™ es un **DBMS** (**b**ata**B**ase **M**anagement **S**ystem) o sistema de gestión de base de datos **SQL** (**S**tructured **Q**uery **L**anguage o Lenguaje Estructurado de Consulta) multiusuario y multihilo con licencia **GNU/GPL**.

MySQL™ es propiedad y patrocinio de **MySQL AB**, compañía fundada por David Axmark, Allan Larsson y Michael Widenius, con base de operaciones en Suecia, la cual posee los derechos de autor de casi todo el código que lo integra. **MySQL AB** desarrolla y mantiene el sistema vendiendo servicios de soporte y otros valores agregados, así como licenciamiento propietario para los desarrollos de equipamiento lógico que requieren mantener cerrado su código.

MySQL™ es actualmente el servidor de base de datos más popular para los desarrollos a través de la red mundial, con una estimación de más de diez millones de instalaciones. Es muy rápido y sólido.

56.2. Equipamiento lógico necesario.

56.2.1. Instalación a través de yum.

Si utiliza **CentOS 4** o **White Box Enterprise Linux 4**, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install mysql mysql-server
```

56.2.2. Instalación a través de up2date.

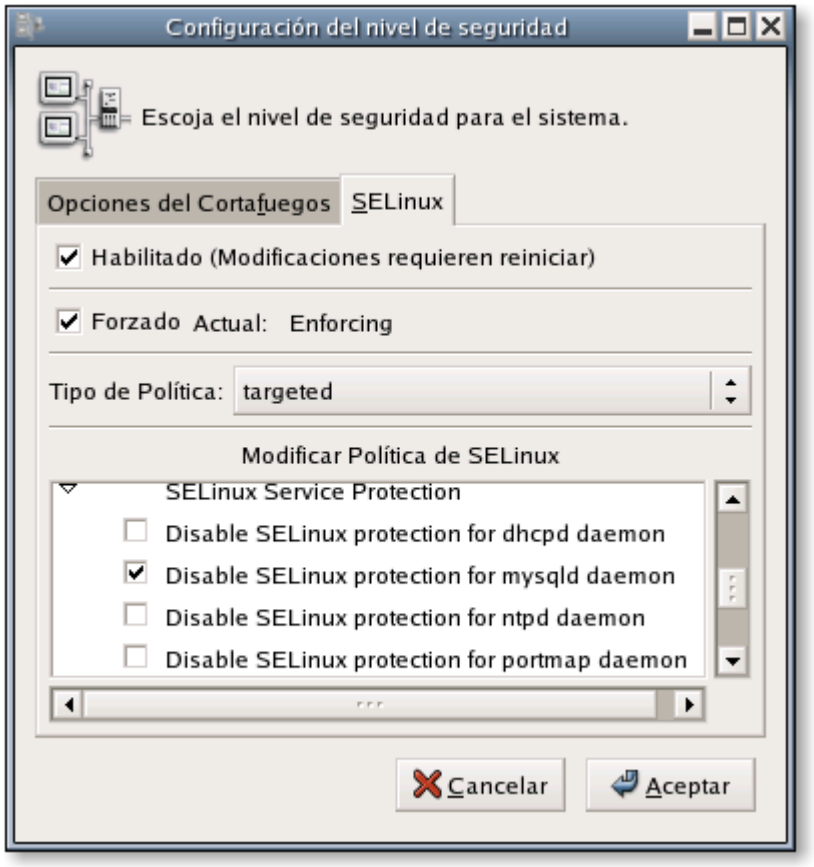
Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date -i mysql mysql-server
```

56.3. Procedimientos.

56.3.1. SELinux y el servicio mysqld

Si utiliza **CentOS 4**, **Red Hat™ Enterprise Linux 4** o **White Box Enterprise Linux 4**, utilice la herramienta system-config-securitylevel (desde el modo gráfico), seleccione la pestaña de **SELinux**, y habilite la casilla con la leyenda **Disable SELInux protection for mysqld daemon** en la sección de **SELinux Service Protection**. De otro modo, el servicio **mysqld** no podrá iniciar.



Desactivar protección de SELinux para mysqld.

56.3.2. Iniciar, detener y reiniciar el servicio mysqld.

Para iniciar por primera vez el servicio **mysqld** y generar la base de datos inicial (**mysql**), utilice:

```
/sbin/service mysqld start
```

Para reiniciar el servicio **mysqld**, utilice:

```
/sbin/service mysqld restart
```

Para detener el servicio **mysqld**, utilice:

```
/sbin/service mysqld stop
```

56.3.3. Agregar el servicio mysqld al arranque del sistema.

Para hacer que el servicio de **mysqld** esté activo con el siguiente inicio del sistema, en todos los niveles de corrida (2, 3, 4, y 5), se utiliza lo siguiente:

```
/sbin/chkconfig mysqld on
```

56.3.4. Asignación de clave de acceso al usuario root.

El usuario **root** en MySQL%trade;, no tiene asignada clave de acceso alguna después de iniciado el servicio por primera vez. Por razones de seguridad, es muy importante asignar una clave de acceso.

56.3.4.1. Método corto.

La forma más simple de asignar una clave de acceso al usuario **root** de **MySQL™** solo requiere de un único mandato, descrito a continuación.

```
mysqladmin -u root password nueva-clave-de-acceso
```

En adelante, será necesario añadir la opción **-p** a cualquier sentencia de línea de mandatos para , **mysqladmin** y **mysqldump** para ingresar la clave de acceso del usuario **root** y poder, de esta forma, realizar diversas tareas administrativas.

56.3.4.2. Método largo.

La forma complicada de realizar lo anterior se describe solo con fines didácticos y **como prueba de concepto**. No es del todo práctico realizar asignación de la clave de acceso del usuario **root** con este método, pero sirve para entender el funcionamiento en cuanto a asignación de claves de acceso.

Como **root**, utilice el mandato **mysql**:

```
# mysql
```

Dentro del intérprete de mandatos de MySQL, indique con el mandato **use mysql** que utilizará única base de datos existente, **mysql**:

```
> use mysql
```

Solicite con el mandato **show tables** que se muestren las tablas de la base de datos **mysql**:

```
> show tables;
```

Con el mandato **select * from user** se mostrará el contenido de la tabla **user** de la base de datos actual:

```
> select * from user;
```

Esto hará que se vea, entre otras **muchas** cosas, lo siguiente:

```
+-------------------------+----------+------------------+--------------+
| Host                    | User     | Password         | Select_priv  |
+-------------------------+----------+------------------+--------------+
| localhost               | root     |                  | Y            |
+-------------------------+----------+------------------+--------------+
```

Como se podrá observar, el usuario **root** no tiene asignada una clave de acceso, por lo que cualquiera que se identifique como root en el sistema tendrá acceso a todo en MySQL. Se asignará una clave de acceso del siguiente modo:

```
> update user set Password=PASSWORD('nuevo_password') where user='root';
```

Utilice de nuevo el mandato **select * from user** y vuelva observar el campo que correspondería al de la clave de acceso del usuario **root**:

```
> select * from user;
```

Deberá aparecer ahora un criptograma en el campo que corresponde a la clave de acceso del usuario **root**.

```
+-------------------------+----------+------------------+--------------+
| Host                    | User     | Password         | Select_priv  |
+-------------------------+----------+------------------+--------------+
| localhost               | root     |4593274b8e0d68j852| Y            |
+-------------------------+----------+------------------+--------------+
```

Se recomienda realizar refresco de los privilegios a fin de que tomen efecto los cambios.

```
> flush privileges
```

Para probar, solo hay que salir del intérprete de MySQL.

```
> quit
```

Intente ingresar de nuevamente al intérprete de mandatos de MySQL™:

```
mysql
```

Notará que ya no se puede acceder como antes, y regresa un mensaje de error.

```
ERROR 1045: Access denied for user: 'root@localhost' (Using password: NO)
```

Ejecute ahora el mismo mandato, pero especificando un usuario (**-u root**) y solicitando se pregunte por una clave de acceso (**-p**):

```
mysql -u root -p
```

A continuación se le pedirá ingrese una clave de e acceso, tras lo cual obtendrá de nuevo acceso al intérprete de mandatos de MySQL™

56.4. Creando y destruyendo bases de datos.

Para crear una nueva base de datos, puede utilizarse el mandato **mysqladmin** con el parámetro **create**:

```
mysqladmin -u root -p create dbejemplo
```

Si queremos eliminar dicha base de datos, utilizamos el parámetro **drop** en lugar de **create**.

```
mysqladmin -u root -p drop dbejemplo
```

56.5. Otorgando permisos a los usuarios.

En adelante el usuario **root** solo se utilizará para tareas administrativas y creación de nuevas bases de datos. Resultará conveniente delegar a los usuarios ordinarios el manejo de sus propias bases de datos.

Una vez generada una base de datos, debemos determinar con que usuario y desde que equipo en la red local, se podrá tener acceso, así como los privilegios para modificar esta. Lo más común, y seguro, es asignar el acceso solo desde el mismo servidor (*localhost*), a menos que el desarrollo web o aplicación se localice en otro equipo.

Genere un base de datos denominada **directorio**:

```
mysqladmin -u root -p create directorio
```

Se accede hacia el intérprete de mandatos de **MySQL™** y se utiliza lo siguiente, suponiendo que se desea asignar permisos **select** (seleccionar), **insert** (insertar), **update** (actualizar), **create** (crear), **alter** (aldetar), **delete** (eliminar) y **drop** (descartar) sobre las tablas de la base de datos **directorio** al usuario **prueba** desde el anfitrión **localhost** (equipo local):

```
GRANT select, insert, update, create, alter, delete, drop ON directorio.* TO
prueba@localhost IDENTIFIED BY 'password_del_usuario_prueba';
```

Al concluir, se tendrá una base de datos denominada **directorio** que podrá ser utilizada y modificada por el usuario **prueba** desde el anfitrión **localhost**. Esto establecerá un nivel de seguridad apropiado, y garantizará que de verse comprometida la seguridad, la clave de acceso de un usuario no podrá ser utilizada desde un sistema remoto.

Si, **por mencionar un ejemplo**, se requiere permitir el acceso hacia la base de datos **directorio** desde otro equipo en la red local, con fines administrativos, se puede otorgar el acceso y permisos al usuario **jperez** desde el anfitrión 192.168.1.253, es decir **jperez@192.168.1.253**.

```
GRANT
select, insert, update, create, alter, delete, drop
ON
directorio.*
TO
jperez@192.168.1.253
IDENTIFIED BY
'clave_de_acceso_para_jperez';
```

56.6. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir el puerto 3306 por TCP (**mysql**).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** en un sistema con una zona (**net**), correspondería a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     3306
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** en un sistema con dos zonas (**net** y **loc**), donde solo se va a permitir el acceso al servicio **mysqld** desde la red local, correspondería a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  loc     fw      tcp     3306
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

57. Configuración básica de Apache.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

57.1. Introducción.

57.1.1. Acerca del protocolo HTTP.

HTTP (**H**yper**t**ext **T**ransfer **P**rotocol, o Protocolo de Trasferencia de Hipertext), es el método utilizado para transferir o transportar información en la Red Mundial (WWW, **W**orld **W**ide **W**eb). Su propósito original fue el proveer una forma depublicar y recupertar documentos HTML.

El desarrollo del protocolo fue coordinado por World Wide Web Consortium y la **IETF** (**I**nternet **E**ngineering **T**ask **F**orce, o Fuerza de Trabajo en Ingeniería de Internet), culminando con la publicación de variso RFC (**R**equest **F**or **C**omments), de entre los que destaca el RFC 2616, mismo que define la versión 1.1 del protocolo, que es el utilizado hoy en día.

HTTP es un protocolo de solicitud y respuesta a través de **TCP**, entre agentes de usuario (Navegadores, motores de índice y otras herramientas) y servidores, regularmente utilizando el puerto 80. Entre la comunicación entre éstos puede intervenir como servidores Intermediarios (Proxies), puertas de enlace y túneles.

URL: http://tools.ietf.org/html/rfc2616

57.1.2. Acerca de Apache.

Apache es un servidor HTTP, de código abierto y licenciamiento libre, que funciona en Linux, sistemas operativos derivados de Unix™, Windows, Novell Netware y otras plataformas. Ha desempeñado un papel muy importante en el crecimiento de la red mundial, y continua siendo el servidor HTTP más utilizado, siendo además el servidor *de facto* contra el cual se realizan las pruebas comparativas y de desempeño para otros productos competidores. Apache es desarrollado y mantenido por una comunidad de desarrolladores auspiciada por Apache Software Foundation.

URL: http://www.apache.org/

57.2. Equipamiento lógico necesario.

57.2.1. Instalación a través de yum.

Si se utiliza de CentOS 4 o White Box Enterprise Linux 4, solo basta utilizar lo siguiente:

```
yum -y install httpd
```

Si se desea que Apache incluya soporte para **PHP**/**MySQL**, **Perl**, **Python** y **SSL**/**TLS**, solo bastará ejecutar:

```
yum -y install php php-mysql mod_perl mod_python mod_ssl
```

57.2.2. Instalación a través de Up2date

Si se utiliza de Red Hat™ Enterprise Linux 4, solo basta utilizar lo siguiente:

```
up2date -i httpd
```

Si se desea que Apache incluya soporte para PHP/MySQL, Perl, Python y SSL, solo bastará utilizar:

```
up2date -i php php-mysql mod_perl mod_python mod_ssl
```

57.3. Iniciar servicio y añadir el servicio al arranque del sistema.

Apache es un servicio que por fortuna solo es necesario instalar e iniciar. No requiere modificaciones adicionales para su funcionamiento básico. Para añadir el servicio a los servicios que inician junto con el sistema, solo basta ejecuta:

```
chkconfig httpd on
```

Para iniciar el servicio por primera vez, solo basta utilizar:

```
service httpd start
```

Para reiniciar el servicio, considerando que se interrumpirán todas las conexiones establecidas en ese momento, solo basta utilizar:

```
service httpd restart
```

Si el servicio ya está trabajando, también puede utilizar **reload** a fin de que Apache vuelva a leer y cargar la configuración sin interrumpir el servicio, y, por ende, las conexiones establecidas.

```
service httpd reload
```

Para detener el servicio, solo basta utilizar:

```
service httpd stop
```

57.4. Procedimientos.

57.4.1. SELinux y Apache.

Si utiliza alguna distribución con núcleo 2.6 basada sobre Red Hat™ Enterprise Linux 4.0, como serían CentOS 4.0 o White Box Enterprise Linux 4.0 en adelante, éstas incluyen SELinux que añade seguridad adicional a Apache, sin embargo algunas opciones impedirán utilizar ciertas funciones en Apache, como directorios virtuales. Ejecute **system-config-securitylevel** desde el modo gráfico y

active la casilla que dice «*Disable SELinux Protection for httpd daemon*» y haga clic en el botón de «*Aceptar*». Si no tiene planeado utilizar directorios virtuales, puede dejar desactivada la casilla y aprovechar toda la seguridad adicional que brinda SELinux.

system-config-securitylevel.

57.4.2. UTF-8 y codificación de documentos.

UTF-8
: UTF-8 es un método de codificación de ASCII para Unicode (ISO-10646), el Conjunto de Caracteres Universal o UCS. éste codifica la mayoría de los sistemas de escritura del mundo en un solo conjunto de caracteres, permitiendo la mezcla de lenguajes y guiones en un mismo documento sin la necesidad de ajustes para realizar los cambios de conjuntos de caracteres.

Cualquier sitio de red que haga uso de bases de datos y documentos HTML suele toparse con problemas cuando se trata de lidiar con el tipo de codificación (UTF-8, ISO-8859-1, etc.), puesto que en algunos casos, por citar un ejemplo, los caracteres latinos se muestran incorrectamente por el cambio de codificación.

Debido a su conveniencia actualmente se está adoptando UTF-8 como codificación para todo, sin embargo aún hay mucho material codificado en, por ejemplo, ISO-8859-1.

Lo correcto es codificar los documentos codificados en ISO8859-1 y otras tablas de caracteres hacia en UTF-8, utilizando métodos como el siguiente:

```
cd /var/www/html/
```

```
for f in *.html
do
vi -c ":wq! ++enc=utf8" $f
done
```

Si desea continuar **viviendo en el pasado** y no aceptar el nuevo estándar, también puede desactivar la función en Apache que establece UTF-8 como codificación predefinida. Edite el fichero **/etc/httpd/conf/httpd.conf** y localice lo siguiente:

```
AddDefaultCharset UTF-8
```

Cambie lo anterior por esto otro:

```
AddDefaultCharset Off
```

57.4.3. Ficheros de configuración.

Cualquier ajuste que se requiera realizar, ya sea para configurar Sitios de Red virtuales u otra funcionalidad adicional, se puede realizar sin tocar el fichero principal de configuración, utilizando cualquier fichero con extensión ***.conf** dentro del directorio **/etc/httpd/conf.d/.**

57.4.4. Directorios virtuales.

Si, por ejemplo, se quisiera añadir el alias para un directorio localizado en **/var/ftp/pub/** y el cual queremos visualizar como el directorio **/pub/** en Apache, solo bastaría crear un fichero que denominaremos arbitrariamente como el fichero denominado **/etc/httpd/conf.d/aliases.conf** con el siguiente contenido:

```
Alias  /pub  /var/ftp/pub
```

Si trata de acceder hacia este nuevo directorio virtual con el navegador, notará que no está permitido el acceso. Para poder acceder deberá haber un documento índice en el interior (index.html, index.php, etc) o bien que dicho directorio sea configurado para mostrar el contenido del siguiente modo:

```
Alias /pub /var/ftp/pub
        <Directory "/var/ftp/pub">
                Options Indexes Includes FollowSymLinks
                AllowOverride all
        </Directory>
```

El parámetro **Indexes** indica que se deberá mostrar el contenido del directorio. El parámetro **FollowSymLinks** posibilita poder colocar enlaces simbólicos dentro del directorio los cuales se seguirán. El parámetro **Includes** especifica que se permite la utilización de los SSI (Server Side Includes) que posibilitan utilizar funciones como autenticación. El parámetro **AllowOverrride all** posibilita utilizar ficheros **.htaccess**.

Reinicie o recargue Apache y acceda hacia *http://127.0.0.1/pub/* con cualquier navegador de red y visualice el resultado.

57.4.5. Redirección de directorios.

Cuando sea necesario, es posible configurar un directorio en particular para Apache redirija de modo transparente éste y su contenido hacia cualquier otra dirección.

```
Redirect 301 /webmail http://mail.su-dominio.net/
```

En el ejemplo anterior, se indica que si se trata de acceder hacia el subdirectorio **/webmail** en el servidor, Apache deberá redirigir hacia *http://mail.su-dominio.net/*. El número 301 corresponde al mensaje del protocolo HTTP para indicar que la redirección es permanente. Si por ejemplo hubiese un objeto en /webmail, como por ejemplo **/webmail/estadisticas/estadisticas.php**, Apache realizará el re-direccionamiento transparente hacia *http://mail.su-dominio.net/estadisticas/estadisticas.php*.

57.4.6. Tipos de MIME.

Si por ejemplo se quisiera añadir algún tipo de extensión y tipo MIME, como por ejemplo Ogg, se podría generar un fichero que denominaremos arbitrariamente como el fichero **/etc/httpd/conf.d/extensiones.conf** con el siguiente contenido:

```
AddType application/ogg .ogg
AddDescription "Ogg Vorbis Audio" .ogg
AddIcon /icons/sound2.png .ogg
```

57.4.7. Soporte para CGI con extensión *.cgi

Si se quisiera añadir que se reconociera la extensión ***.cgi** como un guión **CGI** (**C**ommon **G**ateway **I**nterface), solo bastará añadir un fichero que denominaremos, arbitrariamente, **/etc/httpd/conf.d/cgi.conf** con el siguiente contenido:

```
AddHandler cgi-script .cgi
```

57.4.7.1. Probando la configuración.

Utilice el editor de texto de su preferencia para crear el fichero **/var/www/cgi-bin/tiempo.cgi**. Este deberá llevar lo siguiente como contenido:

```
#!/usr/bin/perl
print "content-type: text/html\n\n";
print scalar localtime;
print "\n";
```

Deberemos de cambiar el permiso del archivo anterior con la siguiente línea de mandato:

```
chmod 755 /var/www/cgi-bin/tiempo.cgi
```

Utilice el navegador de red que prefiera y apunte éste hacia *http://127.0.0.1/cgi-bin/tiempo.cgi*. Si el navegador nos da una salida similar a la siguiente, se habrá configurado exitosamente Apache® para ejecutar guiones CGI:

```
Tue Jul 05 22:10:41 2005
```

57.4.7.2. Problemas posteriores

Antes escribirle al autor de este documento, de recurrir a las listas de soporte o grupos y foros de discusión solicitando ayuda para hacer trabajar un guión CGI en particular, lea cuidadosamente la documentación que acompaña a este y verifique que se han establecido apropiadamente los permisos de lectura, escritura y ejecución, que se han realizado las modificaciones necesarias en los parámetros para el uso del guión en su servidor y que el guión CGI no contenga errores. Recurra al autor de guión CGI o binario si necesita ayuda.

57.4.7.3. Error más común número 1.

```
Forbidden
You don't have permission to access /algun/directorio/guion.cgi on this server
```

Significa que el archivo no cuenta con los permisos apropiados de lectura, escritura y ejecución. La mayoría guiones CGI que encontrará en Internet necesitarán al menos permiso **755** para poder ser utilizados.

57.4.7.4. Error más común número 2.

```
Internal Server Error
The server encountered an internal error or misconfiguration and was unable to complete
your request.
```

Significa que hay problemas con el guión CGI en si y no con Apache®. En la mayoría de los casos se trata de ficheros que fueron elaborados desde un editor de texto en Windows®, cuyo retorno de carro es distinto al de los sistemas operativos basados sobre UNIX®, por lo cual se deberá utilizar el mandato **dos2unix** sobre dichos ficheros. En otros casos, algo menos frecuente, se requerirá que el administrador revise línea por línea para localizar un posible error o parámetro incorrecto. Cuando aplique, verifique que la primera línea del guión que apunta hacia donde se encuentra el mandato **perl** sea correcta. Verifique también si el directorio que albergue el guión CGI requiere algún permiso en particular, como sería 777 en el caso de algunos guiones CGI.

57.4.8. Robo de imágenes.

Suele ocurrir que los administradores de algunos sitios encuentran fácil utilizar imágenes, y otros tipos de contenido, vinculando desde sus documentos hacia los objetos en el servidor. Esto consume ancho de banda adiconal y es una práctica poco ética. En el siguiente ejemplo, considerando que se tiene un directorio **/var/www/html/imagenes**, y se desea proteger éste para que solo se permita utilizar su contenido si es referido desde el mismo servidor, se utilizaría lo siguiente:

```
# Se permite al propio servidor
SetEnvIf Referer "^http://www.midominio.org/" local_referal
# se permite aceder directamente a la imagen o bien si
# no se especifica en el navegador la información de referente.
SetEnvIf Referer "^$" local_referal
<Directory  "/var/www/html/imagenes/">
        Order Deny,Allow
        Deny from all
        Allow from env=local_referal
</Directory>
```

La configuración anterior puede añadirse en cualqueir fichero *.conf dentro del directorio

/etc/httpd/conf.d/.

57.5. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir el puerto 80 por TCP (**HTTP**).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     80
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

57.6. Apéndice: Configuración de Sitios de Red virtuales en Apache.

Puede generarse cualquier fichero con extensión **.conf* dentro del directorio */etc/httpd/conf.d/* de Apache® 2.0.x. Puede incluirse contenido como el siguiente:

```
# Definición del Sitio de Red principal
NameVirtualHost 192.168.1.254
<VirtualHost 192.168.1.254>
        ServerAdmin webmaster@dominio.com
        DocumentRoot /var/www/html/
        ServerName www.dominio.com
</VirtualHost>

# Web virtual con definición de directorio para CGI
<VirtualHost 192.168.1.254>
        DocumentRoot /var/www/lpt/html
        ServerName www.algun-dominio.com
        ServerAlias algun-dominio.com
        ServerAdmin webmaster@algun-dominio.com
        ErrorLog /var/www/algun-dominio/logs/error_log
        CustomLog /var/www/algun-dominio/logs/access_log combined
        ScriptAlias /cgi-bin/ "/var/www/algun-dominio/cgi-bin/"
        <Directory "/var/www/algun-dominio/cgi-bin">
                AllowOverride None
                Options None
                Order allow,deny
                Allow from all
        </Directory>
        AddHandler cgi-script .cgi
</VirtualHost>


# Más Sitios de Red virtuales

<VirtualHost 192.168.1.254>
        ServerAdmin webmaster@dominio.com
        DocumentRoot /usr/share/squirrelmail/
        ServerName webmail.dominio.com
        ErrorLog logs/webmail.dominio.com-error_log
        CustomLog logs/webmail.dominio.com-access_log combined
</VirtualHost>

<VirtualHost 192.168.1.254>
        ServerAdmin webmaster@beta.dominio.com
        DocumentRoot /var/www/beta/
        ServerName beta.dominio.com
        ErrorLog /var/www/beta/logs/beta.dominio.com-error_log
        CustomLog /var/www/beta/logs/beta.dominio.com-access_log combined
</VirtualHost>

<VirtualHost 192.168.1.254>
        ServerAdmin webmaster@dominio.com
        DocumentRoot /usr/share/squirrelmail/
        ServerName mail.dominio.com
        ErrorLog logs/mail.dominio.com-error_log
```

```
        CustomLog logs/mail.dominio.com-access_log combined
</VirtualHost>

<VirtualHost 192.168.1.254>
        ServerAdmin webmaster@dominio.net
        DocumentRoot /var/www/net/
        ServerName www.dominio.net
        ErrorLog /var/www/net/logs/www.dominio.net-error_log
        CustomLog /var/www/net/logs/www.dominio.net-access_log combined
</VirtualHost>
```

58. Cómo habilitar los ficheros .htaccess y SSI) Server Side Includes) en Apache 2.x.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

58.1. Introducción.

Apache® 2.x tiene mejores medidas de seguridad que las versiones anteriores, debido a que su configuración predeterminada viene de tal modo que deshabilita muchas cosas que podrán considerarse de cierto riesgo. Parte de esa seguridad incluye deshabilitar los **SSI** (**S**erver **S**ide **I**ncludes o Inclusiones del Lado del Servidor) y el uso de los ficheros **.htaccess**. Estos últimos sirven para modificar o agregar funciones a directorios.

Básicamente solo se necesita agregar las siguientes líneas a cualquier definición del directorio que se desee utilizar:

```
Options Includes
AllowOverride All
```

58.2. Procedimientos.

58.2.1. Autenticación de directorios.

La autenticación para un directorio, contra un fichero que incluye claves de acceso, se realiza a través de la siguiente sintaxis en cualquier fichero **.htaccess**.

```
AuthName "Acceso solo usuarios autorizados"
AuthType Basic
require valid-user
AuthUserFile /cualquier/ruta/hacia/fichero/de/claves
```

58.2.1.1. Ejemplo.

Se procede a crear un directorio que será visto desde cualquier navegador como *http://127.0.0.1/privado/*.

Genere el fichero **/etc/httpd/conf.d/ejemplo-autenticar.conf** con el siguiente contenido:

```
Alias /privado /var/www/privado
<Directory "/var/www/privado">
        Options Includes
        AllowOverride All
```

```
        Order allow,deny
        Allow from all
</Directory>
```

Genere el directorio **/var/www/privado/** realizando lo siguiente:

```
mkdir -p /var/www/privado
```

Genere el fichero **/var/www/privado/.htaccess** realizando lo siguiente:

```
touch /var/www/privado/.htaccess
```

Edite el fichero **/var/www/privado/.htaccess** y agregue el siguiente contenido:

```
AuthName "Solo usuarios autorizados"
AuthType Basic
require valid-user
AuthUserFile /var/www/claves
```

Genere el fichero de claves de acceso como **/var/www/claves**, utilizando el siguiente procedimiento:

```
touch /var/www/claves
```

Con el fin de establecer la seguridad necesaria, cambie los atributos de lectura y escritura solo para el usuario **apache**:

```
chmod 600 /var/www/claves
chown apache:apache /var/www/claves
```

Agregue algunos **usuarios virtuales** al fichero de claves, **/var/www/claves**, utilizando el siguiente procedimiento con el mandato **htpasswd**:

```
htpasswd /var/www/claves fulano
htpasswd /var/www/claves mengano
```

Reinicie el servicio **httpd**:

```
service httpd restart
```

Acceda con cualquier navegador de red hacia *http://127.0.0.1/privado/* y compruebe que funciona el acceso con autenticación en dicho subdirectorio utilizando cualquiera de los dos usuarios virtuales que generó con el mandato **htpasswd**, es decir fulano o mengano.

```
lynx http://127.0.0.1/privado/
```

58.2.2. Asignación de directivas para PHP.

Suelen darse los casos donde una aplicación, escrita en **PHP**, requiere algunas directivas de **PHP** en particular. En muchos casos se llegan a necesitar variables que pueden comprometer la seguridad

de otras aplicaciones hospedadas en el servidor. Para tal fin es que se puede evitar modificar el fichero **/etc/php.ini** utilizando el parámetro **php_flag** en un fichero **.htaccess**. La siguiente sintaxis es la siguiente:

```
php_flag directiva_php valor
```

58.2.2.1. Ejemplo

Se procederá a asignar las directivas **register_globals**, **magic_quotes_runtime**, **magic_quotes_gpc**, y **upload_max_filesize** al directorio en la ruta **/var/www/aplicacion**, mismo que será visualizado desde Apache como *http://127.0.0.1/aplicacion/*. El valor para **register_globals** será **On**, el valor para **magic_quotes_runtime** será **On**, el valor para **magic_quotes_gpc** será **On** y el valor para **upload_max_filesize** será **4M**.

Genere el fichero **/etc/httpd/conf.d/ejemplo-directivas-php.conf** con el siguiente contenido:

```
Alias /aplicacion /var/www/aplicacion
<Directory "/var/www/aplicacion">
        Options Includes
        AllowOverride All
        Order allow,deny
        Allow from all
</Directory>
```

Genere el fichero **/var/www/aplicacion/.htaccess** realizando lo siguiente:

```
touch /var/www/aplicacion/.htaccess
```

Edite el fichero **/var/www/aplicacion/.htaccess** y agregue el siguiente contenido:

```
php_flag register_globals On
php_flag magic_quotes_gpc On
php_flag magic_quotes_runtime On
php_value upload_max_filesize 4M
```

Genere el fichero **/var/www/aplicacion/info.php**, una función que muestra toda la información acerca de **PHP** en el servidor, a fin de corroborar los valores de las directivas de **PHP** en relación al directorio, con el siguiente contenido:

```
<?phpinfo()?>
```

Reinicie el servicio **httpd**:

```
service httpd restart
```

Acceda con cualquier navegador de red hacia *http://127.0.0.1/aplicacion/info.php* y corrobore que los valores para las variables de **PHP** para el directorio involucrado realmente han sido asignadas. En la sub-sección **PHP Core** de la sección **Configuration**, hay tres columnas: **Directive**, el cual corresponde a la directivas **PHP**, **Local Value**, el cual corresponde a los valores de las directivas de **PHP** para el directorio actual, y **Master Value**, que corresponde a los valores de las directivas generales como están definidas en el fichero **/etc/php.ini**.

Directive	Local Value	Master Value
magic_quotes_gpc	On	Off
magic_quotes_runtime	On	Off
register_globals	On	Off
upload_max_filesize	4M	4M

59. Cómo configurar Apache con soporte SSL/TLS.

Autor: *Joel Barrios Dueña*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

59.1. Introducción.

59.1.1. Acerca de HTTPS.

HTTPS es la versión segura del protocolo **HTTP**, inventada en 1996 por Netscape Communications Corporation. No es un protocolo separado de **HTTP**. Se trata de una combinación de este último con un mecanismo de transporte **SSL** o **TLS**, garantizando una protección razonable durante la comunicación cliente-servidor. Es ampliamente utilizado en la red mundial (**WWW** o **W**orld **W**ide **W**eb) para comunicaciones como transacciones bancarias y pago de bienes y servicios.

El servicio utiliza el puerto 443 por TCP para realizar las comunicaciones (la comunicación normal para HTTP utiliza el 80 por TCP). El esquema **URI** (**U**niform **R**esource **I**dentifier o Identificador Uniforme de Recursos) es, comparando sintaxis, idéntico al de **HTTP** (http:), utilizándose como **«https:»** seguido del subconjunto denominado **URL** (**U**niform **R**esource **L**ocator o Localizador Uniforme de Recursos). Ejemplo: *https://www.dominio.org/*

URL: http://es.wikipedia.org/wiki/HTTPS y http://wp.netscape.com/eng/ssl3/draft302.txt

59.1.2. Acerca de RSA.

RSA, acrónimo de los apellidos de sus autores, Ron **R**ivest, Adi **S**hamir y Len **A**dleman, es un algoritmo para el cifrado de claves públicas que fue publicado en 1977, patentado en EE.UU. en 1983 por el el Instituto Tecnológico de Michigan (**MIT**). **RSA** es utilizado ampliamente en todo el mundo para los protocolos destinados para el comercio electrónico.

URL: http://es.wikipedia.org/wiki/RSA

59.1.3. Acerca de Triple DES.

Triple DES, o **TDES**, es un algoritmo que realiza un triple cifrado DES, desarrollado por IBM en 1978. Su origen tuvo como finalidad el agrandar la longitud de una clave sin necesidad de cambiar el algoritmo de cifrado, lo cual lo hace más seguro que el algoritmo **DES**, obligando a un atacante el tener que triplicar el número de operaciones para poder hacer daño. A pesar de que actualmente está siendo reemplazado por el algoritmo **AES** (**A**dvanced **E**ncryption **S**tandard, también conocido como **Rijndael**), sigue siendo estándar para las tarjetas de crédito y operaciones de comercio electrónico.

URL: http://es.wikipedia.org/wiki/Triple_DES

59.1.4. Acerca de X.509.

X.509 es un estándar **ITU-T** (estandarización de **T**elecomunicaciones de la **I**nternational **T**elecommunication **U**nion) para infraestructura de claves públicas (**PKI**, o **P**ublic **K**ey **I**nfrastructure). Entre otras cosas, establece los estándares para certificados de claves públicas y un algoritmo para validación de ruta de certificación. Este último se encarga de verificar que la ruta de un certificado sea válida bajo una infraestructura de clave pública determinada. Es decir, desde el certificado inicial, pasando por certificados intermedios, hasta el certificado de confianza emitido por una Autoridad Certificadora (**CA**, o **C**ertification **A**uthority).

URL: http://es.wikipedia.org/wiki/X.509

59.1.5. Acerca de OpenSSL.

OpenSSL es una implementación libre, de código abierto, de los protocolos **SSL** (**S**ecure **S**ockets **L**ayer o Nivel de Zócalo Seguro) y **TLS** (**T**ransport **L**ayer **S**ecurity, o Seguridad para Nivel de Transporte). Está basado sobre el extinto proyecto **SSLeay**, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation.

URL: http://www.openssl.org/

59.1.6. Acerca de mod_ssl.

Mod_ssl es un módulo para el servidor HTTP Apache, el cual provee soporte para SSL versiones 2 y 3 y TLS versión 1. Es una contribución de Ralf S. Engeschall, derivado del trabajo de Ben Laurie.

URL: http://www.apache-ssl.org/ y http://httpd.apache.org/docs/2.2/mod/mod_ssl.html

59.2. Requisitos.

Es necesario disponer de una dirección IP pública para cada sitio de red virtual que se quiera configurar con soporte **SSL**/**TLS**. Debido a la naturaleza de los protocolos **SSL** y **TLS**, no es posible utilizar múltiples sitios de red virtuales con soporte **SSL**/**TLS** utilizando una misma dirección IP. Cada certificado utilizado requerirá una dirección IP independiente en el sitio de red virtual.

El paquete mod_ssl instala el fichero **/etc/httpd/conf.d/ssl.conf**, mismo que no es necesario modificar, puesto que se utilizarán ficheros de inclusión, con extensión *.conf, dentro del directorio **/etc/httpd/conf.d/**, a fin de respetar la configuración predeterminada y podre contar con la misma, que es funcional, brindando un punto de retorno en el caso de que algo saliera mal.

59.3. Equipamiento lógico necesario.

59.3.1. Instalación a través de yum.

Si se utiliza de CentOS 4 o White Box Enterprise Linux 4, se ejecuta lo siguiente:

```
yum -y install mod_ssl
```

59.3.2. Instalación a través de Up2date

Si se utiliza de Red Hat™ Enterprise Linux 4, se ejecuta lo siguiente:

```
up2date -i mod_ssl
```

59.4. Procedimientos.

Acceda al sistema como el usuario **root**.

Se debe crear el directorio donde se almacenarán los certificados para todos los sitios SSL. El directorio, **por motivos de seguridad**, debe ser solamente accesible para el usuario **root**.

```
mkdir -m 0700 /etc/ssl
```

A fin de mantener cierta organización, y un directorio dedicado para cada sitio virtual SSL, es conveniente crear un directorio específico para almacenar los certificados de cada sitio virtual SSL. Igualmente, **por motivos de seguridad**, debe ser solamente accesible para el usuario **root**.

```
mkdir -m 0700 /etc/ssl/midominio.org
```

Acceder al directorio que se acaba de crear.

```
cd /etc/ssl/midominio.org
```

59.4.1. Generando clave y certificado.

Se debe crear una clave con algoritmo **RSA** de 1024 octetos y estructura **x509**, la cual se cifra utilizado **Triple DES** (**D**ata **E**ncryption **S**tandard), almacenado en formato **PEM** de modo que sea interpretable como texto ASCII. En el proceso descrito a continuación, se utilizan 5 ficheros comprimidos con **gzip**, que se utilizan como semillas aleatorias que mejoran la seguridad de la clave creada (server.key).

```
openssl genrsa -des3 -rand \
fichero1.gz:fichero2.gz:fichero3.gz:fichero4.gz:fichero5.gz \
-out server.key 1024
```

Si se utiliza este fichero (server.key) para la configuración del sitio virtual, se requerirá de interacción del administrador cada vez que se tenga que iniciar, o reiniciar, el servicio httpd, ingresando la clave de acceso de la clave **RSA**. Este es el procedimiento más seguro, sin embargo, debido a que resultaría poco práctico tener que ingresar una clave de acceso cada vez que se inicie el servicio httpd, resulta conveniente generar una clave sin **Triple DES**, la cual permita iniciar normalmente, sin interacción alguna, al servicio httpd. A fin de que no se sacrifique demasiada seguridad, es un requisito indispensable que esta clave (fichero server.pem) solo sea accesible para **root**. Ésta es la razón por la cual se crea el directorio **/etc/ssl/midominio.org** con permiso de acceso solo para **root**.

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

Opcionalmente se genera un fichero de petición **CSR** (**C**ertificate **S**igning **R**equest) que se hace llegar a una **RA** (**R**egistration **A**uthority o Autoridad de Registro), como **Verisign**, quienes, tras el correspondiente pago, envían de vuelta un certificado (server.crt) firmado por dicha autoridad.

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

Lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o razón social.
- Unidad o sección.
- Nombre del anfitrión.
- Dirección de correo.
- Opcionalmente se puede añadir otra clave de acceso y nuevamente el nombre de la empresa.

La salida devuelta sería similar a la siguiente:

```
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:Mexico
Organization Name (eg, company) [My Company Ltd]:
Mi empresa, S.A. de C.V.
Organizational Unit Name (eg, section) []:Direccion Comercial
Common Name (eg, your name or your server's hostname) []:
www.midominio.org
Email Address []:webmaster@midominio.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Si no se desea un certificado firmado por un **RA**, puede generarse uno certificado propio utilizando el fichero de petición **CSR** (server.csr). En el ejemplo a continuación, se crea un certificado con estructura X.509 en el que se establece una validez por 730 días (dos años).

```
openssl x509 -req -days 730 -in server.csr \
-signkey server.key -out server.crt
```

Con la finalidad de que solo el usuario **root** pueda acceder a los ficheros creados, se deben cambiar los permisos de éstos a solo lectura para **root**.

```
chmod 400 /etc/ssl/midominio.org/server.*
```

59.4.2. Configuración de Apache.

Crear la estructura de directorios para el sitio de red virtual.

```
mkdir -p /var/www/midominio.org/
```

De todos directorios creados, solo **/var/www/midominio.org/html**, **/var/www/midominio.org/etc**, **/var/www/midominio.org/cgi-bin** y **/var/www/midominio.org/var** pueden pertenecer al usuario, sin privilegios, que administrará éste sitio de red virtual. Por motivos de seguridad, y a fin de evitar que el servicio HTTPD no sea trastornado en caso de un borrado accidental de algún directorio, tanto **/var/www/midominio.org/** como **/var/www/midominio.org/logs**, deben pertenecer al usuario **root**.

Crear el fichero **/etc/httpd/conf.d/midominio.conf** con el siguiente contenido, donde **a.b.c.d** corresponde a una dirección IP, y **midominio.org** corresponde al nombre de dominio a configurar para el sitio de red virtual:

```
### midominio.org ###
NameVirtualHost a.b.c.d:80
        <VirtualHost a.b.c.d:80>
                ServerAdmin webmaster@midominio.org
                DocumentRoot /var/www/midominio.org/html
                ServerName www.midominio.org
                ServerAlias midominio.org
                Redirect 301 / https://www.midominio.org/
                CustomLog /var/www/midominio.org/logs/access_log combined
                Errorlog /var/www/midominio.org/logs/error_log
        </VirtualHost>

NameVirtualHost a.b.c.d:443
        <VirtualHost a.b.c.d:443>
                ServerAdmin webmaster@midominio.org
                DocumentRoot /var/www/midominio.org/html
                ServerName www.midominio.org
                ScriptAlias /cgi-bin/ /var/www/midominio.org/cgi-bin/
                SSLEngine on
                SSLCertificatefile /etc/ssl/midominio.org/server.crt
                SSLCertificateKeyfile /etc/ssl/midominio.org/server.pem
                SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
                CustomLog /var/www/midominio.org/logs/ssl_request_log \
                        "%t %h %x %x \"%r\" %b"
                CustomLog /var/www/midominio.org/logs/ssl_access_log combined
                Errorlog /var/www/midominio.org/logs/ssl_error_log
        </VirtualHost>
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **httpd**.

```
service httpd restart
```

59.4.3. Comprobación.

Solo basta dirigir cualquier navegador HTTP hacia **https://www.midominio.org/** a fin de verificar que todo esté trabajando correctamente. Tras aceptar el certificado, en el caso de que éste no haya sido firmado por un **RA**, deberá poderse observar un signo en la barra de estado del navegador, el

cual indica que se trata de una conexión segura.

59.4.4. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir, además del puerto 80 por TCP (**HTTP**), el puerto 443 por TCP (**HTTPS**).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     80,443
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

60. Cómo instalar y configurar Geeklog 1.4.x.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

60.1. Introducción.

60.1.1. Acerca de Geeklog.

Geeklog es una aplicación basada sobre PHP y MySQL, y distribuida bajo los términos de la licencia GNU/GPL, para el manejo dinámico de contenido de red. Sin modificaciones tras su instalación, es un motor de bitácora personal, Sistema de Manejo de Contenido (CMS o **C**ontent **M**anagement **S**ystem) y/o portal de red. Incluye soporte para comentarios, rastreo (o *tracback*, un método para solicitar notificación cuando alguien enlaza hacia un documento), varios formatos de sindicación (es decir, **RSS** o **R**eally **S**imple **S**indication), protección contra Spam y todas las funciones básicas para contar con un sitio de red dinámico y versátil.

Gracias a la plataforma para componentes añadidos (Plug-ins), su funcionalidad puede ser fácilmente extendida con foros, galerías de e imágenes, área de descargas y muchas otras cosas más.

URL: http://www.geeklog.net/

60.1.2. ¿Por qué Geeklog?

Geeklog fue diseñado con la seguridad como prioridad, siendo que su utilización inicial fue precisamente un sitio de seguridad. Las vulnerabilidades son poco frecuentes y los guiones que explotan vulnerabilidades (exploits), que aún funcionen, son raros de encontrar. Una de las grandes ventajas de **Geeklog** contra otro tipo de equipamiento lógico similar, es su esquema de permisos de usuario. Es posible asignar permisos de lectura y/o escritura a un usuario o grupo de usuarios, y hacer que estos usuarios hereden permisos al ser añadidos a un grupo o grupos. Esta funcionalidad cubre los requisitos necesarios para ser utilizado en redes internas en empresas y corporaciones.

Geeklog, además, se enfoca en la calidad del código utilizado, así como también asegurarse que los **API** (**A**pplication **P**rogramming **I**nterface o Interfaz de Programación de Aplicaciones) utilizados, no estropeen componentes añadidos (plug-ins) de terceros tras una actualización, a menos que el caso realmente lo requiera. De tal modo, es posible continuar utilizando componentes creados por terceros para versiones anteriores de Geeklog, y sin embargo estos casi por seguro funcionarán correctamente con la versión más reciente, salvo aquellos que utilicen el sistema de comentarios, mismo que fue rediseñado a partir de la versión 1.4.0.

60.2. Aspectos de seguridad a considerar.

Geeklog es uno de los Sistemas de Manejo de Contenido más seguros y confiables, sin embargo no significa que sea invulnerable. Hay varios aspectos a considerar, los cuales aplicados de forma

correcta pueden mejorar considerablemente la seguridad.

60.2.1. Prefijo de las tablas de Geeklog.

Una de las principales consideraciones que se deben tomar en cuenta es que la mayoría de los guiones disponibles para explotar vulnerabilidades (exploits) indudablemente presupondrán el prefijo de las tablas de Geeklog para lograr su cometido. es decir, el valor de la variable **$_DB_table_prefix**, el cual de forma predeterminada es **gl_**. La mejor forma de impedir ser susceptible a guiones explotables, es cambiar dicho valor por cualquier otro, preferentemente que combine letras y números de forma que sea difícil para un delincuente informático adivinar éste.

60.2.2. Rutas de los directorios de Geeklog.

La siguiente consideración es la localización de los directorios utilizados por **Geeklog** en el sistema. Conviene instalar el directorio público fuera del directorio raíz de apache, es decir, que no esté dentro de **/var/www/html**. La forma de hacer esto es colocando el directorio público en una ruta como **/var/www/nombre_ofuscado** y definiendo dicho directorio como uno virtual en la configuración de Apache.

El directorio de configuración de Geeklog, del mismo modo, y con mayor razón, jamás debe quedar dentro del directorio raíz de Apache. Debe ser instalado en cualquier parte del sistema, como por ejemplo **/var/www/nombre_ofuscado**, y, a diferencia del directorio público, jamás deberá poder accederse desde el navegador.

Muchos guiones explotables pueden hacer daño si se conoce la ruta exacta en el sistema para diversos componentes de **Geeklog**.

60.2.3. Desactivar el despliegue de errores de PHP.

La función **display_errors** función viene deshabilitada de forma predeterminada en el fichero **php.ini**, sin embargo muchos administradores suelen habilitarla para realizar diagnósticos y pruebas. En realidad, jamás se debe habilitar ésta si se trata de un servidor en producción, porque hará que se muestre en el navegador información que puede ser utilizada en un guión explotable, como son rutas en el sistema de archivo y prefijos de tablas en la base de datos.

Cuando se está hospedado en un servidor con esta función habilitada, se puede recurrir a variables en ficheros **.htaccess** del siguiente modo:

```
php_flag display_errors Off
```

60.3. Equipamiento lógico necesario.

Geeklog requiere algunos componentes para poder funcionar. Específicamente se necesitan **Apache**, **MySQL**, **PHP** y el soporte de **MySQL** para **PHP**.

60.3.1. Instalación a través de yum.

Si se utiliza de **CentOS 4** o **White Box Enterprise Linux 4**, solo se necesita utilizar utilizar lo siguiente:

```
yum -y install httpd php php-mysql mysql-server
```

60.3.2. Instalación a través de Up2date

Si se utiliza de **Red Hat™ Enterprise Linux 4**, solo se necesita utilizar lo siguiente:

```
up2date -i httpd php php-mysql mysql-server
```

60.4. Procedimientos

Este documento considera las siguientes variables que deberán ser reemplazadas por valores reales:

- **nueva-clave-de-acceso**: una clave de acceso que asignará a el suaurio root de MySQL en caso de que se trate de una nueva instalación de MySQL.
- **base-de-datos**: Nombre que tendrá la base de datos que se creará para Geeklog.
- **usuario-geeklog**: Nombre del usuario que se utilizará para acceder hacia la base de datos en MySQL y que utilizará Geeklog. Debe ser un nombre de menos de 12 caracteres.
- **clave-de-acceso**: Clave de acceso que se utilizará para acceder a la base de datos en MySQL y que utilizará Geeklog.
- **www.dominio.algo**: Dirección IP o nombre de anfitrión del sistema.
- **alguien@algo.algo**: Cuenta de correo electrónico del usuario administrador.

Arranque de servicios.

Se requiere iniciar los servicios httpd y mysqld.

```
/sbin/service httpd start
```

Si es la primera vez que se inicia **MySQL**, inicie también el servicio **mysqld**.

```
/sbin/service mysqld start
```

Si es la primera vez que utiliza **MySQL** y no se ha asignado clave de acceso para el usuario **root** en **MySQL**, este es buen momento para hacerlo. Es inaporpiado dejar sin clave de acceso al usuario root en MYSQL. Defina una buena clave de acceso que pueda recordar y utilice el siguiente procedimiento:

```
mysqladmin -u root password 'nueva-clave-de-acceso'
```

Los servicios httpd y mysqld se agregan al arranque del sistema utilizando lo siguiente:

```
/sbin/chkconfig httpd on
/sbin/chkconfig mysqld on
```

60.4.1. Instalación de Geeklog.

Geeklog se distribuye en archivos TAR comprimidos con algoritmo Gzip. Una vez descargado desde http://www.geeklog.net/, solo se necesita utilizar el **Gestor de archivadores** (file-roller) desde el modo gráfico, o bien, si solo se dispone de una terminal, la siguiente sentencia de mandatos:

```
tar zxvf geeklog-1.4.1.tar.gz
```

Lo anterior genera un directorio nuevo denominado **geeklog-1.4.1**, bajo el cual están todos los componentes de Geeklog.

60.5. Procedimientos.

60.5.1. Respaldo de la base de datos existente.

Si va a ser utilizada una base de datos existente, conviene respaldar ésta antes de continuar.

```
mysqldump --opt -u root -p base-de-datos > respaldo-base-de-datos.sql
```

Para restaurar el respaldo, se utiliza lo siguiente:

```
mysql -u root -p base-de-datos < respaldo-base-de-datos.sql
```

60.5.2. Creación de la base de datos para Geeklog en MySQL.

Deben definirse previamente tres valores a utilizar con **Geeklog**: nombre de la base de datos, usuario para acceder a esta base de datos y clave de acceso para este usuario. Éstos, preferentemente, deben ser valores difíciles de adivinar para terceros.

Tomando en cuenta lo anterior, se crea la base de datos utilizando el mandato **mysqladmin**.

```
mysqladmin -u root -p create base-de-datos
```

Una vez creada la base de datos, se accede hacia el servidor de **MySQL** con el mandato **mysql**, con la finalidad de asignar permisos, usuario y clave de acceso.

```
mysql -u root -p
```

El usuario y clave de acceso necesarios se asignan del siguiente modo:

```
Welcome to the MySQL monitor.  Commands end with ; or g.
Your MySQL connection id is 4 to server version: 4.1.20

Type 'help;' or 'h' for help. Type 'c' to clear the buffer.

mysql> GRANT ALL ON base-de-datos.*
    -> TO usuario-geeklog@localhost
    -> IDENTIFIED BY 'clave-de-acceso';
mysql> exit
```

60.5.3. Configuración de directorios para Geeklog.

El directorio principal puede quedar en cualquier lugar del sistema de archivos, pero nunca dentro del directorio raíz de Apache, más sin embargo en una ruta a la cual tenga acceso éste último. Un buen lugar es dentro de **/var/www/** o bien **/etc**. Preferentemente utilizando un nombre de directorio ofuscado o bien algo difícil de adivinar.

```
mv geeklog-1.4.1 /var/www/conf_geeklog
```

EL directorio de configuración requiere que los subdirectorios **backup**, **data** y **logs** tengan permisos de escritura para el usuario **apache**. Puede hacerse asignando permiso 707 (drwx---rwx) a éstos, o bien, la forma más conveniente, asignándolos al usuario **apache** del siguiente modo:

```
chown -R apache.apache \
/var/www/conf_geeklog/{backups,data,logs}
```

El directorio público de Geeklog, es decir, **public_html**, también es conveniente esté fuera del directorio raíz de **Apache**. Un buen lugar es dentro de **/var/www/** o bien **/usr/share**.

```
mv /var/www/conf_geeklog/public_html \
/var/www/html_geeklog
```

El acceso desde Apache hacia este directorio conviene más que sea como directorio virtual. Para tal fin se añade la configuración correspondiente en Apache creando el fichero **/etc/httpd/conf.d/geeklog.conf**, considerando que **Geeklog** será accedido como *http://www.dominio.algo/portal/*, con el siguiente contenido:

```
        Alias /portal /var/www/html_geeklog/
```

Geeklog funciona perfectamente sin la variable **register_globals** habilitada, sin embargo algunos de los añadidos para **Geeklog** si lo requieren. Debido a que no es conveniente habilitar **register_globals** en todo el servidor **HTTP**, puede configurarse el directorio **/var/www/html_geeklog/** para permitir utilizar éste en donde sea necesario a través de un fichero **.htaccess**. Siendo así, la configuración en el fichero **/etc/httpd/conf.d/geeklog.conf** quedaría del siguiente modo:

```
        Alias /portal /var/www/html_geeklog/
        <Directory "/var/www/html_geeklog/">
                Options Includes
                AllowOverride all
        </Directory>
```

Para utilizar **register_globals** solo será necesario crear el fichero **/var/www/html_geeklog/.htaccess** con el siguiente contenido:

```
php_flag display_errors Off
php_flag register_globals On
```

El directorio público, hay varios directorios que deben permitir escritura para el usuario **apache**. Puede hacerse asignando permiso 707 (drwx---rwx) a éstos, o bien, la forma más conveniente, asignándolos al usuario **apache** del siguiente modo:

```
chown -R apache.apache \
/var/www/html_geeklog/images/{articles,library,topics,userphotos}

chown -R apache.apache \
/var/www/html_geeklog/backend
```

Para que surtan efectos los cambios y sea posible utilizar el fichero **.htaccess**, es necesario reiniciar el servicio **httpd**.

```
service httpd restart
```

Si no se desea interrumpir conexiones en el servicio **httpd**, se puede hacer que éste solo vuelva a leer la configuración y tomar los cambios, a través de la siguiente sentencia:

```
service httpd reload
```

60.5.4. Fichero lib-common.php.

Es el único fichero del directorio público que requiere modificarse, y es para establecer donde se encuentra el fichero **config.php** de **Geeklog**. Aproximadamente en la línea 84 de **/var/www/html_geeklog/lib-common.php** se encuentra una función **require_once** donde se debe establecer el valor **/var/www/conf_geeklog/config.php** del siguiente modo:

```
/**
* Configuration Include: You should ONLY have to modify this line.
* Leave the rest of this file intact!
*
* Make sure to include the name of the config file,
* i.e. the path should end in .../config.php
*/
require_once( '/var/www/conf_geeklog/config.php' );
```

60.5.5. Fichero config.php.

Se accede hacia el directorio **/var/www/conf_geeklog/**.

```
cd /var/www/conf_geeklog/
```

Se edita el fichero **config.php** y se definen los valores para las siguientes variables, considerando que se utilizará el idioma **español para México** y codificación **UTF-8** para el conjunto de caracteres:

$_DB_host	localhost
$_DB_name	**base-de-datos**
$_DB_user	**usuario-geeklog**
$_DB_pass	**clave-de-acceso**
$_DB_table_prefix	**e3f45g_** (cualquier prefijo, terminado en guión bajo, que no sea fácil de adivinar)
$_CONF['path']	**/var/www/conf_geeklog/**
$_CONF['path_html']	**/var/www/html_geeklog/**

$_CONF['site_url']	http://www.dominio.algo/portal (no debe llevar / al final)
$_CONF['site_admin_url']	http://www.dominio.algo/portal/admin (no debe llevar / al final)
$_CONF['site_mail']	alguien@algo.algo
$_CONF['site_name']	Nombre del portal
$_CONF['site_slogan']	Eslogan del portal
$_CONF['language']	spanish_utf-8
$_CONF['default_charset']	utf-8
$_CONF['locale']	es_MX.utf-8
$_CONF['rdf_language']	es-mx

Nuevamente, la mejor recomendación es que los valores para **$_DB_name**, **$_DB_user**, **$_DB_pass**, **$_DB_table_prefix**, **$_CONF['path']** y **$_CONF['path_html']** deben ser difíciles de adivinar para un atacante.

60.5.6. Instalador de Geeklog

Para concluir la instalación, es necesario acceder hacia *http://www.dominio.algo/portal/admin/install/install.php*, especificar la ruta para el fichero **config.php** (la cual, para el ejemplo de este documento, sería **/var/www/conf_geeklog/config.php**), habilitar la casilla para utilizar tablas **Innodb** y continuar dando clic en los botones de siguiente. Al terminar, Geeklog podrá ser accedido como *http://www.dominio.algo/portal/*, y solo restarán un par de ajustes más desde la recién instalada interfaz HTTP.

60.5.7. Procedimientos posteriores.

Hecho todo lo anterior, por motivos de seguridad, debe ser eliminado el directorio **/var/www/html_geeklog/admin/install/**.

```
rm -fr /var/www/html_geeklog/admin/install/
```

El usuario administrador predeterminado de **Geeklog** es **admin**, y la clave de acceso es **password**. Ambos deben ser cambiados accediendo hacia *http://www.dominio.algo/portal/admin/user.php?mode=edit&uid=2* y definiendo otro nombre de usuario y una nueva clave de acceso.

60.6. Problemas posteriores.

Si algo salió mal durante la instalación, es posible diagnosticarlo examinando las bitácoras de Apache, específicamente **/var/log/httpd/error_log**, o bien la bitácora de Geeklog, es decir, **/var/www/conf_geeklog/logs/error.log**. Los errores más comunes son errores tipográficos en las rutas de directorios o ficheros en el fichero de configuración, es decir, **/var/www/conf_geeklog/config.php**.

61. Cómo configurar un servidor de nombres de dominio (DNS)

Autor: *Joel Barrios Dueña*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

61.1. Introducción.

61.1.1. Bind (Berkeley Internet Name Domain)

BIND (acrónimo de **B**erkeley **I**nternet **N**ame **D**omain) es una implementación del protocolo DNS y provee una implementación libre de los principales componentes del Sistema de Nombres de Dominio, los cuales incluyen:

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

El Servidor DNS BIND es ampliamente utilizado en la Internet (99% de los servidores DNS) proporcionando una robusta y estable solución.

61.1.2. DNS (Domain Name System)

DNS (acrónimo de **D**omain **N**ame **S**ystem) es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombre de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. El **DNS** nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección **IP**.

Los **Servidores DNS** utilizan **TCP** y **UDP** en el puerto 53 para responder las consultas. Casi todas las consultas consisten de una sola solicitud **UDP** desde un **Cliente DNS** seguida por una sola respuesta **UDP** del servidor. **TCP** interviene cuando el tamaño de los datos de la respuesta exceden los 512 bytes, tal como ocurre con tareas como **transferencia de zonas**.

61.1.3. NIC (Network Information Center)

NIC (acrónimo de **N**etwork **I**nformation **C**enter o Centro de Información sobre la Red) es una institución encargada de asignar los nombres de dominio en Internet, ya sean nombres de dominio genéricos o por países, permitiendo personas o empresas montar sitios de Internet mediante a través de un **ISP** mediante un DNS. Técnicamente existe un **NIC** por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país. Por ejemplo: NIC México es la entidad encargada de gestionar todos los dominios con terminación

.mx, la cual es la terminación correspondiente asignada a los dominios de México.

61.1.4. FQDN (Fully Qualified Domain Name)

FQDN (acrónimo de **F**ully **Q**ualified **D**omain **N**ame o Nombre de Dominio Plenamente Calificado) es un Nombre de Dominio ambiguo que especifica la posición absoluta del nodo en el árbol jerárquico del DNS. Se distingue de un nombre regular porque lleva un punto al final.

Como ejemplo: suponiendo que se tiene un dispositivo cuyo nombre de anfitrión es «maquina1» y un dominio «dominio.com», el **FQDN** sería «**maquina1.dominio.com.**», de modo define de modo único al dispositivo mientras que pudieran existir muchos anfitriones llamados «maquina1», solo puede haber uno llamado «**maquina1.dominio.com.**». La ausencia del punto al final definiría que se pudiera tratar tan solo de un prefijo, es decir «**maquina1.dominio.com**» pudiera ser de un dominio más largo como «**maquina1.dominio.com.mx**».

La longitud máxima de un **FQDN** es de 255 bytes, con una restricción adicional de 63 bytes para cada etiqueta dentro del nombre del dominio. Solo se permiten los caracteres A-Z de ASCII, dígitos y el carácter «-». No se distinguen mayúsculas y minúsculas.

Desde 2004, a solicitud de varios países de Europa, existe el estándar **IDN** (acrónimo de **I**nternationalized **D**omain **N**ame) que permite caracteres no-ASCII, codificando caracteres **Unicode** dentro de cadenas de bytes dentro del conjunto normal de caracteres de **FQDN**. Como resultado, los limites de longitud de los nombres de dominio **IDN** dependen directamente del contenido mismo del nombre.

61.1.5. Componentes de un DNS

Los DNS operan a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

61.1.5.1. Clientes DNS

Son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres. Básicamente preguntan por la dirección IP que corresponde a un nombre determinado.

61.1.5.2. Servidores DNS

Son servicios que contestan las consultas realizadas por los **Clientes DNS**. Hay dos tipos de servidores de nombres:

· **Servidor Maestro (o primario)**	Obtiene los datos del dominio a partir de un fichero hospedado en el mismo servidor.
· **Servidor Esclavo (o secundario)**	Al iniciar obtiene los datos del dominio a través de un servidor un Servidor Maestro, realizando un proceso denominado **transferencia de zona**.

Un gran número de problemas de operación de servidores DNS se atribuyen a las pobres opciones de servidores secundarios pata las zona de DNS. De acuerdo al **RFC 2182**, el DNS requiere que **al menos tres servidores existan** para todos los dominios delegados (o zonas).

Una de las principales razones para **tener al menos tres servidores** para cada zona es permitir que la información de la zona misma esté disponible siempre y forma confiable hacia los **Clientes DNS** a través de Internet cuando un servidor DNS de dicha zona falle, no esté disponible y/o esté inalcanzable.

Contar con múltiples servidores también facilitan la **propagación** de la zona y mejoran la eficiencia del sistema en general la brindar opciones a los **Clientes DNS** si acaso encontraran dificultades para realizar una consulta en un **Servidor DNS**. En otras palabras: tener múltiples servidores para una zona permite **contar con redundancia y respaldo del servicio**.

Con múltiples servidores, por lo general uno actúa como **Servidor Maestro o Primario** y los demás como **Servidores Esclavos o Secundarios**. Correctamente configurados y una vez creados los datos para una zona, no será necesario copiarlos a cada **Servidor Esclavo o Secundario**, pues éste se encargará de transferir los datos de manera automática cuando sea necesario.

Los **Servidores DNS** responden dos tipos de consultas:

· **Consultas Iterativas (no recursivas)**	El cliente hace una consulta al **Servidor DNS** y este le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas locales. Si no es posible dar una respuesta, la consulta se reenvía hacia otro Servidor DNS repitiéndose este proceso hasta encontrar al **Servidor DNS** que tiene la **Zona de Autoridad** capaz de resolver la consulta.
· **Consultas Recursivas**	El **Servidor DNS** asume toda la carga de proporcionar la una respuesta completa para la consulta realizada por el **Cliente DNS**. El **Servidor DNS** desarrolla entonces **Consultas Iterativas** separadas hacia otros **Servidores DNS** (en lugar de hacerlo el **Cliente DNS**) para lograr la respuesta.

61.1.5.3. Zonas de Autoridad

Permiten al **Servidor Maestro o Primario** cargar la información de una zona. Cada **Zona de Autoridad** abarca al menos un dominio y posiblemente sus sub-dominios, si estos últimos no son delegados a otras zonas de autoridad.

La información de cada **Zona de Autoridad** es almacenada de forma local en un fichero en el **Servidor DNS**. Este fichero puede incluir varios tipos de registros:

Tipo de Registro	Descripción
A (**A**ddress)	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección **IPv4** de 32 bits.
AAAA	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección **IPv6** de 128 bits.
CNAME (**C**anonical **Name**)	Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtiene los sub-dominios y registros DNS del dominio original.
MX (**M**ail E**x**changer)	Registro de servidor de correo que sirve para definir una lista de servidores de correo para un dominio, así como la prioridad entre éstos.
PTR (**P**oin**t**e**r**)	Registro de apuntador que resuelve direcciones **IPv4** hacia el nombre anfitriones. Es decir, hace lo contrario al registro **A**. Se utiliza en zonas de **Resolución Inversa**.
NS (**N**ame **S**erver)	Registro de servidor de nombres que sirve para definir una lista de servidores de nombres con autoridad para un dominio.

Tipo de Registro	Descripción
SOA (**S**tart **of A**uthority)	Registro de inicio de autoridad que especifica el **Servidor DNS** Maestro (o Primario) que proporcionará la información con autoridad acerca de un dominio de Internet, dirección de correo electrónico del administrador, número de serie del dominio y parámetros de tiempo para la zona.
SRV (**S**e**rv**ice)	Registro de servicios que especifica información acerca de servicios disponibles a través del dominio. Protocolos como **SIP** (**S**ession **I**nitiation **P**rotocol) y **XMPP** (E**x**tensible **M**essaging and **P**resence **P**rotocol) suelen requerir registros **SRV** en la zona para proporcionar información a los clientes.
TXT (**T**e**xt**)	Registro de texto que permite al administrador insertar texto arbitrariamente en un registro DNS. Este tipo de registro es muy utilizado por los servidores de listas negras **DNSBL** (**DNS**-based **B**lackhole **L**ist) para la filtración de Spam. Otro ejemplo de uso son las VPN, donde suele requerirse un registro **TXT** para definir una llave que será utilizada por los clientes.

Las zonas que se pueden resolver son:

Zonas de Reenvío

Devuelven **direcciones IP** para las búsquedas hechas para nombres **FQDN** (**F**ully **Q**ualified **D**omain **N**ame).

En el caso de dominios públicos, la responsabilidad de que exista una **Zona de Autoridad** para cada **Zona de Reenvío** corresponde a la autoridad misma del dominio, es decir, y por lo general, quien esté registrado como autoridad del dominio tras consultar una base de datos **WHOIS**. Quienes compran dominios a través de un **NIC** (por ejemplo ejemplo: www.nic.mx) son quienes se hacen cargo de las **Zonas de Reenvío**, ya sea a través de su propio **Servidor DNS** o bien a través de los **Servidores DNS** de su **ISP**.

Salvo que se trate de un dominio para uso en una red local, todo dominio debe ser primero tramitado con un **NIC** como requisito para tener derecho legal a utilizarlo y poder propagarlo a través de Internet.

Zonas de Resolución Inversa

Devuelven nombres **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) para las búsquedas hechas para **direcciones IP**.

En el caso de segmentos de red públicos, la responsabilidad de que exista de que exista una **Zona de Autoridad** para cada **Zona de Resolución Inversa** corresponde a la autoridad misma del segmento, es decir, y por lo general, quien esté registrado como autoridad del segmento tras consultar una base de datos **WHOIS**.

Los grandes **ISP**, y en algunos casos algunas empresas, son quienes se hacen cargo de las **Zonas de Resolución Inversa**.

61.1.6. Herramientas de búsqueda y consulta

61.1.6.1. Mandato host

El mandato **host** una herramienta simple para hacer búsquedas en **Servidores DNS**. Es utilizada para convertir nombres en direcciones IP y viceversa.

De modo predefinido realiza las búsquedas en las **Servidores DNS** definidos en el fichero **/etc/resolv.conf**, pudiendo definirse opcionalmente el **Servidor DNS** a consultar.

```
host www.linuxparatodos.net
```

Lo anterior realiza una búsqueda en los **Servidores DNS** definidos en el fichero **/etc/resolv.conf** del sistema, devolviendo una dirección IP como resultado.

```
host www.linuxparatodos.net 200.33.146.217
```

Lo anterior realiza una búsqueda en los **Servidor DNS** en la dirección IP 200.33.146.217, devolviendo una dirección IP como resultado.

61.1.6.2. Mandato dig

El mandato **dig** (**d**omain **i**nformation **g**roper) es una herramienta flexible para realizar consultas en **Servidores DNS**. Realiza búsquedas y muestra las respuestas que son regresadas por los servidores que fueron consultados. Debido a su flexibilidad y claridad en la salida es que la mayoría de los administradores utilizan **dig** para diagnosticar problemas de DNS.

De modo predefinido realiza las búsquedas en las **Servidores DNS** definidos en el fichero **/etc/resolv.conf**, pudiendo definirse opcionalmente el **Servidor DNS** a consultar. La sintaxis básica sería:

```
dig @servidor nombre TIPO
```

Donde **servidor** corresponde al nombre o dirección IP del **Servidor DNS** a consultar, **nombre** corresponde al nombre del registro del recurso que se está buscando y **TIPO** corresponde al tipo de consulta requerido (ANY, A, MX, SOA, NS, etc.)

Ejemplo:

```
dig @200.33.146.209 linuxparatodos.net MX
```

Lo anterior realiza una búsqueda en el **Servidor DNS** en la dirección IP 200.33.146.209 para los registros **MX** para el dominio *linuxparatodos.net*.

```
dig linuxparatodos.net NS
```

Lo anterior realiza una búsqueda en los **Servidores DNS** definidos en el fichero **/etc/resolv.conf** del sistema para los registros **NS** para el dominio *linuxparatodos.net*.

```
dig @200.33.146.217 linuxparatodos.net NS
```

Lo anterior realiza una búsqueda en los **Servidor DNS** en la dirección IP 200.33.146.217 para los registros **NS** para el dominio *linuxparatodos.net*.

61.1.6.3. Mandato jwhois (whois).

El mandato **jwhois** es una herramienta de consulta a través de servidores **WHOIS**. La sintaxis básica es:

```
jwhois dominio
```

Ejemplo:

```
jwhois linuxparatodos.net
```

Loa anterior regresa la información correspondiente al dominio *linuxparatodos.net*.

61.2. Equipamiento lógico necesario

Paquete	Descripción
· **bind**	Incluye el **Servidor DNS** (**named**) y herramientas para verificar su funcionamiento.
· **bind-libs**	Biblioteca compartida que consiste en rutinas para aplicaciones para utilizarse cuando se interactúe con **Servidores DNS**.
· **bind-chroot**	Contiene un árbol de ficheros que puede ser utilizado como una jaula *chroot* para **named** añadiendo seguridad adicional al servicio.
· **bind-utils**	Colección de herramientas para consultar **Servidores DNS**.
· **caching-nameserver**	Ficheros de configuración que harán que el **Servidor DNS** actúe como un caché para el servidor de nombres.

61.2.1. Instalación a través de yum

Si se utiliza de CentOS 4 o White Box Enterprise Linux 4, o versiones posteriores, se puede instalar utilizando lo siguiente:

```
yum -y install bind bind-chroot bind-utils caching-nameserver
```

61.2.2. Instalación a través de Up2date

Si se utiliza de Red Hat™ Enterprise Linux 4, o versiones posteriores, se puede instalar utilizando lo siguiente:

```
up2date -i bind bind-chroot bind-utils caching-nameserver
```

61.3. Procedimientos

61.3.1. Preparativos

Idealmente se deben definir primero los siguiente datos:

1. Dominio a resolver.

2. Servidor de nombres principal (SOA). **Éste debe ser un nombre que ya esté plenamente resuelto,** y debe ser un **FQDN** (**F**ully **Q**ualified **D**omain **N**ame).

3. Lista de todos los servidores de nombres (NS) que se utilizarán para efectos de redundancia. **Éstos deben ser nombres que ya estén plenamente resueltos**, y deben ser además **FQDN** (**F**ully **Q**ualified **D**omain **N**ame).

4. Cuenta de correo del administrador responsable de esta zona. **Dicha cuenta debe existir y no debe pertenecer a la misma zona que se está tratando de resolver.**

5. Al menos un servidor de correo (MX), con un registro **A**, nunca **CNAME**.

6. IP predeterminada del dominio.

7. Sub-dominios dentro del dominio (www, mail, ftp, ns, etc.) y las direcciones IP que estarán asociadas a estos.

Es importante tener bien en claro que los puntos 2, 3 y 4 involucran datos que **deben existir previamente** y estar plenamente resueltos por otro servidor DNS; Lo anterior quiere decir no pueden utilizar datos que sean parte o dependan del mismo dominio que se pretende resolver. De igual modo, el servidor donde se implementará el **DNS** deberá contar con un nombre **FQDN** y que esté previa y plenamente resuelto en otro DNS.

Como regla general se generará una zona de reenvío por cada dominio sobre el cual se tenga autoridad plena y absoluta y se generará una zona de resolución inversa por cada red sobre la cual se tenga plena y absoluta autoridad. es decir, si se es propietario del dominio *«cualquiercosa.com»*, se deberá generar el fichero de zona correspondiente a fin de resolver dicho dominio. Por cada red con direcciones IP privadas sobre la cual se tenga control y plena y absoluta autoridad, se deberá generar un fichero de zona de resolución inversa a fin de resolver inversamente las direcciones IP de dicha zona. Regularmente la resolución inversa de las direcciones IP públicas es responsabilidad de los proveedores de servicio ya que son estos quienes tienen la autoridad plena y absoluta sobre dichas direcciones IP.

Todos los ficheros de zona deben pertenecer al usuario «named» a fin de que el servicio **named** pueda acceder a estos o bien modificarlos en el caso de tratarse de zonas esclavas.

61.3.2. Creación de los ficheros de zona

Los siguientes corresponderían a los contenidos para los ficheros de zona requeridos para la red local y por el NIC con el que se haya registrado el dominio. Note por favor que en las zonas de reenvío siempre se especifica al menos un Mail Exchanger (**MX**) y que **se utilizan tabuladores (tecla TAB) en lugar de espacio**. Solo necesitará sustituir nombres y direcciones IP, y quizá añadir nuevos registros para complementar su red local.

61.3.2.1. Zona de reenvío red local /var/named/chroot/var/named/red-local.zone

```
$TTL 86400
```

```
@               IN      SOA     dns.red-local.  jperez.red-local. (
                2006031601; número de serie
                28800 ; tiempo de refresco
                7200 ; tiempo entre reintentos de consulta
                604800 ; tiempo tras el cual expira la zona
                86400 ; tiempo total de vida
                )
@               IN      NS      dns
@               IN      MX      10      mail
@               IN      A       192.168.1.1
intranet        IN      A       192.168.1.1
maquina2        IN      A       192.168.1.2
maquina3        IN      A       192.168.1.3
maquina4        IN      A       192.168.1.4
www             IN      CNAME   intranet
mail            IN      A       192.168.1.1
ftp             IN      CNAME   intranet
dns             IN      CNAME   intranet
```

61.3.2.2. Zona de resolución inversa red local /var/named/chroot/var/named/1.168.192.in-addr.arpa.zone

```
$TTL 86400
@               IN      SOA     dns.red-local.  jperez.red-local. (
                2006031601 ; número de serie
                28800 ; tiempo de refresco
                7200 ; tiempo entre reintentos de consulta
                604800 ; tiempo tras el cual expira la zona
                86400 ; tiempo total de vida
                )
@               IN      NS      dns.red-local.
1       IN      PTR     intranet.red-local.
2       IN      PTR     maquina2.red-local.
3       IN      PTR     maquina3.red-local.
4       IN      PTR     maquina4.red-local.
```

61.3.2.3. Zona de reenvío del dominio /var/named/chroot/var/named/dominio.com.zone

Suponiendo que hipotéticamente se es la autoridad para el dominio **«dominio.com»**, se puede crear una **Zona de Reenvio** con un contenido similar al siguiente:

```
$TTL 86400
@               IN      SOA     fqdn.dominio-resuelto.
cuenta.email.existente. (
                2006031601; número de serie
                28800 ; tiempo de refresco
                7200 ; tiempo entre reintentos de consulta
                604800 ; tiempo tras el cual expira la zona
                86400 ; tiempo total de vida
                )
@               IN      NS      dns
@               IN      MX      10      mail
@               IN      A       148.243.59.1
servidor        IN      A       148.243.59.1
```

```
www             IN      CNAME   servidor
mail            IN      A       148.243.59.1
ftp             IN      CNAME   servidor
dns             IN      CNAME   servidor
```

61.3.2.4. Zona de resolución inversa del dominio /var/named/chroot/var/named/1.243.148.in-addr.arpa.zone

Suponiendo que hipotéticamente se es la autoridad para el segmento de red **148.234.1.0/24**, se puede crear una **Zona de Resolución Inversa** con un contenido similar al siguiente:

```
$TTL 86400
@               IN      SOA     fqdn.dominio-resuelto.
cuenta.email.existente. (
                2006031601 ; número de serie
                28800 ; tiempo de refresco
                7200 ; tiempo entre reintentos de consulta
                604800 ; tiempo tras el cual expira la zona
                86400 ; tiempo total de vida
                )
@               IN      NS      dns.dominio.com.
1       IN      PTR     servidor.dominio.com.
2       IN      PTR     maquina2.dominio.com.
3       IN      PTR     maquina3.dominio.com.
4       IN      PTR     maquina4.dominio.com.
```

Cada vez que haga algún cambio en algún fichero de zona, deberá cambiar el número de serie (**serial**) a fin de que tomen efecto los cambios de inmediato cuando se reinicie el servicio **named**, ya que de otro modo tendría que reiniciar el equipo, algo poco conveniente.

61.3.2.5. Configuración de parámetros en el fichero /etc/named.conf

```
options {
        directory "/var/named/";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        allow-recursion {
                127.0.0.1;
                192.168.1.0/24;
        };
        forwarders {
                200.33.146.209;
                200.33.146.217;
        };
        forward first;
};
zone "." {
        type hint;
        file "named.ca";
};
zone "0.0.127.in-addr.arpa" {
        type master;
        file "0.0.127.in-addr.arpa.zone";
        allow-update { none; };
```

```
};
zone "localhost" {
        type master;
        file "localhost.zone";
        allow-update { none; };
};
zone "dominio.com" {
        type master;
        file "dominio.com.zone";
        allow-update { none; };
};
zone "1.243.148.in-addr.arpa" {
        type master;
        file "1.243.148.in-addr.arpa.zone";
        allow-update { none; };
};
zone "red-local" {
        type master;
        file "red-local.zone";
        allow-update { none; };
};
zone "1.168.192.in-addr.arpa" {
        type master;
        file "1.168.192.in-addr.arpa.zone";
        allow-update { none; };
};
```

61.3.3. Seguridad adicional en DNS para uso público

Un **DDoS** (**D**istributed **D**enial **o**f **S**ervice) es una ampliación del ataque **DoS**, se efectúa con la instalación de varios agentes remotos en muchas computadoras que pueden estar localizadas en diferentes puntos del mundo. El atacante consigue coordinar esos agentes para así, de forma masiva, amplificar el volumen del saturación de información (flood), pudiendo darse casos de un ataque de cientos o millares de computadoras dirigido a una máquina o red objetivo. Esta técnica se ha revelado como una de las más eficaces y sencillas a la hora de colapsar servidores, la tecnología distribuida ha ido haciendo más sofisticada hasta el punto de otorgar poder de causar daños serios a personas con escaso conocimiento técnico.

Un DNS configurado para permitir consultas recursivas indiscriminadamente puede permitir al servidor sufrir o bien participar de un **DDoS**. Solución al problema consiste añadir en el fichero **/etc/named.conf**, en la sección de opciones (options), el parámetro **allow-recursion** definiendo la red, las redes o bien los ACL que tendrán permitido realizar todo tipo de consultas en el DNS, sean locales o de otros dominios.

61.3.3.1. Fichero /etc/named.conf

```
options {
        directory "/var/named/";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        allow-recursion {
                127.0.0.1;
                192.168.1.0/24;
        };
        forwarders {
```

```
                200.33.146.209;
                200.33.146.217;
        };
        forward first;
};
zone "." {
        type hint;
        file "named.ca";
};
zone "dominio.com" {
        type master;
        file "dominio.com.zone";
        allow-update { none; };
};
zone "1.243.148.in-addr.arpa" {
        type master;
        file "1.243.148.in-addr.arpa.zone";
        allow-update { none; };
};
```

Lo anterior hace que solo 192.168.1.0/24 pueda realizar todo tipo de consultas en el DNS, ya sea para un nombre de dominio hospedado de forma local y otros dominios resueltos en otros servidores (*ejemplos: www.yahoo.com, www.google.com, www.linuxparatodos.net, etc.*). El resto del mundo solo podrá realizar consultas sobre las zonas **dominio.com** y **1.243.148.in-addr.arpa**, que están hospedados de forma local.

61.3.4. Seguridad adicional en DNS para uso exclusivo en red local

Si se va a tratar de un servidor de nombres de dominio para uso exclusivo en red local, y se quieren evitar problemas de seguridad de diferente índole, puede utilizarse el parámetro **allow-query**, el cual servirá para especificar que solo ciertas direcciones podrán realizar consultas al servidor de nombres de dominio. Se pueden especificar directamente direcciones IP, redes completas o listas de control de acceso que deberán definirse antes de cualquier otra cosa en el fichero **/etc/named.conf**.

61.3.4.1. Fichero /etc/named.conf

```
acl "redlocal" {
                127.0.0.1;
                192.168.1.0/24;
                192.168.2.0/24;
                192.168.3.0/24;
};

options {
        directory "/var/named/";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        allow-recursion { redlocal; };
        forwarders {
                200.33.146.209;
                200.33.146.217;
        };
        forward first;
        allow-query {
```

```
                redlocal;
                192.168.1.15;
                192.168.1.16;
        };
};
zone "red-local" {
        type master;
        file "red-local.zone";
        allow-update { none; };
};
zone "1.168.192.in-addr.arpa" {
        type master;
        file "1.168.192.in-addr.arpa.zone";
        allow-update { none; };
};
```

61.3.5. Las zonas esclavas

Las zonas esclavas se refieren a aquellas hospedadas en servidores de nombres de dominio secundarios y que hacen las funciones de redundar las zonas maestras en los servidores de nombres de dominio primarios. El contenido del fichero de zona es el mismo que en servidor primario. La diferencia está en la sección de texto utilizada en **/etc/named.conf**, donde las zonas se definen como esclavas y definen los servidores donde está hospedada la zona maestra.

61.3.5.1. Fichero /etc/named.conf Servidor DNS secundario

```
zone "dominio.com" {
        type slave;
        file "dominio.com.zone";
        masters { 192.168.1.254; };
};
zone "1.243.148.in-addr.arpa" {
        type slave;
        file "1.243.148.in-addr.arpa.zone";
        masters { 192.168.1.254; };
};
zone "red-local" {
        type slave;
        file "red-local.zone";
        masters { 192.168.1.254; };
};
zone "1.168.192.in-addr.arpa" {
        type slave;
        file "1.168.192.in-addr.arpa.zone";
        masters { 192.168.1.254; };
};
```

Adicionalmente, si desea incrementar seguridad y desea especificar **en el Servidor DNS primario** que servidores tendrán permitido ser servidores de nombres de dominio secundario, es decir, hacer transferencias, puede utilizar el parámetro **allow-transfer** del siguiente modo:

61.3.5.2. Fichero /etc/named.conf Servidor DNS primario

```
zone "dominio.com" {
```

```
        type master;
        file "dominio.com.zone";
        allow-update { none; };
        allow-transfer {
                200.33.146.217;
                200.33.146.209;
        };
};
zone "1.243.148.in-addr.arpa" {
        type master;
        file "1.243.148.in-addr.arpa.zone";
        allow-update { none; };
        allow-transfer {
                200.33.146.217;
                200.33.146.209;
        };
};
zone "red-local" {
        type master;
        file "red-local.zone";
        allow-update { none; };
        allow-transfer {
                192.168.1.15;
                192.168.1.16;
        };
};
zone "1.168.192.in-addr.arpa" {
        type master;
        file "1.168.192.in-addr.arpa.zone";
        allow-update { none; };
        allow-transfer {
                192.168.1.15;
                192.168.1.16;
        };
};
```

61.3.6. Reiniciar servicio y depuración de configuración

Al terminar de editar todos los ficheros involucrados, solo bastará reiniciar el servidor de nombres de dominio.

```
service named restart
```

Si queremos que el servidor de nombres de dominio quede añadido entre los servicios en el arranque del sistema, deberemos ejecutar lo siguiente a fin de habilitar **named** junto con el arranque del sistema:

```
chkconfig named on
```

Realice prueba de depuración y verifique que la zona haya cargado con número de serie:

```
tail -80 /var/log/messages |grep named
```

Lo anterior, si está funcionando correctamente, debería devolver algo parecido a lo mostrado a

continuación:

```
Aug 17 17:15:15 linux named[30618]: starting BIND 9.2.2 -u named
Aug 17 17:15:15 linux named[30618]: using 1 CPU
Aug 17 17:15:15 linux named: Iniciación de named succeeded
Aug 17 17:15:15 linux named[30622]: loading configuration from '/etc/named.conf'
Aug 17 17:15:15 linux named[30622]: no IPv6 interfaces found
Aug 17 17:15:15 linux named[30622]: listening on IPv4 interface lo, 127.0.0.1#53
Aug 17 17:15:15 linux named[30622]: listening on IPv4 interface eth0, 192.168.1.1#53
Aug 17 17:15:15 linux named[30622]: command channel listening on 127.0.0.1#953
Aug 17 17:15:16 linux named[30622]: zone 0.0.127.in-addr.arpa/IN: loaded serial 3
Aug 17 17:15:16 linux named[30622]: zone 1.168.192.in-addr.arpa/IN: loaded serial
2006031602
Aug 17 17:15:16 linux named[30622]: zone localhost/IN: loaded serial 1
Aug 17 17:15:16 linux named[30622]: zone mi-dominio.com.mx/IN: loaded serial 2006031602
Aug 17 17:15:16 linux named[30622]: running
Aug 17 17:15:16 linux named[30622]: zone 1.168.192.in-addr.arpa/IN: sending notifies
(serial 2006031602)
Aug 17 17:15:16 linux named[30622]: zone mi-dominio.com.mx/IN: sending notifies (serial
2006031602)
```

62. Cómo configurar Squid: Parámetros básicos para Servidor Intermediario (Proxy)

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

62.1. Introducción

62.1.1. ¿Qué es Servidor Intermediario (Proxy)?

El término en ingles **«Proxy»** tiene un significado muy general y al mismo tiempo ambiguo, aunque invariablemente se considera un sinónimo del concepto de **«Intermediario»**. Se suele traducir, en el sentido estricto, como **delegado** o **apoderado** (el que tiene el que poder sobre otro).

Un **Servidor Intermediario** (Proxy) se define como una computadora o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red. Durante el proceso ocurre lo siguiente:

- Cliente se conecta hacia un **Servidor Intermediario** (Proxy).
- Cliente solicita una conexión, fichero u otro recurso disponible en un servidor distinto.
- **Servidor Intermediario** (Proxy) proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.
- En algunos casos el **Servidor Intermediario** (Proxy) puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

Los **Servidores Intermediarios** (Proxies) generalmente se hacen trabajar simultáneamente como muro cortafuegos operando en el **Nivel de Red**, actuando como filtro de paquetes, como en el caso de **iptables**, o bien operando en el **Nivel de Aplicación**, controlando diversos servicios, como es el caso de **TCP Wrapper**. Dependiendo del contexto, el muro cortafuegos también se conoce como **BPD** o **B**order **P**rotection **D**evice o simplemente **filtro de paquetes**.

Una aplicación común de los **Servidores Intermediarios** (Proxies) es funcionar como caché de contenido de Red (principalmente HTTP), proporcionando en la proximidad de los clientes un caché de páginas y ficheros disponibles a través de la Red en servidores HTTP remotos, permitiendo a los clientes de la red local acceder hacia éstos de forma más rápida y confiable.

Cuando se recibe una petición para un recurso de Red especificado en un **URL** (**U**niform **R**esource **L**ocator) el **Servidor Intermediario** busca el resultado del **URL** dentro del caché. Si éste es encontrado, el **Servidor Intermediario** responde al cliente proporcionado inmediatamente el contenido solicitado. Si el contenido solicitado no estuviera disponible en el caché, el **Servidor Intermediario** lo traerá desde servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado luego a través de un algoritmo de expiración de acuerdo a la antigüedad, tamaño e historial de **respuestas a solicitudes** (hits)

(ejemplos: **LRU**, **LFUDA** y **GDSF**).

Los **Servidores Intermediarios** para contenido de Red (Web Proxies) también pueden actuar como filtros del contenido servido, aplicando políticas de censura de acuerdo a criterios arbitrarios.

62.1.2. Acerca de Squid

Squid es un **Servidor Intermediario** (Proxy) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix®. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (**GNU/GPL**). Siendo sustento lógico **libre**, está disponible el código fuente para quien así lo requiera.

Entre otras cosas, **Squid** puede funcionar como **Servidor Intermediario** (Proxy) y **caché de contenido de Red** para los protocolos **HTTP**, **FTP**, **GOPHER** y **WAIS**, Proxy de **SSL**, caché transparente, **WWCP**, aceleración **HTTP**, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.

Squid consiste de un programa principal como servidor, un programa para búsqueda en servidores **DNS**, programas opcionales para reescribir solicitudes y realizar autenticación y algunas herramientas para administración y y herramientas para clientes. Al iniciar **Squid** da origen a un número configurable (5, de modo predefinido a través del parámetro **dns_children**) de procesos de búsqueda en servidores **DNS**, cada uno de los cuales realiza una búsqueda única en servidores **DNS**, reduciendo la cantidad de tiempo de espera para las búsquedas en servidores **DNS**.

> **NOTA ESPECIAL: Squid no debe ser utilizado como Servidor Intermediario (Proxy)** para protocolos como **SMTP**, **POP3**, **TELNET**, **SSH**, **IRC**, etc. Si se requiere intermediar para **cualquier protocolo distinto** a **HTTP**, **HTTPS**, **FTP**, **GOPHER** y **WAIS** se requerirá implementar obligatoriamente un enmascaramiento de IP o **NAT** (**N**etwork **A**ddress **T**ranslation) o bien hacer uso de un servidor **SOCKS** como **Dante** (http://www.inet.no/dante/).

URL: http://www.squid-cache.org/

62.1.2.1. Algoritmos de caché utilizados por Squid.

A través de un parámetro (**cache_replacement_policy**) **Squid** incluye soporte para los siguientes algoritmos para el caché:

- **LRU** Acrónimo de **L**east **R**ecently **U**sed, que traduce como **Menos Recientemente Utilizado**. En este algoritmo los objetos que no han sido accedidos en mucho tiempo son eliminados primero, manteniendo siempre en el caché a los objetos más recientemente solicitados. **Ésta política es la utilizada por Squid de modo predefinido**.

- **LFUDA** Acrónimo de **L**east **F**requently **U**sed with **D**ynamic **A**ging, que se traduce como **Menos Frecuentemente Utilizado con Envejecimiento Dinámico**. En este algoritmo los objetos más solicitados permanecen en el caché sin importar su tamaño optimizando la **eficiencia** (hit rate) por **octetos** (Bytes) a expensas de la eficiencia misma, de modo que un objeto grande que se solicite con mayor

frecuencia impedirá que se pueda hacer caché de objetos pequeños que se soliciten con menor frecuencia.

- **GDSF** Acrónimo de **G**reedy**D**ual **S**ize **F**requency, que se traduce como **Frecuencia de tamaño *GreedyDual*** (*codicioso dual*), que es el algoritmo sobre el cual se basa **GDSF**. Optimiza la **eficiencia** (hit rate) por objeto manteniendo en el caché los objetos pequeños más frecuentemente solicitados de modo que hay mejores posibilidades de lograr **respuesta a una solicitud** (hit). Tiene una eficiencia por **octetos** (Bytes) menor que el algoritmo **LFUDA** debido a que descarta del caché objetos grandes que sean solicitado con frecuencia.

62.2. Equipamiento lógico necesario

Para poder llevar al cabo los procedimientos descritos en este manual y documentos relacionados, usted necesitará tener instalado al menos lo siguiente:

- Al menos squid-2.5.STABLE6
- httpd-2.0.x (Apache), como auxiliar de caché con aceleración.
- **Todos** los parches de seguridad disponibles para la versión del sistema operativo que esté utilizando.

Tómese en consideración que, de ser posible, se debe utilizar **siempre** las versiones estables más recientes de todo el sustento lógico que se vaya a instalar al realizar los procedimientos descritos en este manual, a fin de contar con los parches de seguridad necesarios. **Ninguna versión de Squid anterior a la 2.5.STABLE6 se considera como apropiada** debido a fallas de seguridad de gran importancia.

Squid no se instala de manera predeterminada a menos que especifique lo contrario durante la instalación del sistema operativo, sin embargo viene incluido en casi todas las distribuciones actuales. El procedimiento de instalación es exactamente el mismo que con cualquier o.

62.2.1. Instalación a través de yum

Si cuenta con un sistema con CentOS o White Box Enterprise Linux 3 o versiones posteriores, utilice lo siguiente y se instalará todo lo necesario junto con sus dependencias:

```
yum -y install squid httpd
```

62.2.2. Instalación a través de up2date

Si cuenta con un sistema con Red Hat™ Enterprise Linux 3 o versiones posteriores, utilice lo siguiente y se instalará todo lo necesario junto con sus dependencias:

```
up2date -i squid httpd
```

62.2.3. Otros componentes necesarios

El mandato **iptables** se utilizará para generar las reglas necesarias para el guión de Enmascaramiento de IP. Se instala de modo predefinido en todas las distribuciones actuales que utilicen **núcleo** (kernel) versiones 2.4 y 2.6.

Es importante tener actualizado el núcleo del sistema operativo por diversas cuestiones de seguridad. No es recomendable utilizar versiones del kernel anteriores a la **2.4.21**. Actualice el núcleo a la versión más reciente disponible para su distribución.

Si cuenta con un sistema con CentOS o White Box Enterprise Linux 3 o versiones posteriores, utilice lo siguiente para actualizar el núcleo del sistema operativo e **iptables**, si acaso fuera necesario:

```
yum -y update kernel iptables
```

Si cuenta con un sistema con Red Hat™ Enterprise Linux 3 o versiones posteriores, utilice lo siguiente para actualizar el núcleo del sistema operativo, e **iptables** si acaso fuera necesario:

```
up2date -u kernel iptables
```

62.3. Antes de continuar

Tenga en cuenta que este manual ha sido comprobado varias veces y ha funcionado en todos los casos y si algo no funciona solo significa que usted no lo leyó a detalle y no siguió correctamente las indicaciones.

Evite dejar **espacios vacíos** en lugares indebidos. El siguiente es un ejemplo de como **no** se debe habilitar un parámetro.

Mal

```
# Opción incorrectamente habilitada
  http_port 3128
```

El siguiente es un ejemplo de como **si** se debe habilitar un parámetro.

Bien

```
# Opción correctamente habilitada
http_port 3128
```

62.4. Configuración básica

Squid utiliza el fichero de configuración localizado en **/etc/squid/squid.conf**, y podrá trabajar sobre este utilizando su editor de texto simple preferido. Existen un gran número de parámetros, de los cuales recomendamos configurar los siguientes:

- http_port
- cache_dir
- Al menos una **Lista de Control de Acceso**
- Al menos una **Regla de Control de Acceso**

62.4.1. Parámetro http_port: ¿Qué puerto utilizar para Squid?

De acuerdo a las asignaciones hechas por **IANA** y continuadas por la **ICANN** desde el 21 de marzo de 2001, los **P**uertos **R**egistrados (rango desde 1024 hasta 49151) recomendados para **Servidores Intermediarios** (Proxies) pueden ser el 3128 y 8080 a través de **TCP**.

De modo predefinido **Squid** utilizará el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos

disponibles a la vez.

En el caso de un **Servidor Intermediario** (Proxy) Transparente, regularmente se utilizará el puerto 80 o el 8000 y se valdrá del re-direccionamiento de peticiones de modo tal que no habrá necesidad alguna de modificar la configuración de los **clientes HTTP** para utilizar el **Servidor Intermediario** (Proxy). Bastará con utilizar como puerta de enlace al servidor. Es importante recordar que los **Servidores HTTP**, como Apache, también utilizan dicho puerto, por lo que será necesario volver a configurar el servidor **HTTP** para utilizar otro puerto disponible, o bien desinstalar o desactivar el servidor HTTP.

Hoy en día puede no ser del todo práctico el utilizar un **Servidor Intermediario (Proxy) Transparente**, a menos que se trate de un servicio de **Café Internet** u oficina pequeña, siendo que uno de los principales problemas con los que lidian los administradores es el mal uso y/o abuso del acceso a Internet por parte del personal. Es por esto que puede resultar más conveniente configurar un **Servidor Intermediario** (Proxy) con restricciones por clave de acceso, lo cual no puede hacerse con un **Servidor Intermediario (Proxy) Transparente**, debido a que se requiere un diálogo de nombre de usuario y clave de acceso.

Regularmente algunos programas utilizados comúnmente por los usuarios suelen traer de modo predefinido el puerto 8080 **(servicio de cacheo WWW)** para utilizarse al configurar que **Servidor Intermediario** (Proxy) utilizar. Si queremos aprovechar esto en nuestro favor y ahorrarnos el tener que dar explicaciones innecesarias al usuario, podemos especificar que **Squid** escuche peticiones en dicho puerto también. Siendo así localice la sección de definición de **http_port**, y especifique:

```
#
#    You may specify multiple socket addresses on multiple lines.
#
# Default: http_port 3128
http_port 3128
http_port 8080
```

Si desea incrementar la seguridad, puede vincularse el servicio a una IP que solo se pueda acceder desde la red local. Considerando que el servidor utilizado posee una IP 192.168.1.254, puede hacerse lo siguiente:

```
#
#    You may specify multiple socket addresses on multiple lines.
#
# Default: http_port 3128
http_port 192.168.1.254:3128
http_port 192.168.1.254:8080
```

62.4.2. Parámetro cache_mem

El parámetro **cache_mem** establece la cantidad ideal de memoria para lo siguiente:

- Objetos en tránsito.
- Objetos frecuentemente utilizados (*Hot*).
- Objetos negativamente almacenados en el caché.

Los datos de estos objetos se almacenan en bloques de 4 Kb. El parámetro **cache_mem** especifica un límite máximo en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad. Sin embargo los objetos **Hot** y aquellos negativamente almacenados en el caché podrán utilizar la memoria no utilizada hasta que esta sea requerida. De ser necesario, si un objeto

en tránsito es mayor a la cantidad de memoria especificada, **Squid** excederá lo que sea necesario para satisfacer la petición.

De modo predefinido se establecen 8 MB. Puede especificarse una cantidad mayor si así se considera necesario, dependiendo esto de los hábitos de los usuarios o necesidades establecidas por el administrador.

Si se posee un servidor con al menos 128 MB de RAM, establezca 16 MB como valor para este parámetro:

```
cache_mem 16 MB
```

62.4.3. Parámetro cache_dir: ¿Cuánto desea almacenar de Internet en el disco duro?

Este parámetro se utiliza para establecer que tamaño se desea que tenga el caché en el disco duro para **Squid**. Para entender esto un poco mejor, responda a esta pregunta: **¿Cuanto desea almacenar de Internet en el disco duro?** De modo predefinido **Squid** utilizará un caché de 100 MB, de modo tal que encontrará la siguiente línea:

```
cache_dir ufs /var/spool/squid 100 16 256
```

Se puede incrementar el tamaño del caché hasta donde lo desee el administrador. Mientras más grande sea el caché, más objetos se almacenarán en éste y por lo tanto se utilizará menos el ancho de banda. La siguiente línea establece un caché de 700 MB:

```
cache_dir ufs /var/spool/squid 700 16 256
```

Los números **16** y **256** significan que el directorio del caché contendrá 16 directorios subordinados con 256 niveles cada uno. **No modifique esto números, no hay necesidad de hacerlo**.

Es muy importante considerar que si se especifica un determinado tamaño de caché y éste excede al espacio real disponible en el disco duro, **Squid** se bloqueará inevitablemente. Sea cauteloso con el tamaño de caché especificado.

62.4.4. Parámetro ftp_user

Al acceder a un servidor FTP de manera anónima, de modo predefinido **Squid** enviará como clave de acceso **Squid@**. Si se desea que el acceso anónimo a los servidores FTP sea más informativo, o bien si se desea acceder a servidores FTP que validan la autenticidad de la dirección de correo especificada como clave de acceso, puede especificarse la dirección de correo electrónico que uno considere pertinente.

```
ftp_user proxy@su-dominio.net
```

62.4.5. Controles de acceso

Es necesario establecer **Listas de Control de Acceso** que definan una red o bien ciertas máquinas en particular. A cada lista se le asignará una **Regla de Control de Acceso** que permitirá o denegará el acceso a **Squid**. Procedamos a entender como definir unas y otras.

62.4.5.1. Listas de control de acceso.

Regularmente una lista de control de acceso se establece con la siguiente sintaxis:

```
acl [nombre de la lista] src [lo que compone a la lista]
```

Si se desea establecer una lista de control de acceso que abarque a toda la red local, basta definir la IP correspondiente a la red y la máscara de la sub-red. Por ejemplo, si se tiene una red donde las máquinas tienen direcciones IP 192.168.1.**n** con máscara de sub-red 255.255.255.0, podemos utilizar lo siguiente:

```
acl miredlocal src 192.168.1.0/255.255.255.0
```

También puede definirse una **Lista de Control de Acceso** especificando un fichero localizado en cualquier parte del disco duro, y la cual contiene una lista de direcciones IP. Ejemplo:

```
acl permitidos src "/etc/squid/permitidos"
```

El fichero **/etc/squid/permitidos** contendría algo como siguiente:

```
192.168.1.1
192.168.1.2
192.168.1.3
192.168.1.15
192.168.1.16
192.168.1.20
192.168.1.40
```

Lo anterior estaría definiendo que la **Lista de Control de Acceso** denominada **permitidos** estaría compuesta por las direcciones IP incluidas en el fichero **/etc/squid/permitidos**.

62.4.5.2. Reglas de Control de Acceso

Estas definen si se permite o no el acceso hacia **Squid**. Se aplican a las **Listas de Control de Acceso**. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador, es decir, a partir de donde se localiza la siguiente leyenda:

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
```

La sintaxis básica es la siguiente:

```
http_access [deny o allow] [lista de control de acceso]
```

En el siguiente ejemplo consideramos una regla que establece acceso permitido a **Squid** a la **Lista de Control de Acceso** denominada **permitidos**:

```
http_access allow permitidos
```

También pueden definirse reglas valiéndose de la expresión **!**, la cual significa **no**. Pueden definirse,

por ejemplo, dos listas de control de acceso, una denominada **lista1** y otra denominada **lista2**, en la misma regla de control de acceso, en donde se asigna una expresión a una de estas. La siguiente establece que se permite el acceso a **Squid** a lo que comprenda **lista1** excepto aquello que comprenda **lista2**:

```
http_access allow lista1 !lista2
```

Este tipo de reglas son útiles cuando se tiene un gran grupo de IP dentro de un rango de red al que se debe **permitir** acceso, y otro grupo dentro de la misma red al que se debe **denegar** el acceso.

62.4.6. Aplicando Listas y Reglas de control de acceso

Una vez comprendido el funcionamiento de la Listas y las Regla de Control de Acceso, procederemos a determinar cuales utilizar para nuestra configuración.

62.4.6.1. Caso 1.

Considerando como ejemplo que se dispone de una red 192.168.1.0/255.255.255.0, si se desea definir toda la red local, utilizaremos la siguiente línea en la sección de **Listas de Control de Acceso**:

```
acl todalared src 192.168.1.0/255.255.255.0
```

Habiendo hecho lo anterior, la sección de listas de control de acceso debe quedar más o menos del siguiente modo:

Listas de Control de Acceso: definición de una red local completa

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl todalared src 192.168.1.0/255.255.255.0
```

A continuación procedemos a aplicar la regla de control de acceso:

```
http_access allow todalared
```

Habiendo hecho lo anterior, la zona de reglas de control de acceso debería quedar más o menos de este modo:

Reglas de control de acceso: Acceso a una Lista de Control de Acceso.

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow todalared
http_access deny all
```

La regla **http_access allow todalared** permite el acceso a **Squid** a la **Lista de Control de**

Acceso denominada **todalared**, la cual está conformada por 192.168.1.0/255.255.255.0. Esto significa que cualquier máquina desde 192.168.1.1 hasta 192.168.1.254 podrá acceder a **Squid**.

62.4.6.2. Caso 2

Si solo se desea permitir el acceso a **Squid** a ciertas direcciones IP de la red local, deberemos crear un fichero que contenga dicha lista. Genere el fichero **/etc/squid/listas/redlocal**, dentro del cual se incluirán solo aquellas direcciones IP que desea confirmen la Lista de Control de acceso. Ejemplo:

```
192.168.1.1
192.168.1.2
192.168.1.3
192.168.1.15
192.168.1.16
192.168.1.20
192.168.1.40
```

Denominaremos a esta lista de control de acceso como **redlocal**:

```
acl redlocal src "/etc/squid/listas/redlocal"
```

Habiendo hecho lo anterior, la sección de listas de control de acceso debe quedar más o menos del siguiente modo:

Listas de Control de Acceso: definición de una red local completa

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src "/etc/squid/listas/redlocal"
```

A continuación procedemos a aplicar la regla de control de acceso:

```
http_access allow redlocal
```

Habiendo hecho lo anterior, la zona de reglas de control de acceso debería quedar más o menos de este modo:

Reglas de control de acceso: Acceso a una Lista de Control de Acceso.

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow redlocal
http_access deny all
```

La regla **http_access allow redlocal** permite el acceso a **Squid** a la **Lista de Control de Acceso** denominada **redlocal**, la cual está conformada por las direcciones IP especificadas en el fichero **/etc/squid/listas/redlocal**. Esto significa que cualquier máquina no incluida en

/etc/squid/listas/redlocal no tendrá acceso a **Squid**.

62.4.7. Parámetro chache_mgr

De modo predefinido, si algo ocurre con el caché, como por ejemplo que muera el procesos, se enviará un mensaje de aviso a la cuenta **webmaster** del servidor. Puede especificarse una distinta si acaso se considera conveniente.

```
cache_mgr joseperez@midominio.net
```

62.4.8. Parámetro cache_peer: caches padres y hermanos

El parámetro cache_peer se utiliza para especificar otros **Servidores Intermediarios** (Proxies) con caché en una jerarquía como **padres** o como **hermanos**. Es decir, definir si hay un **Servidor Intermediario** (Proxy) adelante o en paralelo. La sintaxis básica es la siguiente:

```
cache_peer servidor tipo http_port icp_port opciones
```

Ejemplo: Si su caché va a estar trabajando detrás de otro servidor cache, es decir un caché padre, y considerando que el caché padre tiene una IP 192.168.1.1, escuchando peticiones **HTTP** en el puerto 8080 y peticiones ICP en puerto 3130 **(puerto utilizado de modo predefinido por Squid)** ,especificando que no se almacenen en caché los objetos que ya están presentes en el caché del **Servidor Intermediario** (Proxy) padre, utilice la siguiente línea:

```
cache_peer 192.168.1.1 parent 8080 3130 proxy-only
```

Cuando se trabaja en redes muy grandes donde existen varios Servidores Intermediarios (Proxy) haciendo caché de contenido de Internet, es una buena idea hacer trabajar todos los caché entre si. Configurar caches vecinos como **sibling** (hermanos) tiene como beneficio el que se consultarán estos caches localizados en la red local antes de acceder hacia Internet y consumir ancho de banda para acceder hacia un objeto que ya podría estar presente en otro caché vecino.

Ejemplo: Si su caché va a estar trabajando en paralelo junto con otros caches, es decir caches hermanos, y considerando los caches tienen IP 10.1.0.1, 10.2.0.1 y 10.3.0.1, todos escuchando peticiones **HTTP** en el puerto 8080 y peticiones ICP en puerto 3130, especificando que no se almacenen en caché los objetos que ya están presentes en los caches hermanos, utilice las siguientes líneas:

```
cache_peer 10.1.0.1 sibling 8080 3130 proxy-only
cache_peer 10.2.0.1 sibling 8080 3130 proxy-only
cache_peer 10.3.0.1 sibling 8080 3130 proxy-only
```

Pueden hacerse combinaciones que de manera tal que se podrían tener caches padres y hermanos trabajando en conjunto en una red local. Ejemplo:

62.5. Estableciendo el idioma de los mensajes mostrados por de Squid hacia el usuario

Squid incluye traducción a distintos idiomas de las distintas páginas de error e informativas que son desplegadas en un momento dado durante su operación. Dichas traducciones se pueden encontrar en **/usr/share/squid/errors/**. Para poder hacer uso de las páginas de error traducidas al español, es necesario cambiar un enlace simbólico localizado en **/etc/squid/errors** para que

apunte hacia **/usr/share/squid/errors/Spanish** en lugar de hacerlo hacia **/usr/share/squid/errors/English**.

Elimine primero el enlace simbólico actual:

```
rm -f /etc/squid/errors
```

Coloque un nuevo enlace simbólico apuntando hacia el directorio con los ficheros correspondientes a los errores traducidos al español.

```
ln -s /usr/share/squid/errors/Spanish /etc/squid/errors
```

Nota: Este enlace simbólico debe verificarse, y regenerarse de ser necesario, cada vez que se actualizado Squid ya sea a través de yum, up2date o manualmente con el mandato rpm.

62.6. Iniciar, reiniciar y añadir el servicio al arranque del sistema

Una vez terminada la configuración, ejecute el siguiente mandato para iniciar por primera vez **Squid**:

```
service squid start
```

Si necesita reiniciar para probar cambios hechos en la configuración, utilice lo siguiente:

```
service squid restart
```

Si desea que **Squid** inicie de manera automática la próxima vez que inicie el sistema, utilice lo siguiente:

```
chkconfig squid on
```

Lo anterior habilitará a **Squid** en todos los niveles de corrida.

62.7. Depuración de errores

Cualquier error al inicio de **Squid** solo significa que hubo errores de sintaxis, errores de dedo o bien se están citando incorrectamente las rutas hacia los ficheros de las **Listas de Control de Acceso**.

Puede realizar diagnóstico de problemas indicándole a **Squid** que vuelva a leer configuración, lo cual devolverá los errores que existan en el fichero **/etc/squid/squid.conf**.

```
service squid reload
```

Cuando se trata de errores graves que no permiten iniciar el servicio, puede examinarse el contenido del fichero **/var/log/squid/squid.out** con el mandato **less**, **more** o cualquier otro visor de texto:

```
less /var/log/squid/squid.out
```

62.8. Ajustes para el muro corta-fuegos

Si se tiene poca experiencia con guiones de cortafuegos a través de iptables, sugerimos utilizar **Firestarter**. éste permite configurar fácilmente tanto el enmascaramiento de IP como el muro corta-fuegos. Si se tiene un poco más de experiencia, recomendamos utilizar **Shorewall** para el mismo fin puesto que se trata de una herramienta más robusta y completa.

- **Firestarter**: http://www.fs-security.com/
- **Shorewall**: http://www.shorewall.net/

62.8.1. Re-direccionamiento de peticiones a través de iptables y Firestarter

En un momento dado se requerirá tener salida transparente hacia Internet para ciertos servicios, pero al mismo tiempo se necesitará re-direccionar peticiones hacia servicio **HTTP** para pasar a través del el puerto donde escucha peticiones **Squid** (8080), de modo que no haya salida alguna hacia alguna hacia servidores **HTTP** en el exterior sin que ésta pase antes por **Squid**. No se puede hacer **Servidor Intermediario** (Proxy) Transparente para los protocolos HTTPS, FTP, GOPHER ni WAIS, por lo que dichos protocolos tendrán que ser filtrados a través del **NAT**.

El re-direccionamiento lo hacemos a través de **iptables**. Considerando para este ejemplo que la red local se accede a través de una interfaz eth0, el siguiente esquema ejemplifica un re-direccionamiento:

```
/sbin/iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
```

Lo anterior, **que requiere un guión de cortafuegos funcional en un sistema con dos interfaces de red**, hace que cualquier petición hacia el puerto 80 (servicio HTTP) hecha desde la red local hacia el exterior, se re-direccionará hacia el puerto 8080 del servidor.

Utilizando **Firestarter**, la regla anteriormente descrita se añade en el fichero **/etc/firestarter/user-post**.

62.8.2. Re-direccionamiento de peticiones a través de la opción REDIRECT en Shorewall

La acción REDIRECT en **Shorewall** permite redirigir peticiones hacia protocolo **HTTP** para hacerlas pasar a través de **Squid**. En el siguiente ejemplo las peticiones hechas desde la zona que corresponde a la red local serán redirigidas hacia el puerto 8080 del cortafuegos, en donde está configurado **Squid** configurado como **Servidores Intermediario** (Proxy) transparente.

```
#ACTION         SOURCE          DEST    PROTO   DEST
REDIRECT        loc             8080    tcp     80
```

63. Cómo configurar Squid: Acceso por autenticación

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

63.1. Introducción

Es muy útil el poder establecer un sistema de autenticación para poder acceder hacia Internet, pues esto permite controlar quienes si y quienes no accederán a Internet sin importar desde que máquina de la red local lo hagan. Sera de modo tal que tendremos un doble control, primero por dirección IP y segundo por nombre de usuario y clave de acceso.

Este manual considera que usted ya ha leído previamente, a detalle y en su totalidad el manual "Como configurar Squid: Servidor Proxy" y que ha configurado exitosamente Squid como servidor proxy.

63.2. Equipamiento lógico necesario

Para poder llevar la cabo los procedimientos descritos en este manual y documentos relacionados, usted necesitará tener instalado al menos lo siguiente:

- squid-2.5.STABLE3
- httpd-2.0.x (Apache) (opcional)
- openldap-servers-2.2.x (opcional)

63.3. Eligiendo el módulo de autenticación

Este manual considera poder autenticar a través de un fichero de texto simple con claves de acceso creadas con htpasswd o bien a través de un servidor LDAP, lo cual constituye una solución más robusta.

63.3.1. Autenticación a través del módulo LDAP

Considerando que se ha configurado exitosamente OpenLDAP como servidor de autenticación, solo basta definir el directorio (o directorio subordinado) y el servidor LDAP a utilizar.

La sintaxis utilizada para squid_ldap_auth es la siguiente:

```
squid_ldap_auth -b Directorio o DN a utilizar servidor-ldap-a-utilizar
```

63.3.1.1. Parámetros en /etc/squid/squid.conf

Se debe modificar el fichero /etc/squid.conf y se especificar el programa de autenticación se utilizará. Localice la sección que corresponde a la etiqueta *auth_param basic program*. Por defecto no está especificado programa alguno. Considerando que *squid_ldap_auth* se localiza en */usr/lib/squid/ncsa_auth*, procederemos a añadir el siguiente parámetro:

```
auth_param basic program /usr/lib/squid/squid_ldap_auth -b dc=su-red-local,dc=com
127.0.0.1
```

Lo anterior conecta al directorio dc=su-red-local,dc=com en el servidor LDAP en 127.0.0.1.

63.3.2. Autenticación a través del módulo NCSA

Squid puede utilizar el módulo *ncsa_auth*, de la NCSA (**N**ational **C**enter for **S**upercomputing **A**pplications), y que ya viene incluido como parte del paquete principal de Squid en la mayoría de las distribuciones actuales. Este módulo provee una autenticación muy sencilla a través de un fichero de texto simple cuyas claves de acceso fueron creadas con htpasswd.

63.3.2.1. Creación del fichero de claves de acceso

Se requerirá la creación previa de un fichero que contendrá los nombres de usuarios y sus correspondientes claves de acceso (cifradas). El fichero puede localizarse en cualquier lugar del sistema, con la única condición que sea asequible para el usuario *squid*.

Debe procederse a crear un fichero */etc/squid/claves*:

```
touch /etc/squid/claves
```

Salvo que vaya a utilizarse un guión a través del servidor web para administrar las claves de acceso, como medida de seguridad, este fichero debe hacerse leíble y escribible solo para el usuario *squid*:

```
chmod 600 /etc/squid/claves
chown squid:squid /etc/squid/claves
```

A continuación deberemos dar de alta las cuentas que sean necesarias, utilizando el mandato *htpasswd -mismo que viene incluido en el paquete httpd-2.0.x-*. Ejemplo:

```
htpasswd /etc/squid/claves joseperez
```

Lo anterior solicitará teclear una nueva clave de acceso para el usuario *joseperez* y confirmar tecleando ésta de nuevo. Repita con el resto de las cuentas que requiera dar de alta.

Todas las cuentas que se den de alta de este modo son independientes a las ya existentes en el sistema. Al dar de alta una cuenta o cambiar una clave de acceso lo estará haciendo **EXCLUSIVAMENTE** para el acceso al servidor Proxy. Las cuentas son independientes a las que se tengan existentes en el sistema como serían *interprete de mandatos*, correo y Samba.

63.3.2.2. Parámetros en /etc/squid/squid.conf

Lo siguiente será especificar que programa de autenticación se utilizará. Localice la sección que

corresponde a la etiqueta *auth_param basic program*. Por defecto no está especificado programa alguno. Considerando que *ncsa_auth* se localiza en */usr/lib/squid/ncsa_auth*, procederemos a añadir el siguiente parámetro:

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves
```

/usr/lib/squid/ncsa_auth corresponde a la localización del programa para autenticar y */etc/squid/claves* al fichero que contiene las cuentas y sus claves de acceso.

63.4. Listas y reglas de control de acceso

El siguiente paso corresponde a la definición de una *Lista de Control de Acceso*. Especificaremos una denominada *passwd* la cual se configurará para utilizar obligatoriamente la autenticación para poder acceder a Squid. Debe localizarse la sección de *Listas de Control de Acceso* y añadirse la siguiente línea:

```
acl password proxy_auth REQUIRED
```

Habiendo hecho lo anterior, deberemos tener en la sección de *Listas de Control de Acceso* algo como lo siguiente:

Listas de Control de Accesos: autenticación.

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255

acl redlocal src 192.168.1.0/255.255.255.0
acl password proxy_auth REQUIRED
```

Procedemos entonces a modificar la regla de control de accesos que ya teníamos para permitir el acceso a Internet. Donde antes teníamos lo siguiente:

```
http_access allow redlocal
```

Le añadimos *passwd*, la definición de la *Lista de Control de Acceso* que requiere utilizar clave de acceso, a nuestra regla actual, de modo que quede como mostramos a continuación:

```
http_access allow redlocal password
```

Habiendo hecho lo anterior, la zona de reglas de control de acceso debería quedar más o menos de este modo:

Reglas de control de acceso: Acceso por clave de acceso.

```
#
# INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow redlocal password
```

```
http_access deny all
```

63.4.1. Finalizando procedimiento

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

```
service squid restart
```

64. Cómo configurar Squid: Restricción de acceso a Sitios de Red

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

64.1. Introducción

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

Este manual considera que usted ya ha leído previamente, a detalle y en su totalidad el manual "Como configurar Squid: Servidor Proxy" y que ha configurado exitosamente Squid como servidor proxy.

64.2. Equipamiento lógico necesario

Para poder llevar la cabo los procedimientos descritos en este manual y documentos relacionados, usted necesitará tener instalado al menos squid-2.5STABLE1.

64.3. Definiendo patrones comunes

Lo primero será generar una lista la cual contendrá direcciones de Red y palabras usualmente utilizadas en nombres de ciertos dominios. Ejemplos:

```
www.sitioporno.com
www.otrositioporno.com
sitioindeseable.com
otrositioindeseable.com
napster
sex
porn
mp3
xxx
adult
warez
celebri
```

Esta lista, la cual deberá ser completada con todas las palabras (muchas de está son palabras obscenas en distintos idiomas) y direcciones de Red que el administrador considere pertinentes, la guardaremos como */etc/squid/sitiosdenegados*.

64.4. Parámetros en /etc/squid/squid.conf

Debemos definir una *Lista de Control de Acceso* que a su vez defina al fichero */etc/squid/sitiosdenegados*. Esta lista la denominaremos como "*sitiosdenegados*". De modo tal, la línea correspondiente quedaría del siguiente modo:

```
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
```

Habiendo hecho lo anterior, deberemos tener en la sección de *Listas de Control de Acceso* algo como lo siguiente:

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src 192.168.1.0/255.255.255.0
acl password proxy_auth REQUIRED
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
```

A continuación especificaremos modificaremos una *Regla de Control de Acceso* existente agregando con un símbolo de *!* que se denegará el acceso a la *Lista de Control de Acceso* denominada *sitiosdenegados*:

```
http_access allow redlocal !sitiosdenegados
```

La regla anterior permite el acceso a la *Lista de Control de Acceso* denominada *redlocal*, pero le niega el acceso a todo lo que coincida con lo especificado en la *Lista de Control de Acceso* denominada *sitiosdenegados*.

Ejemplo aplicado a una *Regla de Control de Acceso* combinando el método de autenticación explicado en el documento Cómo configurar Squid: Acceso por Autenticación:

Reglas de control de acceso: denegación de sitios.

```
#
# INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow redlocal password !sitiosdenegados
http_access deny all
```

64.4.1. Permitiendo acceso a sitios inocentes incidentalmente bloqueados

Si por ejemplo el incluir una palabra en particular afecta el acceso a un sitio de Red, también puede generarse una lista de dominios o palabras que contengan un patrón pero que consideraremos como apropiados.

Como ejemplo: vamos a suponer que dentro de la *Lista de Control de Acceso* de sitios denegados está la palabra *sex*. esta denegaría el acceso a cualquier nombre de dominio que incluya dicha cadena de caracteres, como extremesex.com. Sin embargo también estaría bloqueando a sitios como sexualidadjovel.cl, el cual no tiene que ver en lo absoluto con pornografía, sino orientación sexual para la juventud. Podemos añadir este nombre de dominio en un ficheros que

denominaremos */etc/squid/sitios-inocentes*.

Este fichero será definido en una *Lista de Control de Acceso* del mismo modo en que se hizo anteriormente con el fichero que contiene dominios y palabras denegadas.

```
acl inocentes url_regex "/etc/squid/sitios-inocentes"
```

Para hacer uso del fichero, solo bastará utilizar la expresión **!** en la misma línea utilizada para la *Regla de Control de Acceso* establecida para denegar el mismo.

```
http_access allow all inocentes
```

La regla anterior especifica que se denegará el acceso a todo lo que comprenda la *Lista de Control de Acceso* denominada *denegados* **excepto** lo que comprenda la *Lista de Control de Acceso* denominada *inocentes*. es decir, se podrá acceder sin dificultad a www.sexualidadjoven.cl manteniendo la restricción para la cadena de caracteres *sex*.

64.4.2. Finalizando procedimiento

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

```
service squid restart
```

65. Cómo configurar Squid: Restricción de acceso a contenido por extensión

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

65.1. Introducción

Denegar el acceso a ciertos tipos de extensiones de fichero permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple, y consiste en denegar el acceso a ciertos tipos de extensiones que coincidan con lo establecido en una *Lista de Control de Acceso*.

Este manual considera que usted ya ha leído previamente, a detalle y en su totalidad el manual "Como configurar Squid: Servidor Proxy" y que ha configurado exitosamente Squid como servidor proxy.

65.2. Equipamiento lógico necesario

Para poder llevar la cabo los procedimientos descritos en este manual y documentos relacionados, usted necesitará tener instalado al menos squid-2.5STABLE1. Cualquier versión anterior a ésta será absolutamente inaceptable en lo referente a seguridad e incompatible para los procedimientos descrito en este manual.

65.3. Definiendo elementos de la Lista de Control de Acceso

Lo primero será generar una lista la cual contendrá direcciones de Red y palabras usualmente utilizadas en nombres de ciertos dominios. Ejemplos:

```
\.avi$
\.mp4$
\.mp3$
\.mp4$
\.mpg$
\.mpeg$
\.mov$
\.ra$
\.ram$
\.rm$
\.rpm$
\.vob$
\.wma$
\.wmv$
\.wav$
```

```
\.doc$
\.xls$
\.mbd$
\.ppt$
\.pps$
\.ace$
\.bat$
\.exe$
\.lnk$
\.pif$
\.scr$
\.sys$
\.zip$
\.rar$
```

Esta lista, la cual deberá ser completada con todas las extensiones de fichero que el administrador considere pertinentes, la guardaremos como */etc/squid/listaextensiones*.

65.4. Parámetros en /etc/squid/squid.conf

Debemos definir una *Lista de Control de Acceso* que a su vez defina al fichero */etc/squid/listaextensiones*. Esta lista la denominaremos como "*listaextensiones*". De modo tal, la línea correspondiente quedaría del siguiente modo:

```
acl listaextensiones urlpath_regex "/etc/squid/listaextensiones"
```

Habiendo hecho lo anterior, deberemos tener en la sección de *Listas de Control de Acceso* algo como lo siguiente:

```
#
# Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src 192.168.1.0/255.255.255.0
acl password proxy_auth REQUIRED
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
acl listaextensiones urlpath_regex "/etc/squid/listaextensiones"
```

A continuación especificaremos modificaremos una *Regla de Control de Acceso* existente agregando con un símbolo de *!* que se denegará el acceso a la *Lista de Control de Acceso* denominada *listaextensiones*:

```
http_access allow redlocal !listaextensiones
```

La regla anterior permite el acceso a la *Lista de Control de Acceso* denominada *redlocal*, pero le niega el acceso a todo lo que coincida con lo especificado en la *Lista de Control de Acceso* denominada *listaextensiones*.

Ejemplo aplicado a una *Regla de Control de Acceso* combinando el método de autenticación explicado en el documento Cómo configurar Squid: Acceso por Autenticación y el de denegación hacia Sitios de Red explicado en el documento Cómo configurar Squid: Restricción de acceso a Sitios de Red:

Reglas de control de acceso: denegación de extensiones.

```
#
# INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow redlocal password !sitiosdenegados !listaextensiones
http_access deny all
```

65.4.1. Finalizando procedimiento.

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

```
service squid restart
```

66. Cómo configurar Squid: Restricción de acceso por horarios

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

66.1. Introducción.

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

Este manual considera que usted ya ha leído previamente, a detalle y en su totalidad el manual «Como configurar Squid: Servidor Proxy» y que ha configurado exitosamente Squid como servidor proxy.

66.2. Equipamiento lógico necesario

Para poder llevar la cabo los procedimientos descritos en este manual y documentos relacionados, usted necesitará tener instalado al menos squid-2.5STABLE1.

66.3. Procedimientos

La sintaxis para crear *Listas de control de acceso* que definan horarios es la siguiente:

```
acl [nombre del horario] time [días de la semana] hh:mm-hh:mm
```

Los días de la semana se definen con letras, las cuales corresponden a la primera letra del nombre en inglés, de modo que se utilizarán del siguiente modo:

- **S** - Domingo
- **M** - Lunes
- **T** - Mastes
- **W** - Miercoles
- **H** - Jueves
- **F** - Viernes
- **A** - Sábado

Ejemplo:

```
acl semana time MTWHF 09:00-21:00
```

Esta regla define a la lista *semana*, la cual comprende un horario de 09:00 a 21:00 horas desde el Lunes hasta el Viernes.

Este tipo de listas se aplican en las *Reglas de Control de Acceso* con una mecánica similar a la siguiente: se permite o deniega el acceso en el horario definido en la *Lista de Control de Acceso* denominada *X* para las entidades definidas en la *Lista de Control de Acceso* denominada *Y*. Lo anterior expresado en una *Regla de Control de Acceso*, quedaría del siguiente modo:

```
http_access [allow | deny] [nombre del horario] [lista de entidades]
```

Ejemplo: Se quiere establecer que los miembros de la *Lista de Control de Acceso* denominada *clasematutina* tengan permitido acceder hacia Internet en un horario que denominaremos como *matutino*, y que comprende de lunes a viernes de 09:00 a 15:00 horas.

La defincón para le horario correspondería a:

```
acl clasematutina src 192.168.1.0/255.255.255.0
acl matutino time MTWHF 09:00-15:00
```

La definición de la *Regla de Control de Acceso* sería:

```
http_access allow matutino clasematutina
```

Lo anterior, en resumen, significa que quienes conformen *clasematutina* podrán acceder a Internet de Lunes a Viernes de 09:00-15:00 horas.

66.3.1. Más ejemplos

66.3.1.1. Restringiendo el tipo de contenido

Como se explica en el documento "*Cómo configurar Squid: Restricción de acceso a contenido por extensión*", es posible denegar acceso a cierto tipo de contenido de acuerdo a su extensión. Igual que con otras funciones, se requiere una *Lista de Control de Acceso* y una *Regla de Control de Acceso*

Si se necesita una lista denominada *musica* que defina a todos los ficheros con extensión .mp3, utilizaríamos lo siguiente:

```
acl clasematutina src 192.168.1.0/255.255.255.0
acl musica urlpath_regex \.mp3$
```

Si queremos denegar el acceso al todo contenido con extensión .mp3, la regla quedaría del siguiente modo:

```
http_access allow clasematutina !musica
```

66.3.1.2. Combinando reglas de tiempo y contenido

Si por ejemplo queremos restringir parcialmente el acceso a cierto tipo de contenido a ciertos horarios, pueden combinarse distintos tipos de reglas.

```
acl clasematutina src 192.168.1.0/255.255.255.0
acl matutino time MTWHF 09:00-15:00
acl musica urlpath_regex \.mp3$

http_access allow matutino clasematutina !musica
```

La *Regla de Control de Acceso* anterior especifica **acceso permitido** a en el horario definido como *matutino* a quienes integran la *Lista de Control de Acceso* denominada *clasematutina* a todo contenido [por omisión] **excepto** a los contenidos que coincidan con los definidos en la *Lista de Control de Acceso* denominada *musica*.

66.3.2. Finalizando procedimiento

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

```
service squid restart
```

67. Apéndice: Listas y reglas de control de acceso para Squid

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

67.0.1. Reglas aplicadas

```
# Lista que define método de autenticación:

acl password proxy_auth REQUIRED

# Listas de control de acceso por defecto:
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255

# Listas que definen conjuntos de maquinas
acl redlocal src "/etc/squid/redlocal"
acl privilegiados src "/etc/squid/privilegiados"
acl restringidos src "/etc/squid/restringidos"
acl administrador src 192.168.1.254

# Listas que definen palabras contenidas en un URL
acl porno url_regex "/etc/squid/porno"
# Contenido:
#
# sex
# porn
# girl
# celebrit
# extasis
# drug
# playboy
# hustler

# Lista de sitios inocentes que accidentealmente sean bloqueados
acl noporno url_regex "/etc/squid/noporno"
# Contenido:
#
# missingheart
# wirelessexcite
# msexchange
# msexcel
# freetown
# geek-girls
# adulteducation
```

```
# Listas que definen tipos de extensiones

# Define una lista estricta de extensiones prohibidas
acl multimedia urlpath_regex "/etc/squid/multimedia"
# Contenido:
#
# \.mp3$
# \.avi$
# \.mov$
# \.mpg$
# \.bat$
# \.pif$
# \.sys$
# \.lnk$
# \.scr$
# \.exe$

# Define una lista moderada de extensiones prohibidas
acl peligrosos urlpath_regex "/etc/squid/peligrosos"
# Contenido:
#
# \.bat$
# \.pif$
# \.sys$
# \.lnk$
# \.scr$
# \.exe$

# Define una sola extensión
acl realmedia urlpath_regex \.rm$

# Reglas de control de acceso

# Regla por defecto:
http_access allow localhost

# Ejemplos de reglas de control de acceso
http_access allow restringidos password !porno !multimedia
http_access allow redlocal password !porno !peligrosos
http_access allow privilegiados password !peligrosos
http_access allow administrador

http_access allow noporno all

# Regla por defecto:
http_access deny all
```

68. Cómo configurar un muro cortafuegos con Shorewall y tres interfaces de red

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

68.1. Introducción.

68.1.1. Acerca de Shorewall.

Shorewall (Shoreline Firewall) es una robusta y extensible **herramienta de alto nivel para la configuración de muros cortafuego**. **Shorewall** solo necesita se le proporcionen algunos datos en algunos ficheros de texto simple y éste creará las reglas de cortafuegos correspondientes a través de **iptables**. **Shorewall** puede permitir utilizar un sistema como muro cortafuegos dedicado, sistema de múltiples funciones como **puerta de enlace, dispositivo de encaminamiento y servidor**.

URL: http://www.shorewall.net/

68.1.2. Acerca de Iptables y Netfilter.

Netfilter es un conjunto de *ganchos* (**Hooks**, es decir, técnicas de programación que se emplean para crear cadenas de procedimientos como manejador) dentro del núcleo de GNU/Linux y que son utilizados para interceptar y manipular paquetes de red. El componente mejor conocido es el cortafuegos, el cual realiza procesos de filtración de paquetes. Los *ganchos* son también utilizados por un componente que se encarga del **NAT** (acrónimo de **N**etwork **A**ddress **T**ranslation o Traducción de dirección de red). Estos componentes son cargados como módulos del núcleo.

Iptables es el nombre de la herramienta de espacio de usuario (**User Space**, es decir, área de memoria donde todas las aplicaciones, en modo de usuario, pueden ser intercambiadas hacia memoria virtual cuando sea necesario) a través de la cual los administradores crean reglas para cada filtrado de paquetes y módulos de **NAT**. **Iptables** es la herramienta estándar de todas las distribuciones modernas de GNU/Linux.

URL: http://www.netfilter.org/

68.1.3. Acerca de Iproute.

Iproute es una colección de herramientas (ifcfg, ip, rtmon y tc) para GNU/Linux que se utilizan para controlar el establecimiento de la red **TCP/IP**, así como también el control de tráfico. Aunque **ifconfig** sigue siendo la herramienta de configuración de red estándar en las distribuciones de GNU/Linux, **iproute** tiende a sustituirlo al proveer soporte para la mayoría de las tecnologías modernas de red (incluyendo IP versiones 4 y 6), permitiendo a los administradores configurar los parámetros de red y el control de tráfico.

URL: http://linux-net.osdl.org/index.php/Iproute2

68.1.4. Requisitos.

- Un sistema GNU/Linux con todos los parches de seguridad correspondientes instalados.
- **Shorewall 3.0.8 o versiones posteriores.**
- Tres interfaces de red:
    - Interfaz para acceso hacia Internet.
    - Interfaz para acceso hacia una **DMZ**, tras la cual se podrán colocar servidores.
    - Interfaz para acceso hacia la **LAN** (acrónimo de **L**ocal **A**rea **N**etwork o Área de Red Local).

68.2. Conceptos requeridos.

68.2.1. ¿Qué es una zona desmilitarizada?

Una zona desmilitarizada (**DMZ**), es parte de una red que no está dentro de la red interna (**LAN**) pero tampoco está directamente conectada hacia Internet. Podría resumirse como una red que se localiza entre dos redes. En términos más técnicos se refiere a un área dentro del cortafuegos donde los sistemas que la componen tienen acceso hacia las redes interna y externa, sin embargo no tienen acceso completo hacia la red interna y tampoco acceso completamente abierto hacia la red externa. Los cortafuegos y dispositivos de encaminamiento (*routers*) protegen esta zona con funcionalidades de filtrado de tráfico de red.

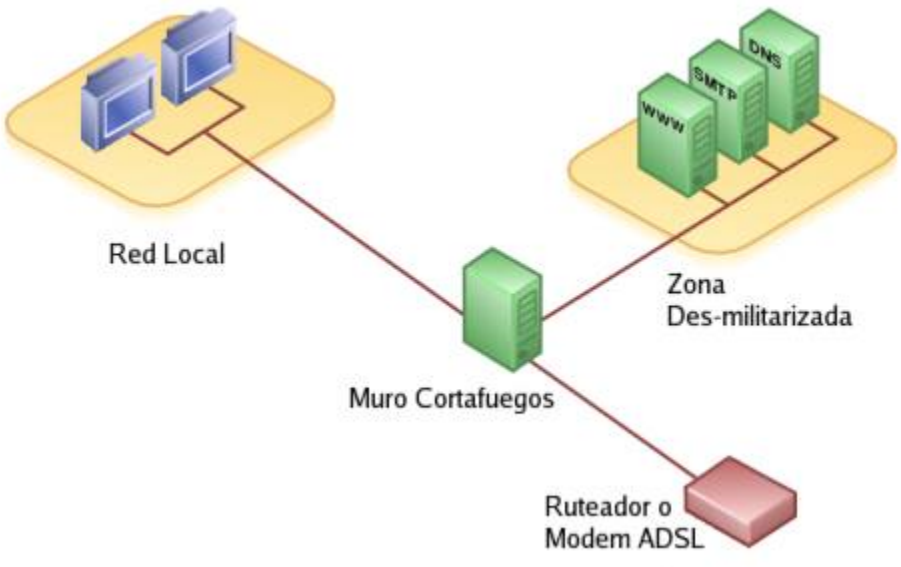


Diagrama de una Zona Desmilitarizada.
Imagen de dominio público tomada de Wikipedia y modificada con el Gimp.

68.2.2. ¿Que es una Red Privada?

Una **Red Privada** es aquella que utiliza direcciones IP establecidas en el RFC 1918. Es decir,

direcciones IP reservadas para **Redes Privadas** dentro de los rangos 10.0.0.0/8 (desde 10.0.0.0 hasta 10.255.255.255), 172.16.0.0/12 (desde 172.16.0.0 hasta 172.31.255.255) y 192.168.0.0/16 (desde 192.168.0.0 hasta 192.168.255.255).

68.2.3. ¿Qué es un NAT?

NAT (acrónimo de **N**etwork **A**ddress **T**ranslation o Traducción de dirección de red), también conocido como enmascaramiento de IP, es una técnica mediante la cual las direcciones de origen y/o destino de paquetes IP son reescritas mientras pasan a través de un dispositivo de encaminamiento (*router*) o muro cortafuegos. Se utiliza para permitir a múltiples anfitriones en una **Red Privada** con direcciones IP para **Red Privada** para acceder hacia una Internet utilizando una sola dirección IP pública.

68.2.4. ¿Qué es un DNAT?

DNAT, (acrónimo de **D**estination **N**etwork **A**ddress **T**ranslation o traducción de dirección de red de destino) es una técnica mediante la cual se hace público un servicio desde una **Red Privada**. Es decir permite redirigir puertos hacia direcciones IP de **Red Privada**. El uso de esta técnica puede permitir a un usuario en Internet alcanzar un puerto en una **Red Privada** (dentro de una **LAN**) desde el exterior a través de un encaminados (*router*) o muro cortafuegos donde ha sido habilitado un **NAT**.

68.3. Procedimientos.

68.3.1. Equipamiento lógico necesario.

- iptables: Controla el código del núcleo de GNU/Linux para filtración de paquetes de red.
- iproute: Conjunto de utilidades diseñadas para utilizar las capacidades avanzadas de gestión de redes del núcleo de GNU/Linux.
- shorewall: Shoreline Firewall.

Shorewall puede descargarse en formato RPM desde http://www.shorewall.net/.

Si dispone de un sistema con Red Hat™ Enterprise Linux 4, CentOS 4 o White Box Enterprise Linux 4, puede utilizar el siguiente depósito yum (utilizado por **Alcance Libre™** para distribuir MailScanner y que además incluye Shorewall):

```
[mailscanner-lpt]
name=MailScanner Alcance Libre para Enterprise Linux 4.0
baseurl=http://www.linuxparatodos.net/lpt/whitebox/4.0/mailscanner/
gpgkey=http://www.linuxparatodos.net/lpt/LPT-RPM-KEY
```

Una vez configurado lo anterior, solo bastará utilizar:

```
yum -y install shorewall
```

68.3.2. Fichero de configuración /etc/shorewall/shorewall.conf

En éste se definen, principalmente, dos parámetros. **STARTUP_ENABLED** y **CLAMPMSS**.

STARTUP_ENABLED se utiliza para activar Shorewall. De modo predefinido está desactivado, solo basta cambiar **No** por **Yes**.

```
STARTUP_ENABLED=Yes
```

CLAMPMSS se utiliza en conexiones tipo PPP (PPTP o PPPoE) y sirve para limitar el **MSS** (acrónimo de **M**aximum **S**egment **S**ize que significa Máximo Tamaño de Segmento). Cambiando el valor **No** por **Yes**, Shorewall calculará el **MSS** más apropiado para la conexión. Si se es osado, puede también especificarse un número en paquetes SYN. La recomendación es establecer **Yes** si se cuenta con un enlace tipo PPP.

```
CLAMPMSS=Yes
```

68.3.3. Fichero de configuración /etc/shorewall/zones

Este fichero se utiliza para definir las zonas que se administrarán con Shorewall y el tipo de zona (firewall, ipv4 o ipsec). La zona **fw** está presente en el fichero **/etc/shorewall.conf** como configuración predefinida. En el siguiente ejemplo se registrarán las zonas de Internet (net), Red Local (loc) y Zona Desmilitarizada (dmz):

```
#ZONE   DISPLAY         OPTIONS
fw      firewall
net     ipv4
loc     ipv4
dmz     ipv4
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

68.3.4. Fichero de configuración /etc/shorewall/interfaces

En éste se establecen cuales serán las interfaces para las tres diferentes zonas. Se establecen las interfaces que corresponden a la Internet, Zona Desmilitarizada **DMZ** y Red Local. En el siguiente ejemplo, se cuenta con una interfaz ppp0 para acceder hacia Internet, una interfaz eth0 para acceder hacia la **LAN** y una interfaz eth1 para acceder hacia la **DMZ**, y en todas se solicita se calcule automáticamente la dirección de transmisión (Broadcast):

```
#ZONE   INTERFACE       BROADCAST       OPTIONS         GATEWAY
net     ppp0            detect
loc     eth0            detect
dmz     eth1            detect
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

En el siguiente ejemplo, se cuenta con una interfaz **eth0** para acceder hacia Internet, una interfaz eth1 para acceder hacia la **LAN** y una interfaz **eth2** para acceder hacia la **DMZ**, y en todas se solicita se calcule automáticamente la dirección de transmisión (Broadcast):

```
#ZONE   INTERFACE       BROADCAST       OPTIONS         GATEWAY
net     eth0            detect
loc     eth1            detect
dmz     eth2            detect
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Hay una cuarta zona implícita que corresponde al cortafuegos mismo y que se denomina **fw**.

Si acaso hubiera un servicio de **DHCP**, sea como cliente, como servidor o como intermediario, en alguna de las interfaces, se debe añadir la opción **dhcp** para permitir la comunicación requerida para este servicio. En el siguiente ejemplo el anfitrión donde opera el muro cortafuegos obtiene su dirección IP, para la interfaz ppp0, a través del servicio **DHCP** del **ISP**; en este mismo anfitrión opera simultáneamente un servidor **DHCP**, el cual es utilizado en la red de área local para asignar direcciones IP; por todo lo anterior se debe activar la opción **DHCP** para las interfaces **ppp0 y eth1**, que correspondientemente son utilizadas por la zona de Internet y la red de área local, pero no es necesario hacerlo para la interfaz **eth2** que es utilizada para la zona de la **DMZ**:

```
#ZONE   INTERFACE       BROADCAST       OPTIONS         GATEWAY
net     ppp0            detect          dhcp
loc     eth1            detect          dhcp
dmz     eth2            detect
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

68.3.5. Fichero de configuración /etc/shorewall/policy

En este fichero se establece como se accederá desde una zona hacia otra y hacia la zona de Internet.

```
#SOURCE         DEST    POLICY  LOG     LIMIT:BURST
loc             net     ACCEPT
dmz             net     ACCEPT
fw              net     ACCEPT
net             all     DROP    info
all             all     REJECT  info
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Lo anterior hace lo siguiente:

1. La zona de la red local puede acceder hacia la zona de Internet.
2. La zona de la DMZ puede acceder hacia la zona de Internet.
3. El cortafuegos mismo puede acceder hacia la zona de Internet.
4. Se impiden conexiones desde Internet hacia el resto de las zonas.
5. Se establece una política de rechazar conexiones para todo lo que se haya omitido.

Todo lo anterior permite el paso entre las diversas zonas hacia Internet, **lo cual no es deseable** si se quiere mantener una política estricta de seguridad. La recomendación es cerrar todo hacia todo e ir abriendo el tráfico de acuerdo a como se vaya requiriendo. Es decir, utilizar algo como lo siguiente:

```
#SOURCE         DEST    POLICY  LOG     LIMIT:BURST
net             all     DROP    info
all             all     REJECT  info
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Lo anterior bloquea todo el tráfico desde donde sea a donde sea. Si es necesario realizar pruebas de diagnóstico desde el cortafuegos hacia Internet para probar conectividad y acceso hacia diversos protocolos, se puede utilizar lo siguiente:

```
#SOURCE         DEST    POLICY  LOG     LIMIT:BURST
fw              net     ACCEPT
net             all     DROP    info
all             all     REJECT  info
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Lo anterior permite al propio cortafuegos acceder hacia la zona de Internet. Esta sería la política más relajada que se pudiera recomendar para mantener un nivel de seguridad aceptable.

68.3.6. Fichero de configuración /etc/shorewall/masq

Se utiliza para definir que a través de que interfaz o interfaces se habilitará enmascaramiento, o **NAT**, y para que interfaz o interfaces o redes se aplicará dicho enmascaramiento. En el siguiente ejemplo, se realizará enmascaramiento a través de la interfaz ppp0 para las redes que acceden desde las interfaces eth0 y eth1:

```
#INTERFACE      SUBNET  ADDRESS         PROTO   PORT(S)         IPSEC
ppp0            eth0
ppp0            eth1
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

En el siguiente ejemplo, se realizará enmascaramiento a través de la interfaz eth0 para las redes 192.168.0.0/24 y 192.168.1.0/24:

```
#INTERFACE      SUBNET  ADDRESS         PROTO   PORT(S)         IPSEC
eth0            192.168.0.0/24
eth0            192.168.1.0/24
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

También es posible hacer **NAT** solamente hacia una IP en particular y para un solo protocolo en particular. En el siguiente ejemplo se hace **NAT** a través de la interfaz ppp0 para la dirección 192.168.3.25 que accede desde la interfaz eth1 y solo se le permitirá hacer **NAT** de los protocolos smtp y pop3. Los nombres de los servicios se asignan de acuerdo a como estén listados en el fichero **/etc/services**.

```
#INTERFACE      SUBNET  ADDRESS         PROTO   PORT(S)         IPSEC
ppp0            eth1    192.168.3.25    tcp     25,110
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

68.3.7. Fichero de configuración /etc/shorewall/rules

Todos los puertos están cerrados de modo predefinido, y es en este fichero donde se habilitan los puertos necesarios. Hay diversas funciones que pueden realizarse.

68.3.7.1. ACCEPT

La acción ACCEPT se hace para especificar si se permiten conexiones desde o hacia una(s) zona (s) un protocolo(s) y puerto(s) en particular. En el siguiente ejemplo se permiten conexiones desde Internet hacia el puerto 80 (www), 25 (smtp) y 110 (pop3). Los nombres de los servicios se asignan de acuerdo a como estén listados en el fichero **/etc/services**.

```
#ACTION SOURCE          DEST                    PROTO   DEST
```

```
#                                                       PORT
ACCEPT  net             fw                      tcp     80,25,110
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

68.3.7.2. REDIRECT

La acción REDIRECT permite redirigir peticiones hacia un puerto en particular. Muy útil cuando se quieren redirigir peticiones para **HTTP** (puerto 80) y se quiere que estas pasen a través de un **Servidor Intermediario** (Proxy) como Squid. En el siguiente ejemplo las peticiones hechas desde la red local y desde la **DMZ** serán redirigidas hacia el puerto 8080 del cortafuegos, en donde hay un **Servidor Intermediario** (Proxy) configurado de modo transparente.

```
#ACTION         SOURCE          DEST            PROTO   DEST
#                                                       PORT
REDIRECT        loc             8080            tcp     80
REDIRECT        dmz             8080            tcp     80
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

68.3.7.3. DNAT

La acción **DNAT** se utiliza para reenviar peticiones desde un puerto del cortafuegos hacia una IP y puerto en particular tanto en la red local como en la **DMZ**. Cabe destacar que para que el **DNAT** funcioné se necesita que:

- Esté habilitado el reenvío de paquetes en **/etc/sysconfig/sysctl.cfg** y **/etc/shorewall/shorewall.conf**
- Los equipos hacia los que se esté haciendo **DNAT** utilicen como puerta de enlace al cortafuegos desde sus correspondientes zonas.

En el siguiente ejemplo, se hace **DNAT** desde la zona de Internet para **HTTP** (puerto 80), **SMTP** (puerto 25) y **POP3** (puerto 110) por TCP y **DNS** (puerto 53) por **TCP** y **UDP** hacia la IP 10.10.10.28 localizada en la zona de la Red Local.

```
#ACTION SOURCE                  DEST            PROTO   DEST
#                                                       PORT
DNAT    net                     dmz:10.10.10.28 tcp     80,25,110,53
DNAT    net                     dmz:10.10.10.28 udp     53
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

68.3.7.4. Ejemplos diversos de reglas.

En el siguiente ejemplo se permite a la zona de Red Local el acceso hacia el puerto 22 (SSH) de cualquier equipo dentro de la **DMZ**:

```
#ACTION SOURCE                  DEST            PROTO   DEST
#                                                       PORT
ACCEPT  loc                     dmz             tcp     22
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

En el siguiente ejemplo se permite solo a la dirección 192.168.2.34 de zona de Red Local el acceso hacia el puerto 22 (SSH) de cualquier equipo dentro de la **DMZ**:

```
#ACTION SOURCE                  DEST            PROTO   DEST
#                                                       PORT
ACCEPT  loc:192.168.2.34        dmz             tcp     22
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

En el siguiente ejemplo se permite solo a la dirección 192.168.2.34 de zona de Red Local el acceso hacia el puerto 22 (ssh) de la dirección 10.10.10.5 que está dentro de la **DMZ**:

```
#ACTION SOURCE                  DEST                    PROTO   DEST
#                                                               PORT
ACCEPT  loc:192.168.2.34        dmz:10.10.10.5          tcp     22
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

En el siguiente ejemplo se hace **DNAT** desde la zona de Internet para los servicios de **HTTP** (puerto 80), **SMTP** (puerto 25) y **POP3** (puerto 110) por **TCP** y **DNS** (puerto 53) por **TCP** y **UDP** hacia diversos servidores localizados **DMZ**:

```
#ACTION SOURCE                  DEST                    PROTO   DEST
#                                                               PORT
DNAT    net                     dmz:10.10.10.1          tcp     80
DNAT    net                     dmz:10.10.10.2          tcp     25,110
DNAT    net                     dmz:10.10.10.3          tcp     53
DNAT    net                     dmz:10.10.10.3          udp     53
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

En el siguiente ejemplo se hace **DNAT** desde la zona de la Red Local para los servicios de **HTTP** (puerto 80), **SMTP** (puerto 25), **POP3** (puerto 110) y **DNS** (puerto 53) hacia diversos servidores localizados **DMZ**:

```
#ACTION SOURCE                  DEST                    PROTO   DEST
#                                                               PORT
DNAT    loc                     dmz:10.10.10.1          tcp     80
DNAT    loc                     dmz:10.10.10.2          tcp     25,110
DNAT    loc                     dmz:10.10.10.3          tcp     53
DNAT    loc                     dmz:10.10.10.3          udp     53
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

En el siguiente ejemplo se hace **DNAT** desde la zona de Internet para los servicios de **HTTP** (puerto 80), **SMTP** (puerto 25), **POP3** (puerto 110) y **DNS** (puerto 53) hacia diversos servidores localizados **DMZ** y limitar la taza de conexiones a diez por segundo con ráfagas de hasta cinco conexiones para cada servicio:

```
#ACTION SOURCE  DEST            PROTO   DEST    SOURCE  ORIGINAL        RATE
#                                       PORT    PORT(S) DEST            LIMIT
DNAT    net     dmz:10.10.10.1  tcp     80      -       -               10/sec:5
DNAT    net     dmz:10.10.10.2  tcp     25,110  -       -               10/sec:5
DNAT    net     dmz:10.10.10.3  tcp     53      -       -               10/sec:5
DNAT    net     dmz:10.10.10.3  udp     53      -       -               10/sec:5
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

En el siguiente ejemplo las peticiones hechas desde la red local (**LAN**) serán redirigidas hacia el puerto 8080 del cortafuegos, en donde hay un **Servidor Intermediario** (Proxy) configurado de modo transparente, limitando la taza de conexiones a diez por segundo con ráfagas de hasta cinco

conexiones. Esto es muy útil para evitar ataques de **DoS** (acrónimo de **D**enial **o**f **S**ervice que se traduce como Denegación de Servicio) desde la red local (**LAN**).

```
#ACTION SOURCE  DEST    PROTO   DEST    SOURCE  ORIGINAL        RATE
#                               PORT    PORT(S) DEST            LIMIT
REDIRET loc     8080    tcp     80      -       -               20/sec:5
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

68.4. Iniciar el cortafuegos y añadirlo a los servicios de arranque del sistema

Para ejecutar por primera vez el servicio, utilice:

```
service shorewall start
```

Para hacer que los cambios hechos a la configuración surtan efecto, utilce:

```
service shorewall restart
```

Para detener el cortafuegos, utilice:

```
service shorewall stop
```

Cabe señalar que detener el cortafuegos también detiene todo tráfico de red, incluyendo el tráfico proveniente desde la **LAN**. Si se desea restaurar el tráfico de red, sin la protección de un cortafuegos, será necesario también utilizar el guión de **iptables**.

```
service iptables stop
```

Lo más conveniente, en caso de ser necesario detener el cortafuegos, es definir que direcciones IP o redes podrán continuar accediendo cuando el cortafuegos es detenido, o cuando éste se encuentra en proceso de reinicio. Esto se define en el fichero **/etc/shorewall/routestopped**, definiendo la interfaz, a través de la cual se permitirá la comunicación, y la dirección IP o red, en un formato de lista separada por comas, de los anfitriones que podrán acceder al cortafuegos. Ejemplo:

```
#INTERFACE      HOST(S)                         OPTIONS
eth0            192.168.1.0/24
eth0            192.168.2.30,192.168.2.31
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Para añadir Shorewall al arranque del sistema, utilice:

```
chkconfig shorewall on
```

69. Cómo configurar SNMP.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

69.1. Introducción.

69.1.1. Acerca de SNMP.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol o Protocolo Simple de administración de red) es uno protocolos del conjunto definido por la Fuerza de Trabajo en Ingeniería de Internet (**IETF** o **I**nternet **E**ngineering **T**ask **F**orce), clasificada en el nivel de aplicación del modelo TCP/IP, y que está diseñado para facilitar el intercambio de información entre dispositivos de red y es ampliamente utilizado en la administración de redes para supervisar el desempeño, la salud y el bienestar de una red, equipo de computo y otros dispositivos.

URL: http://tools.ietf.org/html/rfc1157.

69.1.2. Acerca de Net-SNMP.

Net-SNMP, el equipamiento lógio utilizado en este documento, es un conjunto de aplicaciones utilizados para implementar SNMP v1, SNMP v2c y SNMP v3 utilizando IPv4 y/o IPv6. El proyecto fue iniciado como un conjunto de herramientas SNMP por Steve Waldbusser en la **CMU** (**C**arnegie **M**ellon **U**niversity), Pittsburgh, Pennsylvania, EE.UU., en 1992. Tras ser abandonado, fue retomado por Wes Hardaker en la **UCDavis** (**U**niversity of **C**alifornia, **Davis**), renombrado como **UCD-SNMP** y mejorado para cubrir las necesidades del Departamento de Ingeniería Eléctrica de dicha institución. Tras dejar la universidad, Hardaker continuó el proyecto, cambiando el nombre de éste a **Net-SNMP**.

URL: http://net-snmp.sourceforge.net/

69.2. Equipamiento lógico necesario.

69.2.1. Instalación a través de yum.

Si utiliza **CentOS 4** y **5**, **Red Hat Enterprise Linux 5** o **White Box Enterprise Linux 4** y **5**, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install net-snmp net-snmp-utils
```

69.2.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date -i net-snmp net-snmp-utils
```

69.3. Procedimientos

Este documento considera las siguientes variables que deberán ser reemplazadas por valores reales:

- 192.168.1.0/24: Dirección de red y máscara de subred en bits que correspondan a los de la red local a la que se pertenece.
- Cl4v3-d3-Acc3s0: Cualquier clave de acceso lo suficientemente buena.
- m064.alcancelibre.org: Nombre de anfitrión del sistema donde se está configurando el servicio.
- fulano@algun-dominio.net: Cuenta de correo del administrador del servidor.
- 192.168.1.254: Dirección IP del servidor.

Fichero de configuración /etc/snmp/snmpd.conf.

El fichero **/etc/snmp/snmpd.conf** que se instala junto con el paquete, y puede resultar para algunos una verdadera maraña de comentarios y opciones de todo tipo. Lo más recomendable será crear un fichero nuevo y limpio de contenido para poder partir de algo más simple y funcional.

```
cd /etc/snmp
mv snmpd.conf snmpd.conf-OLD
touch snmpd.conf
```

69.3.1.1. Listas de control de acceso.

Se deben crear las listas de control de acceso (**ACL** o **A**ccess **C**ontrol **L**ist) correspondientes en el fichero **/etc/snmp/snmpd.conf**, las cuales servirán para definir lo que tendrá acceso hacia el servicio **snmpd**. A una de estas listas se le otorgará permiso de acceso de lectura y escritura, para lo que sea necesario en relación con administración, y a la otra de solo lectura. Por razones de seguridad solo la interfaz 127.0.0.1 estará en la lista de lectura escritura. Se otorgará permiso de acceso de solo lectura a una red o bien a una dirección IP en la otra lista de control de acceso.

Considerando lo anterior, se podrían agregar un par de líneas como las siguientes:

```
com2sec local 127.0.0.1/32 Cl4v3-d3-Acc3s0
com2sec miredlocal 192.168.1.0/24 Cl4v3-d3-Acc3s0
```

En lo anterior la primera línea significa que habrá una lista de control de acceso denominada *«local»* y que corresponderá solo a **127.0.0.1/32**, asignando *Cl4v3-d3-Acc3s0* como clave de acceso. La segunda línea hace lo mismo pero definiendo a la red **192.168.1.0/24**. Se puede definir lo que uno guste mientras no sea la clave de **root**, esto debido a que dicha clave se transmite a través de la red en forma de texto simple (es decir, sin cifrar).

69.3.1.2. Definición de grupos.

Se crean al menos dos grupos: **MyRWGroup** y **MyROGroup**. El primero será un grupo al que se

asignarán más adelante permisos de **lectura escritura** y el segundo será un grupo al que posteriormente se asignarán permisos de **solo lectura**. Por cada grupo se asignan tres líneas que especifican el tipo de acceso que se permitirá en un momento dado a un grupo en particular. Es decir, **MyRWGroup** se asocia a **local** y **MyROGroup** a **miredlocal**.

```
#Se asigna local al grupo de lectura escritura
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local

#Se asigna miredlocal al grupo de solo lectura
group MyROGroup v1 miredlocal
group MyROGroup v2c miredlocal
group MyROGroup usm miredlocal
```

69.3.1.3. Ramas permitidas.

Se especifican las ramas que se van a permitir ver a través del servicio. Lo más común, para, por ejemplo, utilizarse con **MRTG**, es lo siguiente:

```
## name   incl/excl subtree   mask(optional)
view all  included  .1        80
```

69.3.1.4. Asignación de permisos a los grupos.

Se debe especificar que permisos tendrán los dos grupos, **MyROGroup** y **MyRWGroup**. Son de especial interés las últimas columnas.

```
## group         context  sec.model sec.level prefix read   write notif
access MyROGroup ""       any       noauth    exact  all    none  none
access MyRWGroup ""       any       noauth    exact  all    all   all
```

69.3.1.5. Parámetros de carácter informativo.

Se definen dos parámetros de carácter informativo para que cuando utilicen aplicaciones cliente como **MRTG** se incluya algo de información acerca de que sistema se está accediendo.

```
syslocation Servidor Linux en SU-SERVIDOR.algun-dominio.net
syscontact Administrador (fulano@algun-dominio.net)
```

69.3.2. Un ejemplo funcional de configuración.

El ejemplo que mostramos a continuación se utiliza en todas los equipos que posee el autor en casa y en la oficina. Solo hay que reemplazar el valor **redlocal** por lo que uno considere apropiado y reemplazar el valor **192.168.1.0/24** por el valor de **la red** o la dirección IP desde donde se requiera acceder con un cliente **snmp**, como **MRTG**.

```
# Listas de control de acceso (ACL)
## sec.name source community (alias clave de acceso)
com2sec local 127.0.0.1/32 Cl4v3-d3-Acc3s0
com2sec miredlocal 192.168.1.0/24 Cl4v3-d3-Acc3s0

#Se asigna ACL al grupo de lectura escritura
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local

#Se asigna ACL al grupo de solo lectura
group MyROGroup v1 miredlocal
group MyROGroup v2c miredlocal
group MyROGroup usm miredlocal

# Ramas MIB que se permiten ver
## name   incl/excl subtree   mask(optional)
view all  included  .1        80

# Establece permisos de lectura y escritura
## group         context  sec.model sec.level prefix read   write notif
access MyROGroup ""       any       noauth    exact  all    none  none
access MyRWGroup ""       any       noauth    exact  all    all   all

# Información de Contacto del Sistema
syslocation Servidor Linux en m064.alcancelibre.org
syscontact Administrador (fulano@algun-dominio.net)
```

Si es necesario añadir más equipos para que accedan al servicio **snmpd**, solo hay que hacer lo siguiente:

- Agregar una ACL con un nombre único. Ejemplo:

  ```
  com2sec micueva 192.168.1.251 Cl4v3-d3-Acc3s0
  ```

- Agregar un juego reglas que asignen al grupo, en este caso **micueva**, con lo siguiente:

  ```
  group otrogrupo v1 local
  group otrogrupo v2c local
  group otrogrupo usm local
  ```

- Agregar una línea donde se establece que permisos tendrá el grupo **otrogrupo**. En este ejemplo, va a ser de solo lectura:

  ```
  access MyROGroup "" any noauth exact all none none
  ```

69.3.3. Iniciar, detener y reiniciar el servicio snmpd.

Para ejecutar por primera vez el servicio **snmpd**, utilice:

```
service snmpd start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service snmpd restart
```

Para detener el servicio **snmpd** utilice:

```
service snmpd stop
```

69.3.4. Agregar el servicio snmpd al arranque del sistema.

Para hacer que el servicio de **snmpd** esté activo con el siguiente inicio del sistema, en todos los niveles de corrida (2, 3, 4, y 5), se utiliza lo siguiente:

```
chkconfig snmpd on
```

69.4. Comprobaciones.

Considerando, **como ejemplo**, que sea signó como clave de acceso **Cl4v3-d3-Acc3s0** en un sistema cuya dirección IP es **192.168.1.254**, para probar si la configuración funciona, solo hay que ejecutar los dos siguiente mandatos a fin verificar que devuelvan información acerca del sistema consultado.

```
snmpwalk -v 1 192.168.1.254 -c Cl4v3-d3-Acc3s0 system

snmpwalk -v 1 192.168.1.254 -c Cl4v3-d3-Acc3s0 interfaces
```

69.5. Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir los puerto 161 y 162 por UDP (**SNMP** y **SNMPTRAP**, respectivamente).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** en un sistema con una zona (**net**), correspondería a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      udp     161,162
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** en un sistema con dos zonas (**net** y **loc**), donde solo se va a permitir el acceso al servicio **snmpd** desde la red local, correspondería a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  loc     fw      udp     161,162
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

70. Cómo configurar MRTG.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

70.1. Introducción.

70.1.1. Acerca de MRTG.

MRTG (**M**ulti **R**outer **T**raffic **G**rapher) es una herramienta, escrita en C y Perl por Tobias Oetiker y Dave Rand, que se utiliza para supervisar la carga de tráfico de interfaces de red. **MRTG** genera los resultados en ficheros HTML con gráficos, que proveen una representación visual de este tráfico.

MRTG utiliza **SNMP** (**S**imple **N**etwork **M**anagement **P**rotocol o Protocolo Simple de administración de red) para recolectar los datos de tráfico de un determinado dispositivo (dispositivos encaminamiento o servidores), por tanto es requisito contar con al menos un sistema a supervisar con **SNMP** funcionando, y con dicho servicio correctamente configurado.

70.2. Equipamiento lógico necesario.

70.2.1. Instalación a través de yum.

Si utiliza **CentOS 4** o **White Box Enterprise Linux 4**, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install mrtg
```

70.2.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date -i mrtg
```

70.3. Procedimientos

Este documento considera las siguientes variables que deberán ser reemplazadas por valores reales:

- Cl4v3-d3-Acc3s0: Cualquier clave de acceso lo suficientemente buena.
- 192.168.1.1: Dirección IP del servidor.

- 192.168.1.2, 192.168.1.3, 192.168.1.4: Direcciones IP de otros servidores que estén configurados con SNMP y se quiera supervisa con MRTG.

Accediendo al sistema como el usuario **root**, se debe generar el directorio de trabajo de MRTG del siguiente modo:

```
mkdir -p /var/www/mrtg/miredlocal
```

Debe respladarse el fichero de configuración predeterminado, con el fin de poder restaurarlo en el futuro si fuese necesario:

```
cp /etc/mrtg/mrtg.cfg /etc/mrtg/mrtg.cfg-OLD
```

Para **generar el fichero** de configuración para supervisar una sola dirección IP, **utilice el siguiente mandato**, donde **Cl4v3-d3-Acc3s0** es la clave de acceso definida en la configuración de **SNMP** del sistema involucrado:

```
cfgmaker \
--global "workdir: /var/www/mrtg/miredlocal" \
--global "Options[_]: bits,growright" \
--output /etc/mrtg/mrtg.cfg \
Cl4v3-d3-Acc3s0@192.168.1.1
```

Para **generar el fichero** de configuración para supervisar varias direcciones IP, **utilice el siguiente mandato**, donde **Cl4v3-d3-Acc3s0** es la clave de acceso si esta fue definida así en la configuración de **SNMP** de todos los sistemas involucrados:

```
cfgmaker \
--global "workdir: /var/www/mrtg/miredlocal" \
--global "Options[_]: bits,growright" \
--output /etc/mrtg/mrtg.cfg \
--community=Cl4v3-d3-Acc3s0 \
192.168.1.1 \
192.168.1.2 \
192.168.1.3 \
192.168.1.4
```

70.4. Comprobaciones

El paquete de **MRTG** incluye un guión para **crond**, el cual se instala en la ruta **/etc/cron.d/mrtg**, de modo que éste ejecute **MRTG**, de forma **automática**, cada 5 minutos. Si se quiere comprobar la configuración solo es necesario esperar algunos minutos y consultar los resultados. Si se quiere generar un reporte al momento, utilice el mandato **mrtg** del siguiente modo:

```
env LANG=C mrtg /etc/mrtg/mrtg.cfg
```

Se debe reiniciar el servico **httpd** (Apache) a fin de cargar la configuración necesaria y específicada en el fichero **/etc/httpd/conf.d/mrtg.conf**, la que permitirá acceder hacia los reportes de **MRTG** a través de interfaz por protocolo **http**.

```
service httpd restart
```

Se pueden observarlos resultados con cualquier navegador gráfico examinando el directorio **/var/www/mrtg/miredlocal** del disco duro, o bien accediendo a través de hacia *http://127.0.0.1/mrtg/miredlocal/**192.168.1.1**_2.html*, considerando, **como ejemplo**, que se desea observar el reporte de el sistema con la dirección IP 192.168.1.1.

71. Cómo configurar Asterisk 1.4 para utilizar Ekiga y Linphone como clientes SIP.

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

71.1. Introducción.

71.1.1. Acerca de Ekiga.

Ekiga es una aplicación para VoIP (**V**oice **o**ver **IP** o Voz sobre IP) y vídeo-conferencia, distribuido bajo los términos de la licencia GNU/GPL. Incluye soporte para los protocolos **SIP** (**S**ession **I**nitiation **P**rotocol o Protocolo de Inicialización de Sesiones) y H.323.

El proyecto fue iniciado por Damien Sandras con el nombre **GnomeMeeting**, como parte de los requisitos para graduarse de la Universidad Católica de Louvain, en la ciudad de Bruselas, Bélgica. El nombre del proyecto fue cambiado por **Ekiga** el 18 de enero de 2006, con el fin de evitar se le asociara como equivalente de Microsoft NetMeeting. Actualmente es mantenido por una comunidad de desarrolladores, con Sandras como líder.

URL: http://www.ekiga.org/

71.1.2. Acerca de Asterisk.

Asterisk es una implementación de código abierto para central telefónica (**PBX**, **P**rivate **B**ranch e**X**change o **P**rivate **B**usiness e**X**change). Cuenta con un doble licenciamiento, GNU/GPL y licencia propietaria. Esta última es con el objeto de poder incluir soporte para el protocolo G.729, el cual está sujeto a las limitaciones de una patente, aunque el codificador correspondiente funciona indistintamente con una u otra versión.

Asterisk está diseñado para servir como **PBX**. Como cualquier **PBX**, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí, e incluso conectar a un proveedor de **VoIP** o bien a una , tanto básicos como primarios.

La versión libre de **Asterisk** incluye **todas** las funcionalidades de las más costosas alternativas de código cerrado, como son correo de voz, llamada en conferencia, respuesta interactiva de voz (a través de menús del teléfono) y distribución automática de llamadas.

URL: http://www.asterisk.org/

71.1.3. Acerca de Linphone.

Linphone es un cliente **SIP** para **VoIP** creado por Simon Morlat. Está hecho en GTK2, es pequeño, ligero y muy estable e incluye además **linphonec**, una **poderosa** versión para terminales en modo

texto. La versión de **AL Desktop** incluye soporte para voz y mensajes instantáneos, pero el código incluye también soporte para vídeo.

Características:

- Cumple con los estándares **SIP** (**S**ession **I**nitiation **P**rotocol o Protocolo de Inicialización de Sesiones).
- Puede registrarse en servidores Asterisk.
- Soporte para subscripción de **VoIP** hacia RTC (**R**ed **T**elefónica **C**onmutada, también conocida como **PSTN** o **P**ublic **S**witched **T**elephone network). Es decir, telefonía **red telefónica básica.**
- Es equipamiento lógico libre.
- Es muy estable en GNU/Linux, y probablemente también en los diversos sabores de Unix.
- Hay versión estable para Windows, pero con algunas funciones aún sin portar.
- Funciona bien con las siguientes implementaciones, probadas por el autor de Linphone: eStara softphone, Teléfonos Pingtel, Hotsip, Vocal (Vivida), Siproxd y Partysip

URL: http://www.linphone.org/

71.1.4. Acerca del protocolo SIP.

SIP (**S**ession **I**nitiation **P**rotocol o Protocolo de Inicialización de Sesiones) es un protocolo propuesto como estándar por la **IETF** (**I**nternet **E**ngineering **T**ask **F**orce o Fuerza de Trabajo en Ingeniería de Internet), descrito en el RFC 3261, para la iniciación, modificación y finalización de sesiones interactivas de usuario, en las cuales intervienen elementos de medios electrónicos, como pueden ser vídeo, voz y mensajería instantánea. Es uno de los varios protocolos de señalización para la tecnología de Voz sobre IP (**VoIP** o **V**oice **o**ver **IP**), y forma parte de la arquitectura IMS (**I**P **M**ultimedia **S**ubsystem o Subsistema multimedios por IP).

URL: http://tools.ietf.org/html/rfc3261

71.2. Equipamiento lógico necesario.

Considerando que se va a instalar el cliente (**Ekiga**) en un sistema distinto al del servidor que sustentará a Asterisk, las instalaciones de equipamiento lógico correspondientes proceden de la siguiente forma.

71.2.1. Instalación de servidor Asterisk.

Para poder llevar al cabo los procedimientos descritos en este y otros documentos relacionados, usted necesitará tener instalado al menos lo siguiente, lo cual no está incluido en la instalación estándar de **CentOS 4**, **Red Hat™ Enterprise Linux 4** o **White Box Enterprise Linux 4** (disponible a través de los depósitos de equipamiento lógico de Alcance libre).

- asterisk-1.4.1
- asterisk-addons-1.4.0
- asterisk-sounds-es
- gsm-1.0.12
- libidn-0.6.9
- libpri-1.4.0
- spandsp-0.0.3-7_pre28
- speex-1.2

- zaptel-1.4.0

71.2.1.1. Instalación a través de yum.

Si dispone de un servidor con **CentOS 4**, **Red Hat™ Enterprise Linux 4** o **White Box Enterprise Linux 4**, puede utilizar el el depósito yum de Alcance Libre para servidores en producción:

```
[alcance-libre]
name=Alcance Libre para Enterprise Linux 4
baseurl=http://www.alcancelibre.org/al/el/4/
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

La instalación solo requiere utilizar lo siguiente:

```
yum -y install asterisk asterisk-addons asterisk-sounds-es zaptel kernel-module-zaptel
```

Al terminar, solo bastará iniciar el servicio **asterisk**, puesto que de forma predeterminada arrancará solo la siguiente vez que reinicie el sistema.

```
service asterisk start
```

71.2.2. Instalación de cliente Ekiga.

71.2.2.1. Instalación a través de yum.

Si dispone de un escritorio con **AL Desktop** en **CentOS 4 Red Hat™ Enterprise Linux 4** o **White Box Enterprise Linux 4**, puede utilizar el depósito yum de **AL Desktop**:

```
[AL-Desktop]
name=Enterprise Linux $releasever - $basearch - AL Desktop
mirrorlist=http://www.alcancelibre.org/al/el4/al-desktop
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

La instalación requiere utilizar lo siguiente:

```
yum -y install ekiga
```

71.2.3. Instalación de clientes Linphone y Linphonec.

71.2.3.1. Instalación a través de yum.

Si dispone de un escritorio con **AL Desktop** en **CentOS 4 Red Hat™ Enterprise Linux 4** o **White Box Enterprise Linux 4**, puede utilizar el depósito yum de **AL Desktop**:

```
[AL-Desktop]
name=Enterprise Linux $releasever - $basearch - AL Desktop
mirrorlist=http://www.alcancelibre.org/al/el4/al-desktop
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

La instalación requiere utilizar lo siguiente:

```
yum -y install linphone
```

71.3. Procedimientos.

71.3.1. Configuración de servidor Asterisk.

71.3.1.1. Fichero /etc/asterisk/manager.conf.

Si se considera necesario, se puede configurar el acceso remoto hacia el gestor de Asterisk. Se requiere definir un usuario, las correspondiente clave de acceso y los privilegios necesarios, a fin de poder permitir utilizar diversas herramientas para la administración y/o supervisión remota(s). En el siguiente ejemplo para el contenido del fichero **/etc/asterisk/manager.conf**, se activa acceso remoto a través del **puerto 5038**, se define **admin** como usuario, **secreto** como clave de acceso y se otorgan todos privilegios.

```
[general]
displaysystemname = yes
enabled = yes
;webenabled = yes
port = 5038
;httptimeout = 60
; De modo predefinido, el gestor de Asterisk escuchará peticiones
; por cualquier interfaz activa en el sistema, pero puede
; definirse, por ejmeplo, que solo se permitan conexiones desde
; la dirección IP de red privada (RFC 1918).
bindaddr = 0.0.0.0
;displayconnects = yes
;timestampevents = yes

[admin]
secret = secreto
deny=0.0.0.0/0.0.0.0
permit=192.168.12.0/255.255.255.128
writetimeout = 100
read = system,call,log,verbose,command,agent,user,config
write = system,call,log,verbose,command,agent,user,config
```

71.3.1.2. Fichero /etc/asterisk/sip.conf.

El siguiente ejemplo corresponde a la configuración de tres cuentas **SIP** (101, 102 y 103). El contenido se agrega, o bien modifica opciones, al fichero **/etc/asterisk/sip.conf**.

```
[general]
context=default
srvlookup=yes
videosupport=yes ; Asterisk puede también gestionar las conferencias de vídeo
disallow=all   ; Desactivar todos los codificadores
allow=alaw     ; Permitir codificadores en orden de preferencia
allow=ilbc
allow=gsm
allow=h261
; El paquete asterisk-sounds-es de alcance libre instala los ficheros de audio
; al español. Por tanto, se puede definir éste como idioma pata los mensajes.
language=es
```

```
; Realizar registro en ekiga.net con un usuario y clave de acceso válidos y
; encaminar las llamadas hacia la extensión 101
register => usuario:clave-de-acceso@ekiga.net/101

; Hacer acceder a Asterisk hacia una cuenta en ekiga.net para permitir
; realizar llamadas
[ekiga]
type=friend
username=usuario
secret=clave-de-acceso
host=ekiga.net
canreinvite=no
qualify=300
; Si se utiliza asterisk 1.4.x:
insecure=port,invite
; Si se utiliza asterisk 1.2.x:
; insecure=very

; Extensión 101
[101]
type=friend
secret=secreto1
qualify=yes    ; El par correspondiente está no más allá de 2000 mS.
nat=no         ; No hay NAT.
host=dynamic   ; Dispositivo se registrará con servidor.
canreinvite=no ; Asterisk tratará de redireccionar de forma predeterminada.
context=home   ; Contexto predefinido (ver → extensions.conf)
;port=5061     ; Descomentar si Ekiga o Linphone y Asterisk están en el mismo sistema.

; Extensión 102
[102]
type=friend
secret=secreto2
qualify=yes
nat=no
host=dynamic
canreinvite=no
context=home
;port=5061

; Extensión 103
[103]
type=friend
secret=secreto3
qualify=yes
nat=no
host=dynamic
canreinvite=no
context=home
;port=5061
```

71.3.1.3. Fichero /etc/asterisk/voicemail.conf.

A fin de habilitar el acceso al correo de voz para cada extensión, y al mismo tiempo especificar una cuenta de correo electrónico hacia la cual se enviará un mensaje de correo electrónico con el mensaje de voz como adjunto, solo es necesario verificar que las siguientes opciones estén

habilitadas. En el ejemplo, se configuran las cuentas para las extensiones 101, 102 y 103.

```
[general]
; Escoger el formato del correo de voz. Recomendado usar WAV, por
; razones de compatibilidad.
format=wav
;
; Si se dispone de espacio suficiente en la cuenta de correo, la
; siguiente opción especifica que se adjunte el mensaje de voz a un
; mensaje de correo electrónico, de modo que se pueda escuchar al dar
; clic desde el cliente.
;
attach=yes
;
[default]
; Cada buzón de voz se lista en el siguiente formato:
; buzón => clave de acceso,Nombre de persona,correo electrónico,correo
; electrónico de servicio de localizador. Ejemplos:
101 => secreto1,Nombre,alguien@algo.algo,numero@mi-celular.algo
102 => secreto2,Nombre,otro@algo.algo
103 => secreto3,Nombre,alguien-mas@algo.algo
```

71.3.1.4. Fichero /etc/asterisk/extensions.conf.

El siguiente ejemplo corresponde a la configuración de tres extensiones (101, 102 y 103). El contenido se agrega al fichero **/etc/asterisk/extensions.conf**.

```
; Macro que habilita el uso de correo de voz, de modo que no hará falta
; repetir complejas configuraciones en cada cuenta.
[macro-correovoz]
exten => s,1,Dial(${ARG1},20)
exten => s,2,Goto(s-$DIALSTATUS},1)
exten => s-NOANSWER,1,Voicemail(u${MACRO_EXTEN})
exten => s-NOANSWER,2,Hangup()
exten => s-BUSY,1,Voicemail(b${MACRO_EXTEN})
exten => s-BUSY,2,Hangup()
exten => _s-.,1,Goto(s-NOANSWER,1)

[home]
; Extensión 101
exten => 101,1,Macro(correovoz,SIP/101)

; Extensión 102
exten => 102,1,Macro(correovoz,SIP/102)

; Extensión 103
exten => 103,1,Macro(correovoz,SIP/103)

; Lo siguiente permite acceder al correo de voz desde Ekiga, simplemente
; marcando el número 8
exten => 8,1,VoiceMailMain(s${CALLERIDNUM})
exten => 8,2,Hangup

; Prueba de Eco
exten => 600,1,Answer()
exten => 600,2,Playback(demo-echotest)
exten => 600,3,Echo()
exten => 600,4,Playback(demo-echodone)
exten => 600,5,Hangup()

; Lo siguiente permite realizar llamadas hacia cuentas de Ekiga.net
; solo antecediendo un número 9 antes de la cuenta. Es decir:
; Si antes se tenía que marcar sip:alguien@ekika.net, ahora se hará
; como sip:9alguien@ekiga.net
```

```
exten => _9.,1,Dial(SIP/ekiga/${EXTEN:1},20,r))
```

Al terminar, solo bastará reiniciar el servicio **asterisk** para que surtan efecto los cambios.

```
service asterisk restart
```

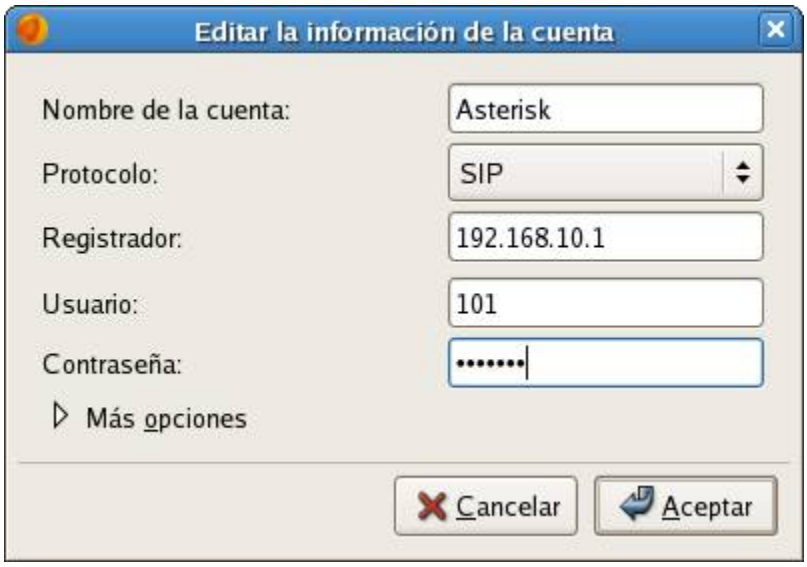
También puede ingresar a la interfaz de línea de mandatos (**CLI** o **C**ommand **L**ine **I**nterface), desde el servidor que sustenta a Asterisk, utilizando el mandato **asterisk -r**, y ejecutando desde ésta el mandato **reload**. Al terminar, ingrese el mandato **exit** para salir de la interfaz de línea de mandatos.

71.3.2. Configuración de cliente Ekiga.

Ekiga, además de ajustar los niveles de audio del sistema para permitir el funcionamiento del micrófono (captura), requiere y desactivar cualquier método de **NAT** que esté especificado (por lo general, **STUN**).

En la versión 2.0.7, si activa la casilla de **cancelación de eco**, Ekiga no enviará el **DTMF** y no será posible autenticar en el buzón de voz. **Deje la casilla sin activar**.

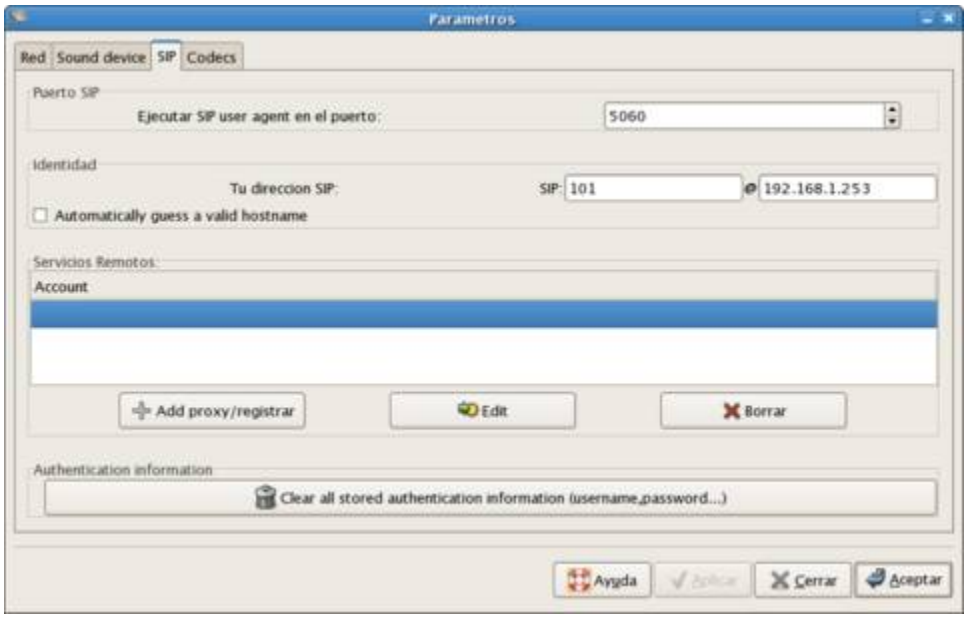
Al terminar y aplicar los cambios, se debe acceder al menú de la aplicación *Editar* → *Cuentas* y añadir una nueva cuenta tipo **SIP**, especificando un nombre para identificar la cuenta, la IP del servidor Asterisk, el usuario a utilizar y la correspondiente clave de acceso.



Al terminar, solo se necesitará hacer clic en la casilla para activar la cuenta y registrarse en el servidor.

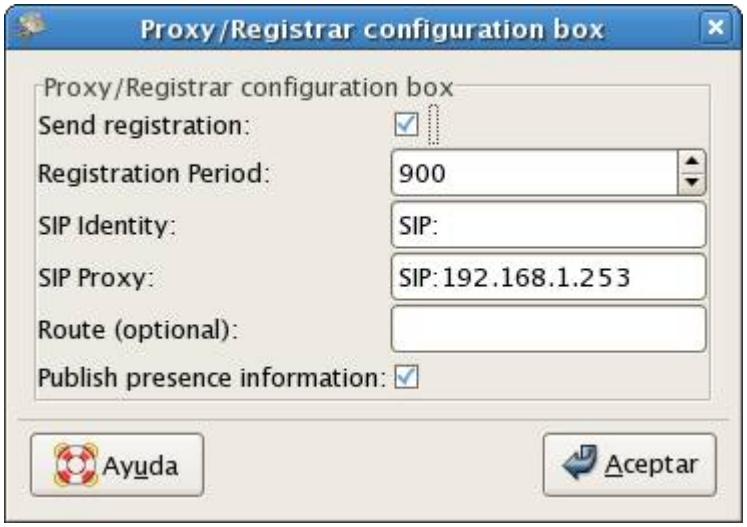
71.3.3. Configuración de cliente Linphone y Linphonec.

Solo es necesario añadir la cuenta desde la pestaña **SIP** de la ventana de preferencias. Un pequeño error en el despliegue de texto en la versión 1.6.0 hace que no se muestren las cuentas que se dan de alta, pero de hecho deberán estar ahí.



Pestaña **SIP** de la ventana de preferencias.

Se hace clic en el botón **Add proxy/registar**, acción que abrirá una ventana para ingresar los datos necesarios.



Ventana de registro de cuenta.

Si se prefiere, a fin de verificar datos y hacer otros ajustes, puede editarse el fichero **~/linphonerc** y modificar, con cualquier editor de texto, la configuración de las cuentas, ejemplificada a continuación:

```
[sip]
sip_port=5060
guess_hostname=0
contact=sip:101@192.168.1.253
inc_timeout=15
use_info=0
```

```
use_ipv6=0
default_proxy=0

[proxy_0]
reg_proxy=SIP:192.168.1.253
reg_expires=900
reg_sendregister=1
publish=1

[auth_info_0]
username=101
userid=101
passwd=secreto1
realm="asterisk"
```

La configuración hecha es utilizada tanto por el cliente gráfico, **linphone**, como el cliente para terminal de texto, **linphonec**.

Particularmente es muy interesante las aplicaciones prácticas **linphonec**, el cual se puede utilizar en sistemas sin entorno gráfico. Puede dejarse iniciando automáticamente en algún guión con la opción **-a** para contestar llamadas automáticamente y utilizarlo como la imaginación lo determine. Es ideal para ser utilizado en terminal telefónica en clientes ligeros o equipos obsoletos.

71.4. Comprobaciones.

Para si uno marca **600**, deberá contestar el servidor Asterisk con un mensaje de *prueba de eco*. Si se conectan los clientes al servidor Asterisk, podrán comunicarse entre si marcando solo el número de extensión, o bien como *sip:extension@servidor*. Ejemplo: *sip:103@192.168.10.1*. Marcando el número **8** desde Ekiga, se podrá acceder al correo de voz.

Si necesita depurar la configuración, puede hacerlo ingresando a la interfaz de línea de mandatos utilizando el mandato **asterisk -r**, añadiendo de una a cinco letras **v** para indicar el nivel de depuración. Ejemplo:

```
asterisk -vvvr
```

Lo anterior mostrará mensajes de depuración de nivel 3. Al terminar, ingrese el mandato **exit** para salir de la interfaz de línea de mandatos.

71.5. Modificaciones necesarias en el muro cortafuegos en el servidor Asterisk.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir el puerto 5060 por UDP para comunicaciones a través de protocolo **SIP**, y opcionalmente los puertos 4569,5036, 10000:20000 y 2727 por UDP, de forma correspondiente para los protocolos **IAX2**, **IAX**, **RTP** y **MGCP**, en el caso dado que se quiera acceder hacia éstos con clientes que incluyan dicho soporte. Si se va a utilizar herramientas para administración y/o supervisión remota(s), el puerto del gestor de Asterisk corresponde al 5038 por TCP.

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall**, como cortafuegos de una sola zona (**net**), correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      udp     5060
ACCEPT  net     fw      tcp     5038
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall**, como cortafuegos de dos zonas (**net** y **loc**), considerando que se desea permitir acceso tanto desde redes públicas como privadas, pero el acceso al gestor de Asterisk solo desde la red local, correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      udp     5060
ACCEPT  loc     fw      udp     5060
ACCEPT  loc     fw      tcp     5038
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

71.6. Bibliografía.

- http://wiki.ekiga.org/index.php/Ekiga_as_an_Asterisk_client
- http://wiki.ekiga.org/index.php/Asterisk_and_Voicemail
- http://wiki.ekiga.org/index.php/Connecting_Asterisk_to_ekiga.net
- http://en.wikipedia.org/wiki/Asterisk_%28PBX%29
- http://en.wikipedia.org/wiki/Ekiga
- http://es.wikipedia.org/wiki/Session_Initiation_Protocol
- http://tools.ietf.org/html/rfc3261

72. Cómo instalar correctamente Java™ a partir de paquete RPM

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

72.1. Procedimiento

1. Dirija el navegador hacia el sitio de red de Java y proceda a descargar el paquete auto-extraíble que contiene el RPM de *Java™ 2 Runtime Environment* 1.4.2 desde http://www.java.com/en/download/linux_manual.jsp.

2. Haga ejecutable jre-1_5_0_04-linux-i586-rpm.bin a fin de poder extraerlo:

   ```
   chmod +x jre-1_5_0_04-linux-i586-rpm.bin
   ```

3. Ejecute jre-1_5_0_04-linux-i586-rpm.bin:

   ```
   ./jre-1_5_0_04-linux-i586-rpm.bin
   ```

4. **Lea en su totalidad** la licencia y confirme que acepta los términos de la misma, si ése es el caso. Una vez hecho lo anterior, se extraerá automáticamente el paquete RPM j2re-1_5_0_04-linux-i586.rpm.

5. Como root instale jre-1_5_0_04-linux-i586.rpm:

   ```
   su
   rpm -Uvh jre-1_5_0_04-linux-i586.rpm
   ```

6. Proceda a crear el fichero **/etc/profile.d/java.sh** a fin de incluir en éste una línea que añadirá la ruta de binarios de Java 2 (/usr/java/jre1.5.0_04/bin, o lo que corresponda según la versión del paquete RPM) a las rutas predeterminadas de ejecutables del sistema.

   ```
   export PATH=/usr/java/jre1.5.0_04/bin:$PATH
   JAVA_HOME="/usr/java/jre1.5.0_04/"
   export JAVA_HOME
   ```

7. Haga ejecutable **/etc/profile.d/java.sh:**

   ```
   chmod 755 /etc/profile.d/java.sh
   ```

8. Instale la extensión (Plug-in) Java™ para Mozilla del siguiente modo:

   Si utiliza una versión de Mozilla, Firefox o Netscape compilada con GCC 3.x (Red Hat™

Enterprise Linux 3, CentOS 3.0 **y versiones posteriores**), deberá ejecutar:

```
cd /usr/lib/mozilla/plugins/
ln -s /usr/java/jre1.5.0_04/plugin/i386/ns7/libjavaplugin_oji.so ./
```

Si utiliza una versión de Mozilla o Netscape compilada con GCC 2.96 (Red Hat™ Enterprise Linux 2.1 y CentOS 2.1), deberá ejecutar:

```
cd /usr/lib/mozilla/plugins/
ln -s /usr/java/jre1.5.0_04/plugin/i386/ns7-gcc29/libjavaplugin_oji.so ./
```

9. **En algunas versiones** del paquete RPM se **incluye un fichero que muestra una entrada para el escritorio**, pero hay un error de omisión en dicho fichero. Éste es responsable de que las preferencias de Java™ aparezcan en el menú de preferencias del escritorio. De existir, modifique el fichero **/usr/share/applications/sun_java.desktop** y añada un ";" (punto y coma) al final de la línea **Categories=Application;Settings**, de modo tal que el contenido quede de la siguiente manera:

```
[Desktop Entry]
Name=Java
Comment=Java Control Panel
Exec=/usr/java/jre1.5.0_04/bin/ControlPanel
Icon=/usr/java/jre1.5.0_04/plugin/desktop/sun_java.png
Terminal=false
Type=Application
Categories=Application;Settings;
```

Si el fichero no existe, puede generarlo con el contenido anteriormente mostrado.

10. **Cierre todas las sesiones gráficas y de consola que estén abiertas (NO SIGNIFICA QUE DEBE REINICIAR EL SISTEMA) y vuelva a ingresar como usuario**.

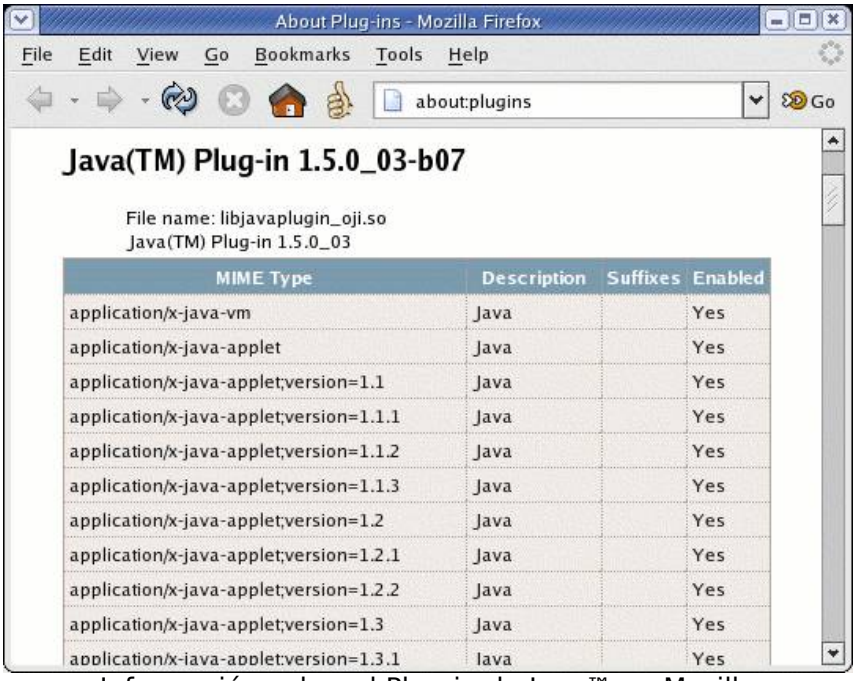
72.2. Comprobaciones

Para comprobar si Java™ quedó instalado correctamente, ejecute lo siguiente desde una terminal

```
which java
```

Lo anterior debe devolver que el mandato *java* está en **/usr/java/jre1.5.0_04/bin/java**.

Abra Mozilla, Epiphany o Galeon y en la barra de direcciones escriba **about:plugins**. Pulse la tecla ENTER. Deberá aparecer la información acerca de las extensiones instaladas para Mozilla, y entre éstas deberá aparecer la información correspondiente a la extensión (plug-in) Java™



Información sobre el Plug-in de Java™ en Mozilla

Por último, verifique en el menú de GNOME que aparezca la entrada de menú del Panel de Control de Java™ en ***Menú principal > Preferencias > Más preferencias***. Haga clic en ***Java*** y verifique que funcione.

Panel de Control de Java™ 2

Pruebe acceder hacia algún sitio que tenga un aplique Java™ para corroborar que la extensión para Mozilla ha quedado instalada correctamente. Encontrará varios enlaces hacia Juegos y otras aplicaciones en http://www.java.com/es/.

73. Cómo instalar la extensión (plug-in) Flash para Mozilla

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

73.1. Introducción

Los procedimientos descritos permitirán visualizar desde Mozilla, Mozilla Firebird, Epiphany o Galeon contenido Web en Macromedia™ Flash 5 (y versiones anteriores) y Macromedia™ Flash MX con extensiones *.swf y *.spl.

Los procedimientos de Instalación del sustento lógico necesario suponen que ya leyó **en su totalidad** y siguió los procedimientos del documento de Yum correspondiente.

73.2. Procedimientos

73.2.1. Instalación del sustento lógico necesario en CentOS, White Box y Red Hat™ Enterprise Linux 3

- Modifique **/etc/yum.conf** y añada el siguiente contenido:

```
[flash-plugin]
name=Macromedia Flash Player
baseurl=http://sluglug.ucsc.edu/macromedia/apt/redhat/3/
```

- `yum -y install flash-plugin`

- Si está instalando por primera vez aparecerá una ventana gráfica que solicitará leer la licencia y aceptar los términos de la misma.

73.2.2. Instalación del sustento lógico necesario en CentOS, White Box y Red Hat™ Enterprise Linux 4

- Genere el fichero **/etc/yum.repos.d/flash.repo** y añada el siguiente contenido:

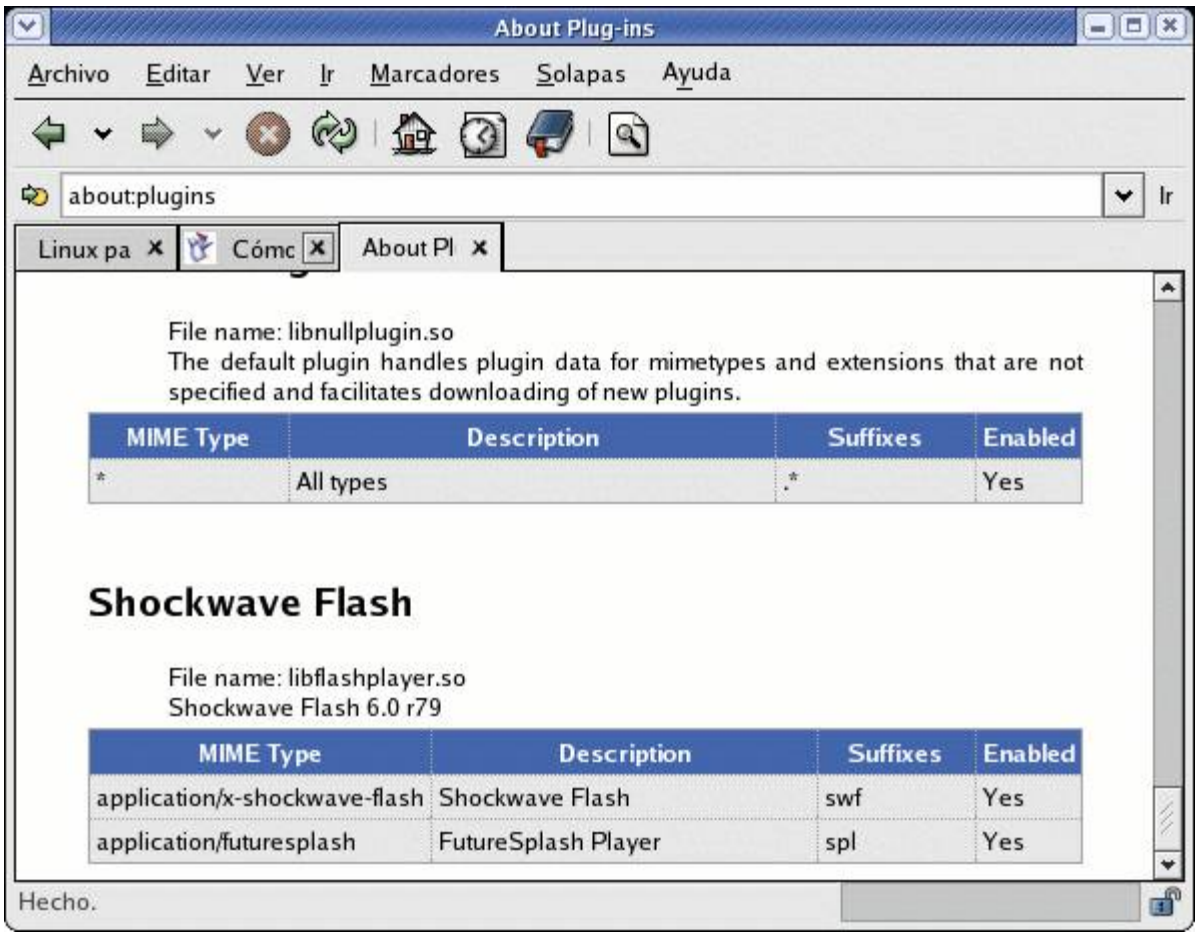
```
[flash-plugin]
name=Macromedia Flash Player
baseurl=http://sluglug.ucsc.edu/macromedia/apt/redhat/3/
```

- `yum -y install flash-plugin`

- Si está instalando por primera vez aparecerá una ventana gráfica que solicitará leer la licencia y aceptar los términos de la misma.

73.2.3. Comprobaciones

Abra Mozilla, Mozilla Firebird, Epiphany o Galeon y en la barra de direcciones y tecle **about:plugins**. Pulse enter. Deberá aparecer la información acerca de las extensiones instaladas para Mozilla; entre éstas deberá aparecer la información correspondiente a la extensión (plug-in) Macromedia™ Flash



Información sobre el Plug-in de Macromedia™ Flash en Mozilla.

74. Cómo configurar escáner en red

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

74.1. Introducción.

74.1.1. Acerca de SANE.

SANE (**S**canner **A**ccess **N**ow **E**asy) es un **API** (**A**pplication **P**rogramming **I**nterface o Interfaz de Programación de Aplicaciones) que proporciona un acceso estandarizado hacia cualquier dispositivo de captura de imágenes.

Difiere del **API TWAIN**, utilizado en Microsoft Windows y Mac OS, el cual gestiona simultáneamente las interfaz y las comunicaciones con el dispositivo. **SANE** está separado dos partes: programas de cliente y controladores de dispositivo. Un controlador **SANE** solo provee una interfaz con el sustento físico y describe un determinado número opciones que cada dispositivo puede utilizar. Las opciones, a su vez, especifican parámetros tales como la resolución para captura, tamaño del área a capturar, colores, brillantes, contraste, etc. Una de las ventajas de esta separación es que es relativamente fácil de implementar el servicio en red, sin consideraciones particulares tanto en los programas cliente como controladores de dispositivos.

URL: http://www.sane-project.org/

74.1.2. Acerca de Xsane.

Xsane es un programa cliente para **SANE**. Utiliza la biblioteca **SANE** para realizar la comunicación con los dispositivos escáner.

Xsane tiene las siguientes capacidades con las imágenes adquiridas a través de **SANE**:

- Mostrar la imagen capturada en un visor.
- Guardar una imagen como fichero.
- Hacer una fotocopia.
- Crear un documento de múltiples páginas.
- Crear un fax.
- Crear un mensaje de correo electrónico.

URL: http://www.xsane.org/

74.2. Equipamiento lógico necesario.

74.2.1. Instalación del servicio saned.

74.2.1.1. Instalación a través de yum.

Si utiliza **CentOS 4** o **White Box Enterprise Linux 4**, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install sane-backends sane-frontends xinetd
```

74.2.1.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date -i sane-backends sane-frontends xinetd
```

74.2.2. Instalación del cliente Xsane.

74.2.2.1. Instalación a través de yum.

Si utiliza **CentOS 4** o **White Box Enterprise Linux 4**, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y sane-backends sane-frontends xsane-gimp xsane sane-frontends
```

74.2.2.2. Instalación a través de up2date.

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date -i sane-backends sane-frontends xsane-gimp xsane sane-frontends
```

74.3. Procedimientos

74.3.1. Configuración del servicio saned.

Se debe verificar que en el fichero **/etc/sane.d/dll.conf** esté habilitada la línea correspondiente al controlador para escáner a través de red, es decir **net**.

```
# enable the next line if you want to allow access through the network:
net
```

Se añade en el fichero **/etc/sane.d/saned.conf** la lista de direcciones IP que tendrán permitido conectarse al servicio **saned** para escáner en red. En el siguiente ejemplo se permite el acceso a las direcciones IP 192.168.1.254, 192.168.1.253, 192.168.1.252, 192.168.1.251 y 192.168.1.250:

```
#
```

```
# saned.conf
#
# The contents of the saned.conf file is a list of host
# names or IP addresses that are permitted by saned to
# use local SANE devices in a networked configuration.
# The hostname matching is not case-sensitive.
#
#scan-client.somedomain.firm
#192.168.0.1
192.168.1.254
192.168.1.253
192.168.1.252
192.168.1.251
192.168.1.250
```

Con la finalidad de que las diversas aplicaciones y servicios puedan proporcionar una identificación para el servicio, se edita el fichero **/etc/services** y se añade la siguiente línea, donde **6566** corresponde al puerto correspondiente al servicio **saned**:

```
saned          6566/tcp      saned   # SANE network scanner daemon.
```

Debe crearse el fichero **/etc/xinetd.d/saned** con el siguiente contenido, a fin de que el acceso al servicio sea gestionado sobre demanda a través de el servicio **xinetd**:

```
service saned
            {
              socket_type = stream
              server = /usr/sbin/saned
              protocol = tcp
              user = root
              group = root
              wait = no
              disable = no
            }
```

Una vez hecho todo lo anterior, se especifica al activación del servicio **saned** con el mandato **chkconfig**, el cual a su vez notificará a el servicio **xinetd** que inicie automáticamente este al recibir cualquier petición en el puerto 6566 del sistema:

```
chkconfig saned on
```

Si todo ha ido bien, se puede comprobar el funcionamiento del servicio utilizando el mandato **telnet** dirigido hacia el puerto 6566 del retorno del sistema.

```
telnet localhost 6566
```

Lo anterior debe devolver algo como lo siguiente:

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
```

Para salir del intérprete del mandato **telnet**, solo se debe ingresar `quit` y pulsar la tecla ENTER.

74.3.2. Configuración del cliente Xsane.

Se debe especificar en el fichero **/etc/sane.d/net.conf** de los equipos cliente con **Xsane** la dirección IP del servidor recién configurado. En el siguiente ejemplo. se específica que el servicio **saned** está en el sistema con dirección IP 192.168.1.1:

```
# This is the net config file.  Each line names a host to attach to.
# If you list "localhost" then your backends can be accessed either
# directly or through the net backend.  Going through the net backend
# may be necessary to access devices that need special privileges.
192.168.1.1
```

Una vez hecho lo anterior, al utilizar **Xsane** en los clientes, estos deberán detectar automáticamente el escáner en el servidor 192.168.1.1. Es importante recordar que solo se puede acceder hacia el escáner con un solo cliente por vez.

75. Usando Smartd para anticipar los desastres de disco duro

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

75.1. Introducción

La mayoría de las distribuciones recientes incluyen **smartctl** y **smartd** (parte de **smartmontools** incluido en el paquete **kernel-utils**), que son herramientas utilizadas para supervisar la salud de los discos duros realizando pruebas para comprobar su buen funcionamiento. Mientras el disco y la tarjeta madre (soporte que se activa en el BIOS) tenga capacidad para utilizar S.M.A.R.T. (**S**elf-**M**onitoring, **A**nalysis and **R**eporting **T**echnology), es posible anticipar las fallas de un disco duro. Sólo basta configurar un fichero (**/etc/smartd.conf**) e iniciar un servicio (**smartd**).

75.2. Procedimientos

El fichero **/etc/smartd.conf** sólo requiere una línea de configuración por cada disco duro en el sistema. Ejemplos:

```
/dev/hda -a -m alguien@cuenta-de-correo.algo
/dev/sda -d scsi -a -m alguien@cuenta-de-correo.algo
/dev/sdb -d scsi -a -m alguien@cuenta-de-correo.algo
```

Lo anterior hace que se envié un reporte completo y detallado de toda la información S.M.A.R.T. y las alertas pendientes. La opción -a en discos IDE equivale a '-H -i -c -A -l error **-l selftest -l selective**', y en discos SCSI equivale a '**-H -i -A -l error -l selftest**', donde:

`-H`	Incluye en el reporte el estado de salud y alertas pendientes. Si se quiere enviar reportes a un teléfono móvil, ésta sería la opción única a utilizar.
`-i`	Incluye en el reporte el numero de modelo, número de serie, versión de Firmware e información adicional relacionada.
`-c`	Incluye en el reporte las capacidades S.M.A.R.T.
`-A`	Incluye en le reporte atributos S.M.A.R.T. específicos del fabricante del disco.
`-l error`	Incluye en el reporte la bitácora de errores de S.M.A.R.T.
`-l selftest`	Incluye en el reporte la bitácora de pruebas de S.M.A.R.T.
`-l selecti`	Algunos discos tipo ATA-7 (ejemplo: Maxtor) incluyen una bitácora de pruebas selectivas.

-H	Incluye en el reporte el estado de salud y alertas pendientes. Si se quiere enviar reportes a un teléfono móvil, ésta sería la opción única a utilizar.
ve	
-m	Cuenta de correo electrónico a la cual se enviarán reportes.

Si por ejemplo, sólo nos interesa recibir reportes de salud en un teléfono móvil, se utilizaría solamente lo siguiente:

```
/dev/hda -H -m alguien@cuenta-de-correo.algo
/dev/sda -d scsi -H -m alguien@cuenta-de-correo.algo
/dev/sdb -d scsi -H -m alguien@cuenta-de-correo.algo
```

Hecho lo anterior, sólo basta agregar el servicio a los servicios de arranque del sistema e iniciar (o reiniciar, según el caso) smartd:

```
chkconfig smartd
service smartd start
```

El servicio se encarga de ejecutar automáticamente en el trasfondo del sistema todas las pruebas necesarias y soportadas por las unidades de disco duro presentes. El reporte se envía automáticamente junto con el mensaje con el reporte de la bitácora del sistema unos minutos después de las 4:00 AM.

Si se quiere ver un reporte al momento, completo y detallado, suponiendo que se trata de un disco duro en el IDE 1, basta ejecutar:

```
smartctl -a /dev/hda
```

Si se quiere ver un reporte al momento y que sólo muestre el estado de salud de la unidad, suponiendo que se trata de un disco duro en el IDE 1, basta ejecutar:

```
smartctl -H /dev/hda
```

76. Glosario de mandatos básicos

Actualizado el Sábado 19/04/2003, 07:36:14 GMT -0600.

Pablo Marcelo Moia
gammexane@linuxparatodos.net
http://www.linuxparatodos.net/

76.1. Mandatos generales

Búsquedas	
`man mandato`	Muestra un manual sobre el mandato. Su modo de uso y sus variantes.
`shutdown -h 5`	Apaga el sistema en 5 minutos después de ejecutarse y no reinicia.
`shutdown -h now`	Apaga el sistema en ese momento y NO lo vuelve a reinicia
`halt`	Apaga el sistema de la misma manera que el mandato anterior.
`shutdown -r 5`	Apaga el sistema 5 minutos después de haberlo ejecutado y reinicia.
`shutdown -r now`	Apaga el sistema en ese momento y reinicia.
`reboot`	Reinicia el sistema.
`startx`	Inicia el entorno gráfico.
`adduser miusuario`	Agrega un usuario llamado miusuario.
`passwd miusuario`	Le asigna la clave de acceso al usuario miusuario.
`userdel miusuario`	Borra la cuenta miusuario.
`su`	Da momentáneamente privilegios de ROOT (Si sabemos la clave :))
`su - miusuario`	Se toma momentáneamente los privilegios del usuario miusuario.
`exit`	Sale del perfil del usuario que lo ejecuta.
`mount -t iso9660 /dev/cdrom /mnt/cdrom`	Monta la unidad de CD-ROM en el directorio especificado (/mnt/cdrom)
`mount -t msdos /dev/hda1 /mnt/win_c`	Monta el disco "C" en el directorio especificado con partición msdos.
`mount -t vfat /dev/hda1 /mnt/win_c`	Monta el disco "C" con partición FAT en el directorio especificado.
`umount /mnt/cdrom`	Desmonta el CD-ROM.
`umount /mnt/win_c`	Desmonta el disco rígido "C"
`usermount`	Una forma fácil y rápida de montar y desmontar unidades.

`Xconfigurator`	Sirve para cambiar la resolución, profundidad y placa de vídeo.
`xf86config`	Archivo de configuración de X.
`switchdesk`	Cambia el entorno gráfico por defecto (GNOME, KDE, etc.).

76.2. Tratamiento de archivos

`cd /home/miusuario`	Ingresa al directorio /home/miusuario.
`cd ..`	Vuelve al directorio raíz.
`ls -l`	Lista los archivos del directorio actual con todos sus atributos.
`ls -F`	Lista los archivos del directorio actual indicando su tipo (archivo, directorio, etc.).
`ls -lC`	Lista los archivos del directorio actual en columnas.
`ls -a`	Lista los archivos invisibles del directorio actual.(los que empiezan con "../../../../home/jbarrios/.").
`rm lpt.txt`	Borra el archivo con nombre lpt.txt.
`rm -R /miusuario`	Borra el directorio miusuario con todos los archivos que tiene dentro (Recursivo).
`rm -Rf /miusuario`	Borra el directorio miusuario en forma recursiva y SIN PREGUNTAR. -Atención con este mandato siendo Root-.
`cp lpt.txt /home/miusuario`	Copia el Archivo lpt.txt dentro del directorio /home/miusuario.
`mv lpt.txt /home/miusuario`	Mueve el Archivo lpt.txt dentro del directorio /home/miusuario.
`mv lpt.txt linux_para_todos.txt`	Le cambia el nombre al archivo lpt.txt por linux_para_todos.txt.
`*`	Representa todo. Ejemplo: ls *.rpm (lista todos los archivos con extensión rpm).
`?`	Representa un sólo carácter. Ejemplo: ls ?.txt (lista todos los archivos de un sólo carácter con extensión txt).

76.3. Manejo de paquetería

`rpm -ivh lpt-news-0.1-5.i386.rpm`	Instala el paquete lpt-news-0.1-5.i386.rpm (Use preferentemente -Uvh)
`rpm -Uvh lpt-news-0.1-5.i386.rpm`	Instala o actualiza el paquete lpt-news-0.1-5.i386.rpm¬ (usar éste, preferentemente, para instalar)
`rpm -e lpt-news`	Desinstala el paquete lpt-news (no se necesita ni la versión ni la extinción)
`rpm -qf /bin/ls`	Muestra en qué paquete está incluido el mandato ls. *-ver whereis, en sección búsqueda-*
`rpm -q lpt-news`	Muestra la versión del paquete ya instalado lpt-news.
`rpm -ql lpt-news`	Lista los componentes del paquete lpt-news, previamente instalado, con sus respectivas rutas.

`rpm -qa`	Lista todos los paquetes instalados en el sistema (no se necesitan privilegios de ROOT)
`rpm -qa |grep lpt`	Lista todos los paquetes que contengan lpt en su nombre.
`tar -zxvf lpt.tar.gz`	Descomprime y Desempaqueta el archivo lpt.tar.gz
`tar -zcvf lpt.tar.gz /home/miusuario`	Empaqueta y Comprime el directorio /home/miusuario dentro de lpt.tar.gz
`tar -jxvf lpt.tar.bz2`	Descomprime y Desempaqueta el archivo lpt.tar.bz2
`tar -jcvf lpt.tar.bz2 /home/miusuario`	Empaqueta y Comprime el directorio /home/miusuario dentro de lpt.tar.bz2
`tar -cMf /dev/fd0`	Empaqueta el directorio actual en múltiples Diskettes.

76.4. Sistema

`ps -axu |less`	Lista los procesos que se están corriendo.
`kill -9 123`	Mata el proceso con número de PID 123, sin darle tiempo a terminar
`kill -15 123`	Fuerza a terminar el proceso (el -15 no es necesario ya que es el número por defecto)
`kill -l`	Lista los posibles argumentos de el mandato, -15 (terminar), -9(matar) etc.
`top`	Cumple la función de ps y kill simultáneamente en consola.
`[Ctrl]+[Alt]+[Del]`	Shutdown. Apaga el sistema de forma organizada desde una terminal de texto.
`[Ctrl]+[Alt]+[F1]`	Cambia a la primera terminal de texto.
`[Ctrl]+[Alt]+[Fn]`	Cambia a la terminal de texto número n (n=1,...,8)
`[Ctrl]+[Alt]+[F7]`	Cambia a la primera terminal X (si se está usando alguna)
`[Ctrl]+[Alt]+[Fn]`	Cambia a la terminal X número n (n=7,...,12)
`[Tab]`	Auto-completa el nombre de un mandato, fichero, directorio, programa, cuando trabajamos en una terminal texto.
`[ArrowUp]`	(Flecha arriba) Va modificando la historia de mandatos que hemos escrito anteriormente en terminal texto.
`[Shift][PgUp]`	Scroll la salida de la terminal hacia arriba, en terminal texto.
`[Shift][PgDown]:`	Scroll la salida de la terminal hacia abajo, en terminal texto.
`[Ctrl]+c`	Termina el proceso actual. Si no está corriendo de fondo
`[Ctrl]+d`	Termina la terminal actual.
`[Ctrl]+s`	Para la transferencia a la terminal.
`[Ctrl]+z`	Manda el proceso actual a correr de fondo.
`hostname`	Devuelve el nombre de la máquina.
`uptime`	Devuelve la cantidad de tiempo transcurrido desde la

	última vez que se arrancó el sistema.
`uname -a`	Información sobre el sistema operativo de la máquina.
`dmesg|more`	Imprime el "ring buffer" del kernel.
`free -tm`	Información sobre la cantidad de memoria disponible y utilizada.
`df -h`	Información sobre todo los dispositivos montados en la máquina.
`du -bh /|more`	Información sobre el espacio ocupado por cada directorio subordinado, comenzando en el directorio raíz (/)
`cat /proc/cpuinfo`	Información sobre el microprocesador
`cat /proc/interrupts`	Información sobre las interrupciones en uso (IRQs)
`cat /proc/filesystems`	Información sobre los sistemas de archivos que se pueden utilizar (compilados en el kernel).
`who`	Información sobre los usuarios usando el sistema.
`id miusuario`	Información sobre UID, GID y GROUPS del usuario miusuario
`last`	Información sobre los últimos usuarios que han usado el sistema.
`/sbin/ifconfig`	Información sobre los distintos dispositivos de red
`netstat`	Información valiosa sobre la conexión de red
`find / -name lpt.txt -print`	Busca el archivo lpt.txt empezando por el directorio / y lo muestra en pantalla .
`find / -name lpt.txt > búsqueda.txt`	Busca el archivo lpt.txt empezando por el directorio / y guarda la salida en el archivo búsqueda.txt
`whereis fichero`	Busca los ficheros binarios, fuentes y páginas del manual correspondientes a un paquete

77. AL Desktop

Autor: *Joel Barrios Dueñas*
Correo electrónico: darkshram@gmail.com
sitio de Red: http://www.alcancelibre.org/
Jabber ID: *darkshram@jabber.org*

77.1. ¿Que es AL Desktop?

AL Desktop, continuación de LPT Desktop, es una colección de equipamiento lógico cuyo objetivo es enriquecer los sistemas operativos con aplicaciones y herramientas de vanguardia.

AL Desktop 1.0 la más reciente versión, está constituido por **más de 2300 paquetes** que incluyen, entre otras cosas, los más recientes lanzamientos de **GNOME 2.20**, Firefox 2.0, Evolution 2.12, Gimp 2.2, Gthumb 2.10, Xine-lib 1.1, Mplayer, Totem 2.20, GStreamer 0.10, Transcode, K3b 0.12.x, **Compiz Fusion 0.6.0**, **muchos juegos libres** para GNU/Linux y muchos otros paquetes más para la plataforma Enterprise Linux (CentOS, Red Hat™ Entrerprise Linux y White Box Entrerprise Linux), los cuales regularmente solo están disponibles para Fedora™ Core y otras distribuciones.

77.2. Sistemas operativos soportados por AL Desktop.

Alcance Libre ofrece soporte para las siguientes versiones de AL Desktop:

Versión	Sistemas operativos soportados	Arquitectura
1.0	Red Hat™ Enterprise Linux 4 CentOS 4 White Box Enterprise Linux 4	ix86
1.0	Red Hat™ Enterprise Linux 5 CentOS 5 White Box Enterprise Linux 5	ix86

77.3. ¿Cómo puedo instalarlo?

Se require instalar en el sistema una llave pública disponible en http://www.alcancelibre.org/al/AL-RPM-KEY.

```
wget http://www.alcancelibre.org/al/AL-RPM-KEY
rpm --import AL-RPM-KEY
```

Si no se han añadido las llaves públicas de la distribución utilizada, proceda a hacerlo ahora:

```
rpm --import /usr/share/rhn/*KEY*
```

Es indispensable estén configurados correctamente los depósitos yum predeterminados del sistema

específicos para la distribución utilizada. Para más detalles al respecto, consulte la documentación correspondiente para cada distribución en particular.

Se require además añadir la siguiente configuración a los depósitos yum del sistema.

77.3.1. AL Desktop 1.0

77.3.1.1. CentOS 4, Red Hat Enterprise Linux 4, Whitebox Enterprise Linux 4.

```
[AL-Desktop]
name=Enterprise Linux $releasever - $basearch - AL Desktop
mirrorlist=http://www.alcancelibre.org/al/el4/al-desktop
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

77.3.1.2. CentOS 5, Red Hat Enterprise Linux 5, Whitebox Enterprise Linux 5.

```
[AL-Desktop]
name=Enterprise Linux $releasever - $basearch - AL Desktop
mirrorlist=http://www.alcancelibre.org/al/el5/al-desktop
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

77.3.2. Procedimientos.

77.3.2.1. AL Desktop 1.0

- Respaldar los directorios ~/.gconf de las cuentas de usuario.
- **Cerrar** cualquier sesión de GNOME abierta. A fin de evitarnos sustos y molestias, GNOME no debe estar ejecutándose al momento de instalar el software.
- Cambiar a nivel de corrida 3 (GDM no debe estar ejecutándose)

  ```
  init 3
  ```
- Como root ejecutar:

  ```
  yum update
  ```
- Ser **muy** pacientes e irse a cenar o por un café. Algunos de los espejos están a su máxima capacidad.
- Regresar a nivel de corrida 5 y acceder como usuario.

77.4. Errores conocidos

77.4.1. AL Desktop 1.0

- Cuando se utiliza Firefox por primera vez en una nueva cuenta de usuario en un sistema recién instalado, se genera un directorio ~/.mozilla propiedad de Root, lo cual no deja iniciar Firefox. Este problema no es exclusivo de AL Desktop sino de versiones recientes de Firefox. La solución es eliminar el directorio ~/.mozilla y dejar que se genere un nuevo directorio automáticamente.
- **Java** (de Sun Microsystems) deja de funcionar tras actualizar AL Desktop debido a que no es compatible (por el momento) con la más reciente versión de libX11 (que utiliza libxcb, que es una ligadura de C para el protocolo X11). Para poder lograr que funcionen de nuevo **Java**, solo es necesario instalar la versión anterior de **libX11**, aunque eso impedirá poder utilizar algunos juegos 3D, **Compiz Fusion** y **Beryl**. Si es prioritario el uso de aplicaciones gráficas previamente compiladas con

Java (de Sun Microsystems), se debe utilizar **libX11-1.0.3-8.0.1.el5.i386.rpm**, en lugar del que instala AL Desktop. Solución al problema, si es indispensable utilizar Java, sería lo siguiente:

```
wget \
http://mirrors.kernel.org/centos/5/updates/i386/RPMS/libX11-1.0.3-8.0.1.el5.i386.rpm
rpm -Uvh --force libX11-1.0.3-8.0.1.el5.i386.rpm
echo "exclude=libX11*" >> /etc/yum.conf
```

CentOS 5 y **Red Hat Enterprise Linux 5** incluyen la máquina virtual Java de GNU.org, equivalente a Java 1.4.2, junto con el sistema, la cual permite ejecutar programas escritos en Java a través del paquete **java-1.4.2-gcj-compat-1.4.2.0-40jpp.112**, disponible a través de los depósitos de equipamiento lógico (software) de estas distribuciones. No incluye componente (plugin) para los navegadores.

77.5. ¿Cómo puedo cooperar con el proyecto?

- Donando espacio y ancho de banda para poner más servidores espejo. Los actuales están a toda su capacidad, y salvo por uno, el resto son enlaces ADSL con IP dinámica.
- Enviando reportes de errores.
- Ayudando a depurar errores.
- Donaciones a través de PayPal.

77.6. ¿Más preguntas?

¿Donde puedo consultar la lista de paquetes que include? En este enlace.

¿Qué tan estable es? Lo suficiente para el uso diario.

¿Por que no han incluido la más reciente versión de KDE? Porque implica mucho trabajo. Pero estamos abiertos a colaboración de cualquier tipo para la creación de los paquetes RPM correspondientes.

¿Cual es la motivación de este proyecto Hacer de plataformas como Red Hat™ Enterprise Linux, CentOS y White Box Enterprise Linux sistemas operativos más amistosos y divertidos para el usuario que quiere un sistema operativo estable y al mismo tiempo un escritorio bonito y con suficientes herramientas como para no extrañar ni envidiar mucho otros sistemas operativos como Fedora™ Core.

¿Qué paquetería no puede ser incluida en AL Desktop? Aquella que no sea equipamiento lógico (software) libre o que no permita su libre distribución en forma binaria.

¿Desde cuando se mantiene este proyecto? Fue iniciado como **LPT Desktop** a principios de 2002, e inicialmente consistía en mantener el conjunto de paquetes para Red Hat Linux 7.3.

78. Ejercicios

78.1. Ejercicio NFS

78.1.1. Introducción

Haga equipo con algún compañero de curso a fin de poder realizar el procedimiento, pruebas y depuración entre si.

78.1.2. Procedimientos

78.1.2.1. Servidor

1. Como root genere el directorio **/var/nfs/publico/** y asigne a éste un permiso 1777.

```
mkdir -p /var/nfs/publico
chmod 1777 /var/nfs/publico
```

2. Como root **modifique /etc/exports** y defina que se compartirá **/var/nfs/publico** a sistema del compañero con el cual está haciendo equipo en modo de lectura y escritura **con el siguiente contenido**:

```
/var/nfs/publico  192.168.0.n(rw,sync)
```

3. Como root **inicie o reinicie** el servicio de nfs.

```
service nfs restart
```

78.1.2.2. Cliente

1. Como root genere el directorio **/mnt/publico** a fin de que posteriormente sea utilizado para montar el volumen NFS de esta práctica.

2. Como root modifique **/etc/fstab** y especifique que se montará el volumen **/var/nfs/publico/** del sistema del compañero con el que está haciendo equipo en el directorio **/mnt/publico/**, utilizando las opciones de montado no automático (noauto), lectura y escritura (rw), montado con expiración (soft), continuar en trasfondo de ser necesario (bg), se pueda montar por el usuario (user) y permitir interrumpir procesos (intr).

```
192.168.0.n:/var/nfs/publico  /mnt/publico      nfs
noauto,rw,soft,bg,user,intr   0 0
```

3. Como usuario (fulano) intente montar el volumen NFS:

```
mount /mnt/publico
```

4. Como «fulano» cambie al directorio **/mnt/publico/** e intente crear un fichero con cualquier

contenido dentro del directorio **/mnt/publico/**.

```
cd /mnt/publico/
echo “Hola mundo" > holamundo.txt
ls
```

78.2. Ejercicio SAMBA

Usted deberá configurar a través de Samba un directorio sobre el cual se quiere permitir el ingreso sólo a dos usuarios, jefe y contador, quienes pertenecen al grupo de contabilidad. Dicho directorio deberá contar con permisos de escritura, de modo que tanto jefe como contador puedan trabajar en dicho directorio con una aplicación administrativa.

78.2.1. Procedimientos

1. Defina que dirección IP y mascara de subred tiene el servidor utilizando los siguientes mandatos:

   ```
   /sbin/ifconfig eth0 | grep inet | cut -d : -f 2 | cut -d \  -f 1
   /sbin/ifconfig eth0 | grep Mas | cut -d : -f 4
   ```

   El primer mandato donde aparece un \, debe haber **dos espacios** entre **** y **-f 1**, porque se está específicando *un espacio* como secuencia de escape. Utilizando **man cut** y **man grep**, explique que fue lo que realizaron los dos mandatos anteriores en el reporte escrito de este ejercicio.

2. Instale samba, samba-cliente y samba common del siguiente modo:

   ```
   yum -y install samba samba-client samba-common
   ```

3. Utilizando como referencia el documento titulado Cómo configurar SAMBA., edite el fichero **/etc/samba/smb.conf** y configure los siguientes parámetros de la sección **[global]** donde además deberá explicar en un **reporte por escrito** en papel qué es lo que hace cada uno de estos parámetros con los valores que serán asignados en el ejercicio:

   ```
   workgroup = cursolinux
   hosts allow = 192.168.0. 127.
   interfaces = lo, eth0, 127.0.0.1/32, 192.168.0.XXX/24
   remote announce = 192.168.0.255/cursolinux
   ```

   NOTA: 192.168.0.XXX se refiere a la dirección IP que posee el servidor y no literalmente 192.168.0.XXX.

   Salga del fichero.

4. Iniciar el servicio recién configurado.

   ```
   service smb start
   ```

5. Añadir el servicio **smb** al arranque del sistema.

   ```
   chkconfig smb on
   ```

6. Genere el directorio **/var/samba/contabilidad**:

   ```
   mkdir -p /var/samba/contabilidad
   ```

7. Genere el grupo de trabajo:

```
groupadd contabilidad
```

8. Genere los usuarios jefe y contador de modo que no tengan acceso al intérprete de mandatos y tengan como grupo primario a contabilidad. Asigne a éstos contraseña

```
useradd -s /sbin/nologin -g contabilidad jefe
useradd -s /sbin/nologin -g contabilidad contador
smbpasswd -a jefe
smbpasswd -a contador
```

9. Asigne los permisos necesarios a **/var/samba/contabilidad**, de modo tal, que se permita sólo la escritura, lectura y ejecución a dicho directorio al usuario y al grupo contabilidad, y de modo que se preserven los permisos del contenido de dicho directorio:

```
chmod 1770 /var/samba/contabilidad
chgrp contabilidad /var/samba/contabilidad
```

10. Modifique **/etc/samba/smb.conf** y configure lo necesario para compartir **/var/samba/contabilidad** en modo lectura-escritura con acceso solo para jefe y contador, redundando los permisos que se asignaron localmente a dicho directorio, y definiendo el permiso que deberá tener por defecto todo fichero o documento nuevo en el interior, a fin de que solamente puedan ser leídos y modificados por jefe y contador:

```
[contabilidad]
 comment = Contabilidad
 path = /var/samba/contabilidad
 writable = yes
 browseable = yes
 public = no
 printable = no
 valid users = jefe contador
 directory mode = 1770
 create mode = 0660
 veto files = /*.mp3/*.wma/*.avi/*wmv/*.mpg/*.mpeg/*.mov/
```

11. Reinicie el servicio de Samba:

```
service smb restart
```

12. Haga las pruebas pertinentes accediendo desde el administrador de archivos copiando, moviendo o eliminado objetos en el recurso que acaba de configurar.

```
smbclient -N -L 127.0.0.1
smbclient //127.0.0.1/contabilidad -U jefe%123qwe
```

13. Realice cualquier tipo de transferencia utilizando mget o mput desde el intérprete smb. Al terminar, utilice **exit** para salir.

78.3. Ejercicio Apache® y VSFTPD

Usted deberá simular ser un proveedor de servicio de hospedaje y configurar lo siguiente a través de apache y vsftpd:

- Una sitio de red virtual denominado «**su-máquina**.**dominio-a-definir**» asociado a la dirección IP 192.168.**10**.**n**.
- El dominio virtual debe poder ser administrado a través de una cuenta de usuario accediendo por medio de una conexión FTP.
- El usuario deberá estar enjaulado a través de FTP y tener acceso a las bitácoras generadas por el sitio de red virtual, pero sin permitir al usuario que pueda borrar accidentalmente el directorio que contiene a dichas bitácoras.

78.3.1. Procedimientos

1) Modifique **/etc/hosts** y proceda a resolver localmente la dirección IP y el nombre que tendrá el servidor en la red 192.168.10.0:

```
127.0.0.1       localhost.localdomain   localhost
192.168.0.n     su-máquina.nombre-de-dominio-resuelto    su-máquina
192.168.10.n    su-máquina.dominio-a-definir
```

2) Proceda a crear el fichero de configuración del dispositivo virtual en **/etc/sysconfig/network-scripts/ifcfg-eth0:1** con el siguiente contenido:

```
DEVICE=eth0:1
IPADDR=192.168.10.n
NETMASK=255.255.255.0
```

3) Reinicie el servicio de red del sistema y compruebe que haya levantado la interfaz virtual **eth0:1** que acaba de configurar:

```
service network restart
ifconfig eth0:1
```

4) Genere el árbol de directorios necesario:

```
mkdir /var/www/net
mkdir /var/www/net/html
mkdir /var/www/net/log
mkdir /var/www/net/etc
```

5) Genera la cuenta de usuario que será utilizada para administrar el sitio de red virtual:

```
useradd -s /sbin/nologin -d /var/www/net adminnet
passwd adminnet
saslpasswd adminnet
saslpasswd2 adminnet
```

6) Configure los permisos apropiados a **/var/www/net** y su contenido:

```
chmod 1755 /var/www/net
chmod 1755 /var/www/net/html
chown root:apache /var/www/net
chown adminnet:apache /var/www/net/html
chown adminnet:apache /var/www/net/etc
chown root:root /var/www/net/log
```

7) Configure apache para poder acceder hacia este sitio de red virtual haciendo uso del fichero localizado en la ruta **/etc/httpd/conf.d/virtuales.conf** con el siguiente contenido:

```
NameVirtualHost 192.168.10.n
      <VirtualHost 192.168.10.n>
            DocumentRoot /var/www/net/html
            ServerName su-maquina.dominio-a-definir
            ServerAdmin webmaster@su-maquina.dominio-a-definir
            ErrorLog /var/www/net/log/error_log
            CustomLog /var/www/net/log/access_log combined
      </VirtualHost>
```

8) Este sitio virtual generará su propia bitácora. Por tal motivo, es importante configurar el sistema para que realice la rotación de bitácoras correspondiente. Genere o bien verifique que exista el fichero de configuración correspondiente, en la ruta **/etc/logrotate.d/virtuales** con el siguiente contenido, donde las comillas se establecerán utilizando **acentos graves**:

```
/var/www/*/log/*log {
      missingok
      notifempty
      sharedscripts
      postrotate
      /bin/kill -HUP `cat /var/run/httpd.pid 2>/dev/null` 2> /dev/null
|| true
      endscript
}
```

9) Reinicie apache y haga comprobaciones y diagnóstico si fuese necesario.

```
service httpd restart
```

78.3.2. Comprobaciones

Reinicialice Apache® y pruebe publicar un documento HTML utilizando cualquier herramienta para publicación de red, como puede ser Mozilla Composer, Frontpage o cualquier editor HTML y publicando a través de FTP, haciendo uso de la cuenta FTP de **adminnet**. Visualice desde el navegador que prefiera el sitio de red virtual que se configuró.

Si desea hacer todo desde modo terminal, utilice el siguiente procedimiento.

1. Acceda al sistema como usuario local (**fulano**).

2. Genere un documento HTML denominado **index.html** utilizando el editor de texto que prefiera con el siguiente contenido:

```
<html>
<head>
<title>Bienvenido a su-máquina.dominio-a-definir</title>
</head>
<body>
<h1>Bienvenido a su-máquina.dominio-a-definir</h1>
<p>&iexcl;Hola mundo!</p>
</body>
</html>
```

3. Publique como el usuario adminnet el documento anterior utilizando ftp:

```
ftp su-máquina.dominio-a-definir
Connected to amdk6 (192.168.1.1).
220 Bienvenido al servidor FTP de Alcance Libre.
Name (su-máquina.dominio-a-definir:fulano):adminnet
331 Please specify the password.
Password:
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>cd html
ftp>put index.html
ftp>bye
```

4. Finalmente visualice la página **su-máquina.dominio-a-definir** principal utilizando elinks.

```
elinks http://su-máquina.dominio-a-definir/
```

78.4. Ejercicio: Cuotas de disco, Apache, VSFTPD y DNS

Usted deberá simular ser un proveedor de servicio de hospedaje y configurar lo siguiente a través de apache, bind y vsftpd:

- Deberá configurar la zona de reenvío para el DNS que se hará cargo de resolver los sub-dominios www, ns1, mail, ftp y **su-máquina** del dominio «que se le especifique».
- Un sitio de red virtual denominado «**su-máquina**.**dominio-a-definir**» con alias «**dominio-a-definir**» asociado a la dirección IP 192.168.**20**.***n***.
- El dominio virtual debe poder ser administrado a través de una cuenta de usuario accediendo por medio de una conexión FTP.
- El usuario deberá estar enjaulado a través de FTP y tener acceso a las bitácoras generadas por el sitio de red virtual, pero sin permitir que el usuario pueda borrar accidentalmente el directorio que contiene a dichas bitácoras.
- El usuario deberá tener asignada una cuota de disco de 300 MB.

78.4.1. Procedimientos

1) Añada en **/etc/hosts** la resolución local del nombre de dominio del sitio de red virtual asociado a la dirección IP definida para el mismo:

```
127.0.0.1   localhost.localdomain              localhost
192.168.0.n su-máquina.nombre-de-dominio-resuelto    su-máquina
192.168.10.n      su-máquina.dominio-ejercicio-anterior
192.168.20.n      su-máquina.dominio-a-definir  www.dominio-a-definir
dominio-a-definir
```

2) Proceda a crear el fichero de configuración localizado en la ruta **/etc/sysconfig/network-scripts/ifcfg-eth0:2** para el dispositivo **eth0:2** utilizando el siguiente contenido:

```
DEVICE=eth0:2
IPADDR=192.168.20.n
NETMASK=255.255.255.0
```

3) Reinicie el servicio de red del sistema y compruebe que haya levantado la interfaz virtual **eth0:2** que acaba de configurar:

```
service network restart
ifconfig eth0:2
```

4) Dentro del directorio **/var/named/chroot/var/named**, genere el fichero **dominio-a-definir**.zone, que servirá para resolver la zona de reenvío para el dominio «**dominio-a-definir**» con los sub-dominios www, ns1, mail, ftp y **su-máquina**:

```
$TTL 86400
@                IN    SOA   su-máquina.nombre-de-dominio-resuelto.
      fulano.su-máquina.nombre-de-dominio-resuelto. (
                       2004040801 ; número de serie
                       28800 ; tiempo refresco
                       7200 ; tiempo reintentos
                       604800 ; expiración
                       86400 ; tiempo total de vida
                       )
@                IN    NS    su-máquina.nombre-de-dominio-resuelto.
@                IN    NS    ns1
@                IN    MX    10    mail
@                IN    A     192.168.20.n
su-máquina       IN    A     192.168.20.n
www              IN    A     192.168.20.n
mail             IN    A     192.168.20.n
ns1              IN    A     192.168.20.n
ftp              IN    A     192.168.20.n
```

5) Modifique **/var/named/chroot/etc/named.conf** y añada la zona correspondiente:

```
zone “dominio-a-definir" {
      type master;
      file “dominio-a-definir.zone";
      allow-update { none; };
};
```

6) Cambie la pertenencia del fichero de zona al usuario «named» ejecutando lo siguiente:

```
chown named.named /var/named/chroot/var/named/dominio-a-definir.zone
```

7) Reinicie el servicio de servidor de nombres:

```
service named restart
```

8) Realice prueba de depuración y verifique que la zona haya cargado con número de serie:

```
tail -80 /var/log/messages |grep named
```

9) Compruebe que el dominio resuelve correctamente:

```
host dominio-a-definir 192.168.20.n
dig @192.168.20.n dominio-a-definir
dig @192.168.20.n dominio-a-definir mx
```

10) Si el dominio resuelve correctamente, **proceda a colocar como DNS primario** a su propio servidor en el fichero **/etc/resolv.conf**, simplemente definiendo éste como el primer registro **nameserver** de este fichero, justo debajo de los registros **search**:

```
; Parte superior del fichero /etc/resolv.conf
search nombre-de-dominio-resuelto
search dominio-a-definir
nameserver 192.168.0.n
nameserver 192.168.1.1
```

11) Genere el árbol de directorios necesario para el sitio de red virtual a través de Apache utilizando los siguientes **mandatos**:

```
mkdir -m 1755 /var/www/dominio-a-definir
mkdir -m 3755 /var/www/dominio-a-definir/html
mkdir /var/www/dominio-a-definir/{log,etc,mail}
```

12) Genere la cuenta de usuario que será utilizada para administrar el sitio de red virtual:

```
useradd -s /sbin/nologin -d /var/www/dominio-a-definir admindominio
passwd admindominio
saslpasswd admindominio
saslpasswd2 admindominio
```

13) Configure los permisos apropiados a **/var/www/dominio-a-definir** y los directorios en su interior utilizando **lo siguientes mandatos**:

```
chown root:apache /var/www/dominio-a-definir
chown admindominio:apache /var/www/dominio-a-definir/html
chown admindominio:apache /var/www/dominio-a-definir/etc
chown admindominio:admindominio /var/www/dominio-a-definir/etc
chown root:root /var/www/dominio-a-definir/log
```

14) Configure Apache para poder acceder hacia este sitio de red virtual haciendo uso del fichero localizado en la ruta **/etc/httpd/conf.d/virtuales.conf** con el siguiente contenido:

```
NameVirtualHost 192.168.20.n
<VirtualHost 192.168.20.n>
      DocumentRoot /var/www/dominio-a-definir/html
      ServerName su-máquina.dominio-a-definir
      ServerAlias dominio-a-definir www.dominio-a-definir
      ServerAdmin webmaster@dominio-a-definir
      ErrorLog /var/www/dominio-a-definir/log/error_log
      CustomLog /var/www/dominio-a-definir/log/access_log combined
</VirtualHost>
```

15) Este sitio virtual generará su propia bitácora. Por tal motivo es importante configurar el sistema para que realice la rotación de bitácoras correspondiente. Genere o bien verifique que exista el fichero de configuración correspondiente en la ruta **/etc/logrotate.d/virtuales** con el siguiente contenido, donde las comillas se establecerán utilizando **acentos graves**:

```
/var/www/*/log/*log {
      missingok
      notifempty
      sharedscripts
      postrotate
      /bin/kill -HUP `cat /var/run/httpd.pid 2>/dev/null` 2> /dev/null
|| true
      endscript
}
```

16) Reinicie el servicio de httpd (apache) y haga las comprobaciones, la depuración y el diagnóstico si fuese así necesario.

```
service httpd restart
```

17) Configure los dominios virtuales para que Sendmail pueda recibir correo para los mismos añadiendo **dominio-a-definir** y mail.**dominio-a-definir** en el interior del fichero **/etc/mail/local-host-names** con el siguiente contenido:

```
domino-a-definir
mail.domino-a-definir
```

18) Configure el dominio virtual **dominio-a-definir** a fin de que Sendmail permita enviar correo para el mismo en el fichero **/etc/mail/relay-domain**s con el siguiente contenido:

```
dominio-a-definir
```

19) Genere los nuevos ficheros necesarios para los dominios virtuales en Sendmail, si es que aún existen:

```
touch /etc/mail/{virtusertable,genericstable,generics-domain}
```

20)Si no ha hecho aún, habilitar la re-escritura de las cuentas de correo, añada en el fichero **/etc/mail/sendmail.mc,** debajo de **FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable.db')dnl** las siguientes dos líneas de configuración:

```
FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable.db')dnl
FEATURE(`genericstable',`hash -o /etc/mail/genericstable.db')dnl
GENERICS_DOMAIN_FILE(`/etc/mail/generics-domains')dnl
```

21)Añada en el fichero **/etc/mail/sendmail.mc** los dominios virtuales:

```
Cwdominio-a-definir
Cwmail.dominio-a-definir
```

22) Genere la cuenta de correo virtual denominada webmaster@**dominio-a-definir** como alias de la cuenta local admindominio, modificando el fichero **/etc/mail/virtusertable** del siguiente modo:

```
webmaster@dominio-a-definir    admindominio
```

23) Al terminar, y a fin de que el usuario virtual sea reconocido por el servicio de Sendmail, se deberá convertir el fichero **/etc/mail/virtusertable** en **/etc/mail/virtusertable.db ejecutando** lo siguiente:

```
makemap hash /etc/mail/virtusertable.db < /etc/mail/virtusertable
```

24)A fin de reescribir como webmaster@**dominio-a-definir** al correo emitido desde la cuenta local **admindominio**, modificando el fichero **/etc/mail/genericstable** del siguiente modo:

```
admindominio    webmaster@dominio-a-definir
```

25) Al terminar, y a fin de que el correo del usuario real se reescriba como la cuenta de correo del usuario virtual, se deberá convertir el fichero **/etc/mail/genericstable** en **/etc/mail/genericstable.db ejecutando** lo siguiente:

```
makemap hash /etc/mail/genericstable.db < /etc/mail/genericstable
```

26) Añada en el fichero **/etc/mail/generics-domains** el nuevo dominio virtual:

```
  dominio-a-definir
```

27)Reinicie el servidor de Sendmail:

```
service sendmail restart
```

28) Ejecutando «**edquota admindominio**», asigne una cuota de 300 MB (307200 kb) al usuario **admindominio**:

```
Disk quotas for user admindominio (uid 508):
  Filesystem   blocks     soft     hard   inodes    soft    hard
  /dev/hda6         0        0        0        0       0       0
  /dev/hda3        24        0   307200       10       0       0
```

78.4.2. Comprobaciones

Reinicialice Apache® y pruebe publicar un documento HTML utilizando cualquier herramienta para publicación de red, como puede ser Mozilla Composer, Frontpage o cualquier editor HTML y publicando a través de FTP, haciendo uso de la cuenta FTP de **admindominio** en el URL **ftp://dominio-a-definir/html/**

Visualice desde el navegador el sitio de red virtual que se configuró.

Pruebe enviar correo a la cuenta virtual **webmaster@dominio-a-definir** y leer dicho correo a través de POP3 o IMAP desde la cuenta de **admindominio**.

Si desea hacer todo desde modo terminal, utilice el siguiente procedimiento.

1. Acceda al sistema como usuario local (**fulano**).

2. Genere un documento HTML denominado **index.html** utilizando el editor de texto que prefiera

con el siguiente contenido:

```
<html>
<head>
<title>Bienvenido a www.dominio-a-definir</title>
</head>
<body>
<h1>Bienvenido a www.dominio-a-definir</h1>
<p>&iexcl;Hola mundo!</p>
</body>
</html>
```

3. Publique como el usuario ***admindominio*** el documento anterior utilizando ftp:

```
ftp ftp.dominio-a-definir
Connected to amdk6 (192.168.1.1).
220 Bienvenido al servidor FTP de Alcance Libre.
Name (ftp.dominio-a-definir:fulano):admindominio
331 Please specify the password.
Password:
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>cd html
ftp>put index.html
ftp>bye
```

4. Finalmente, visualice la página **su-máquina.dominio-a-definir** principal de utilizando el navegador elinks.

```
elinks http://su-máquina.dominio-a-definir/
```

5. Utilice **mutt** y envíe un mensaje al usuario **webmaster@dominio-a-definir**.

```
echo “Mensaje de prueba" | mutt -s “Mensaje de prueba"
webmaster@dominio-a-definir
```

6. Verifique la cuenta de correo de **admindominio** a través de **cualquier** cliente de correo electrónico o bien el correo con interfaz HTTP.

```
elinks http://su-máquina.dominio-a-definir/webmail/
```

78.5. Ejercicio: Servidor Intermediario (Proxy)

78.5.1. Introducción.

Utilizando como referencia los siguientes documentos, elabore un reporte por escrito de cada uno de los mandatos y parámetros utilizados en este ejercicio.

- Cómo configurar Squid: Parámetros básicos para servidor de intermediación (Proxy).
- Cómo configurar Squid: Acceso por Autenticación.
- Cómo configurar Squid: Restricción de acceso a Sitios de Red.
- Cómo configurar Squid: Restricción de acceso a contenido por extensión.
- Cómo configurar Squid: Restricción de acceso por horarios.
- Cómo configurar Squid: Como configurar el administrador de cache.

Procedimientos

1. Proceda a instalar squid y el navegador lynx:

   ```
   sudo yum -y install squid lynx
   ```

2. Cambie al directorio /etc/squid

   ```
   cd /etc/squid
   ```

3. Genere el subdirectorio listas:

   ```
   sudo mkdir listas/
   ```

4. Genere los ficheros que se utilizarán para las listas de control de acceso y claves de acceso:

   ```
   sudo touch
   listas/{libres,redlocal,porno,extensiones,claves,inocentes}
   ```

5. Listar las propiedades del fichero que será utilizado para almacenar las claves de acceso:

   ```
   ls -l listas/claves
   ```

6. Cambiar atributos de lectura y escritura solo para el usuario propietario:

   ```
   sudo chmod 600 listas/claves
   ```

7. Cambiar el propietario del fichero de claves de acceso hacia el usuario **squid**:

   ```
   sudo chown squid.squid listas/claves
   ```

8. Listar **de nuevo** las propiedades del fichero que será utilizado para almacenar las claves de acceso, y observar cambios:

```
ls -l listas/claves
```

9. Ejecutar lo siguiente y asignar claves de acceso a los usuarios virtuales (para este ejercicio, asignar a todos **qwerty** como clave de acceso)

```
for usuario in juanito pepito pedrito paquito
do
sudo htpasswd listas/claves $usuario
done
```

10. Editar el fichero listas/libres:

```
sudo vim listas/libres
```

Poner como contenido la IP de mi máquina.

Opcionalmente, también se puede hacer realizar lo siguiente para determinar su dirección IP:

```
/sbin/ifconfig eth0
| grep inet | cut -d : -f 2 | cut -d  -f 1 > /tmp/libres
mv /tmp/libres /etc/squid/listas/libres
```

11. Editar el fichero listas/redlocal:

```
sudo vim listas/redlocal
```

Poner como contenido las IP del resto de la LAN. Un renglón por IP.

12. Editar el fichero listas/porno:

```
sudo vim listas/porno
```

Poner como contenido lo siguiente:

```
www.sitioporno.com
www.otrositioporno.com
sitioindeseable.com
otrositioindeseable.com
napster
sex
porn
mp3
xxx
adult
warez
celebri
youtube
```

13. Editar el fichero listas/extensiones:

```
sudo vim listas/extensiones
```

14. Poner como contenido:

```
.avi$
.mp4$
.mp3$
.mp4$
.mpg$
.mpeg$
.mov$
.ra$
.ram$
.rm$
.rpm$
.vob$
.wma$
.wmv$
.wav$
.doc$
.xls$
.mbd$
.ppt$
.pps$
.ace$
.bat$
.exe$
.lnk$
.pif$
.scr$
.sys$
.zip$
.rar$
```

15. Editar el fichero listas/inocentes:

```
sudo vim listas/inocentes
```

Poner como contenido:

```
.alcancelibre.org
.google.com.mx
.eluniversal.com.mx
.milenio.com.mx
.diariolarazon.com.mx
.reforma.com.mx
.cnn.com
```

16. Editar el fichero squid.conf:

```
sudo vim squid.conf
```

17. Desde vim, ejecutar la siguiente búsqueda:

```
/http_port 3128
```

Reemplazar por:

```
http_port 192.168.0.XXX:8080 transparent
```

Donde **192.168.0.XXX** corresponde a la dirección IP de su servidor.

18. Desde vim, realizar la siguiente búsqueda:

```
/100 16 256
```

Reemplazar:

```
# cache_dir ufs /var/spool/squid 100 16 256
```

Por:

```
cache_dir ufs /var/spool/squid 512 16 256
```

19. Desde vim, realizar la siguiente búsqueda:

```
/#auth_param basic program <uncomment and complete this line>
```

Reemplazar:

```
#auth_param basic program <uncomment and complete this line>
```

Por:

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/listas/claves
```

20. Desde vim, realizar la siguiente búsqueda:

```
/#acl password proxy_auth REQUIRED
```

Descomentar la línea, quitando el símbolo #

21. Desde vi, realizar la siguiente búsqueda:

```
/acl to_localhost dst 127.0.0.0
```

Debajo de ésta línea, agregar:

```
acl redlocal src "/etc/squid/listas/redlocal"
acl libres src "/etc/squid/listas/libres"
```

```
acl porno url_regex "/etc/squid/listas/porno"
acl extensiones urlpath_regex "/etc/squid/listas/extensiones"
acl inocentes dstdomain "/etc/squid/listas/inocentes"
acl matutino time MTWHF 08:00-19:00
```

22. Desde vim, realizar la siguiente búsqueda:

```
/http_access deny all
```

Arriba de dicha línea, agregar:

```
http_access allow matutino redlocal password !porno !extensiones
http_access allow inocentes redlocal password
http_access allow libres
```

23. Desde vim, realizar la siguiente búsqueda:

```
/# error_directory
```

Reemplazar lo siguiente:

```
# error_directory /usr/share/squid/errors/English
```

Por:

```
error_directory /usr/share/squid/errors/Spanish
```

24. Reinicie o, en su defecto, inicie la configuración de Squid a fin de verificar si hubo errores fatales:

```
sudo service squid restart
```

Si hay errores, corregirlos. Sino devuelve depuración, examinar **/var/log/squid/squid.out** y realizar correcciones:

```
sudo tail -f /var/log/squid/squid.out
```

25. Recargar la configuración de Squid a fin de verificar si hubo errores no fatales:

```
sudo service squid reload
```

Si hay errores, realizar correcciones pertinentes.

26. Realizar comprobaciones utilizando navegador en modo texto:

Defina el propio servidor como el valor para la variable de ambiente http_proxy:

```
export http_proxy="http://192.168.0.XXX:8080/"
```

Donde **192.168.0.XXX** corresponde a la dirección IP de su servidor.

27. Realice una prueba de búsqueda a través de Google México para la palabra **sex**:

```
lynx "http://www.google.com.mx/search?q=sexo"
```

Deberá permitir realizar la búsqueda e ingresar hacia sitios cuyo URL contenga la cadena de caracteres **sex**.

Defina otro servidor donde la IP del sistema donde está trabajando esté en la lista de **redlocal** como el valor para la variable de ambiente http_proxy:

```
export http_proxy="http:// IP de la PC de al lado:8080/"
```

Realice una prueba de búsqueda a través de Google México para la palabra **sex**:

```
lynx -accept_all_cookies "http://www.google.com.mx/search?q=sexo"
```

Deberá permitir realizar la búsqueda pero denegar el ingreso hacia sitios cuyo URL contenga la cadena de caracteres **sex**.

78.6. Ejercicio de configuración del sistema para Linux, Apache, PHP y MySQL

Este ejercicio le mostrará como configurar el sistema para hacer uso de **L**inux, **A**pache, **P**HP y **M**ySQL, lo que se conoce como L.A.M.P., y mostrará también algunas funciones básicas de PHP. Este ejercicio se realiza **como cortesía** a fin de preparar los sistemas para poder ser utilizados por quienes tomarán el curso de PHP y MySQL.

1. Si acaso existiera, por favor elimine la configuración en Apache® hecha durante las prácticas anteriores:

```
rm -f /etc/httpd/conf.d/virtuales.conf
rm -f /etc/httpd/conf.d/misvariables.conf
```

2. A fin de limpiar el sistema de las configuraciones derivadas de este curso, elimine los servicios que no serán necesarios ejecutando lo siguiente:

```
yum -y remove bind caching-nameserver nfs-utils samba
yum -y remove vsftpd squirrelmail squid firestarter iptables
```

3. Instale o verifique que esté instalado todo lo necesario ejecutando lo siguiente:

```
yum -y install httpd php php-mysql bluefish mysql mysql-server
```

4. Añada los servicios de Apache® y MySQL al inicio del sistema:

```
chkconfig httpd on
chkconfig mysqld on
```

5. Proceda a crear el directorio de trabajo **/var/www/cursolamp** y el árbol de trabajo correspondiente, sobre el cual podrá realizar pruebas de configuración de servicios sin necesidad de tocar ficheros de configuración central ejecutando lo siguiente:

```
  mkdir -p /var/www/cursolamp/
  mkdir -p /var/www/cursolamp/html/
  mkdir -p /var/www/cursolamp/cgi-bin/
  mkdir -p /var/www/cursolamp/etc/
  mkdir -p /var/www/log-cursolamp/
  ln -s /var/www/log-cursolamp /var/www/cursolamp/log
```

6. Proceda a crear un usuario específico para trabajar con el directorio de trabajo /var/www/cursolamp/. Dicho usuario deberá darlo de alta con acceso al intérprete de mandatos (Shell) a fin de poder permitir acceso por SSH, asignando como **clave de acceso** la palabra «**qwerty**». Ejecute lo siguiente:

```
  useradd -s /bin/bash -m -d /var/www/cursolamp cursolamp
  passwd cursolamp
```

7. Asigne los permisos necesarios al directorio de trabajo y directorios subordinados en el interior, ejecutando lo siguiente:

```
chown cursolamp.apache /var/www/cursolamp
chmod 1755 /var/www/cursolamp
chown cursolamp.apache /var/www/cursolamp/html/
chown cursolamp.apache /var/www/cursolamp/cgi-bin/
chown cursolamp.apache /var/www/cursolamp/etc/
chown root.root /var/www/log-cursolamp/
ln -s /var/www/cursolamp/html /var/www/cursolamp/Desktop/html
```

8. Configure apache para que utilice el dominio **su-máquina**.**dominio-red-local** asociado al de la dirección IP 192.168.0.**n** en el fichero de configuración **/etc/httpd/conf.d/cursolamp.conf** utilizando el siguiente contenido:

```
NameVirtualHost *:80
      <VirtualHost *:80>
            ServerName su-máquina.dominio-red-local
            ServerAlias su-máquina
            DocumentRoot /var/www/cursolamp/html/
            ServerAdmin cursolamp@su-máquina.dominio-red-local
            ErrorLog /var/www/log-cursolamp/error_log
            CustomLog /var/www/log-cursolamp/access_log combined

# Permitir ver contenido de directorio y activar uso de ficheros
.htaccess
            <Directory /var/www/cursolamp/html/>
                  Options Indexes Includes FollowSymLinks
                  AllowOverride All
                  Order allow,deny
                  Allow from all
            </Directory>

# Configurar directorio cgi-bin independiente al del sistema.
            ScriptAlias /cgi-bin/ "/var/www/cursolamp/cgi-bin/"
            <Directory "/var/www/cursolamp/cgi-bin">
                  Options Includes
                  AllowOverride None
                  Order allow,deny
                  Allow from all
            </Directory>

      </VirtualHost>
```

9. Reinicie o inicie el servicio de Apache® ejecutando lo siguiente:

```
service httpd restart
```

10. Cierre la sesión de root e **ingrese** como el usuario **cursolamp**.

11. Como el usuario **cursolamp**, cambie al directorio ~/html/

```
cd ~/html/
```

12. Utilizando cualquier editor de texto (vi o bluefish, por ejemplo), genere el fichero ~/html/cabecera.php utilizando el siguiente contenido:

```
<html lang="es">
<head>
```

13. Utilizando cualquier editor de texto (vi o bluefish, por ejemplo), genere el fichero ~/html/cuerpo.php utilizando el siguiente contenido:

```
</head>
<body style="background-color: red; color: #FFFF00; font-weight:
bolder; ">
```

14. Utilizando cualquier editor de texto (vi o bluefish, por ejemplo), genere el fichero ~/html/pie.php utilizando el siguiente contenido:

```
</body>
</html>
```

15. Utilizando cualquier editor de texto (vi o bluefish, por ejemplo), genere el fichero ~/html/ejemplo-includes.php utilizando el siguiente contenido:

```
<?php function titulo() { echo "P&aacute;gina de prueba PHP"; } ?>
<?php include "cabecera.php"; ?>
<title><?php titulo() ?></title>
<?php include "cuerpo.php"; ?>
<h1><?php titulo() ?></h1>
<p>Documento de ejemplo de funciones b&aacute;sicas de PHP.</p>
<p>Hoy es <?php echo date("l dS of F Y h:i:s A");?></p>
<?php include "pie.php"; ?>
```

16. Utilice cualquier navegador, ya sea en modo texto o bien en modo gráfico y visualice el documento localizado en el url http://**su-máquina.dominio-redlocal**/ejemplo-includes.php.

```
  elinks  http://su-máquina.dominio-redlocal/ejemplo-includes.php
```

78.7. Configuración del sistema como estación de trabajo

1. Edite el fichero /etc/inittab y localice la siguiente línea:

   ```
   id:3:initdefault:
   ```

2. Lo anterior establece que el sistema inicia en nivel de corrida 3; es decir, en modo multiusuario completo, sin modo gráfico activo. A fin de que el sistema inicie en modo gráfico, cambie la línea anterior por esta otra:

   ```
   id:5:initdefault:
   ```

3. Localice más adelante en este mismo fichero lo siguiente:

   ```
   # Run gettys in standard runlevels
   1:2345:respawn:/sbin/mingetty tty1
   2:2345:respawn:/sbin/mingetty tty2
   3:2345:respawn:/sbin/mingetty tty3
   4:2345:respawn:/sbin/mingetty tty4
   5:2345:respawn:/sbin/mingetty tty5
   6:2345:respawn:/sbin/mingetty tty6
   ```

4. Lo anterior especifica que las seis terminales de texto estarán habilitadas en los niveles de corrida 2, 3, 4 y 5. Se deshabilitarán las seis terminales solamente en el nivel de corrida 5. Edite lo anterior de modo que quede del siguiente modo:

   ```
   # Run gettys in standard runlevels
   1:234:respawn:/sbin/mingetty tty1
   2:234:respawn:/sbin/mingetty tty2
   3:234:respawn:/sbin/mingetty tty3
   4:234:respawn:/sbin/mingetty tty4
   5:234:respawn:/sbin/mingetty tty5
   6:234:respawn:/sbin/mingetty tty6
   ```

5. Edite el fichero /etc/rc.local y añada la instrucción /usr/bin/clear, de modo que la pantalla sea limpiada una vez que haya concluido el arranque.

   ```
   #!/bin/sh
   #
   # This script will be executed *after* all the other init scripts.
   # You can put your own initialization stuff in here if you don't
   # want to do the full Sys V style init stuff.

   touch /var/lock/subsys/local
   /usr/bin/clear
   ```

6. Modifique /etc/grub.conf y localice la línea del núcleo:

   ```
   title White Box Enterprise Linux (2.4.21-20.EL)
           root (hd0,0)
           kernel /vmlinuz-2.4.21-20.EL ro root=LABEL=/
           initrd /initrd-2.4.21-20.EL.img
   ```

7. Añada los parámetros **rhgb** y **quiet** a la línea que especifica el núcleo a ejecutar, **teniendo**

cuidado de dejar un espacio después de root=LABEL=/ ya que de otro modo no podrá iniciar el sistema:

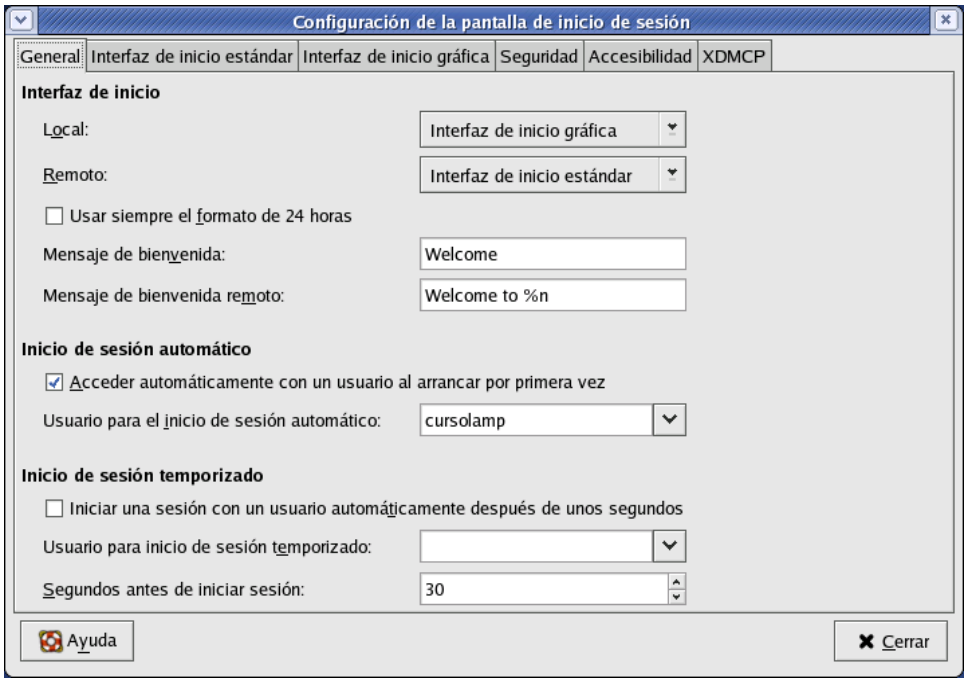
```
title White Box Enterprise Linux (2.4.21-20.EL)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-20.EL ro root=LABEL=/ rhgb quiet
        initrd /initrd-2.4.21-20.EL.img
```

8. Instale el paquete denominado **rhgb**, el cual es un programa que hará que el sistema tenga un arranque gráfico más amistoso para el usuario no-técnico:

```
yum -y install rhgb
```

9. Inicie una sesión gráfica con el mandato xinit. Esto iniciará una sesión gráfica simple con una única terminal xrvt. **No olvide posicionar el puntero del ratón sobre la terminal a fin de darle foco**.

10. Ejecute el mandato **gdmsetup** y establezca que el sistema inicie automáticamente con el usuario cursolamp.



11. **Elimine todas las interfaces virtuales**; es decir, todos los ficheros **ifcfg-eth0:*** localizados dentro del directorio **/etc/sysconfig/network-scripts/**

```
rm -f /etc/sysconfig/network-scripts/ifcfg-eth0:*
```

12. Edite el fichero **/etc/hosts** y elimine todas la resoluciones locales asociadas a las diferentes direcciones IP que fueron configuradas a lo largo del curso. El fichero **/etc/hosts** debe quedar únicamente con el siguiente contenido:

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain localhost
```

13. Edite también el fichero **/etc/sysconfig/network** y establezca de nuevo **localhost.localdomain** como **HOSTNAME** del sistema. Elimine también la línea que deshabilita la configuración de Zeroconf. De modo tal, el fichero **/etc/sysconfig/network** debe quedar únicamente con el siguiente contenido:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

14. Configure de nuevo la interfaz eth0; esta vez como **DHCP** y utilizando el mandato **netconfig**. Desde cualquier terminal, como el usuario root, ejecute el mandato **netconfig**.

15. **Reinicie el sistema** y compruebe que éste lo hace con rhgb y que además inicia automáticamente con la sesión del usuario cursolamp.

Notas

Notas

Notas

Notas