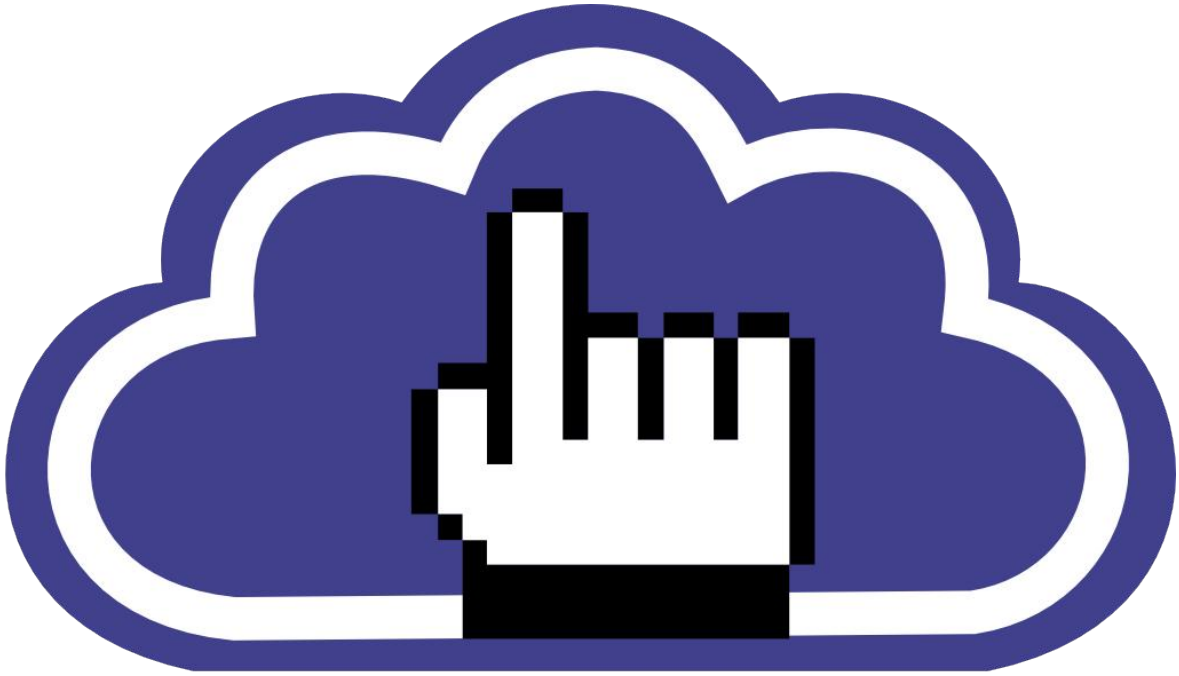


alcance libre

Implementación De Servidores Con GNU/Linux

Edición Septiembre 2009

10 De Septiembre De 2009

Joel Barrios Dueñas

http://visualbook.blogspot.com

Si este libro le ha sido de utilidad, puede contribuir al desarrollo de éste a través de donativos. Sus aportaciones nos ayudarán a crecer y desarrollar más y mejor contenido en el sitio de red y para mejorar este libro.

http://www.alcancelibre.org/staticpages/index.php/donativos

Alcance Libre ofrece soporte técnico gratuito a través de nuestros foros localizados en:

http://www.alcancelibre.org/forum/

Alcance Libre ofrece los siguientes productos y servicios basados sobre Software Libre, gracias a los cuales financia sus operaciones. Para mayor información, estamos disponibles a través del número telefónico (52) (55) 5677-7130 de la ciudad de México, a través de nuestro **Formulario de contacto** o bien directamente en nuestras oficinas centrales en Sicilia 12, Residencial Acoxpa, Tlalpan, México, D.F., C.P. 14300, México.

- Capacitación (cursos)
- Conferencias y pláticas
- Consultoría
- Implementaciones (Servidores)
- Soporte Técnico
- Publicidad en el portal

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 y Julieta, 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.

A mi hijo, Joel Alejandro Barrios Caullieres.

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 de mí. Solía ser médico veterinario zootecnista, dedicado principalmente a 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 la vida en un ámbito completamente distinto al que me dedicaba durante ese tiempo. Yo ya tenía un consultorio veterinario y negocio pequeño de distribución de alimentos para mascotas, los cuales me aseguraban un ingreso regular y constante. 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 cómputo 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.

¿Cómo empecé este proyecto?

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 un instante después mi amigo abrió la puerta. Le saludé con un apretón de manos y tras saludarle de la acostumbrada forma cortés, quedé mudo al ver que la chica de la que me había enamorado durante mis 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, al 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 de comunidad que inicié con Linux Para Todos un 27 de agosto de 1999 y que hoy en día continuo con **Alcance Libre**. Surgió como un sueño, se materializó, se desarrollo y creció más allá de lo que hubiera imaginado.

Es irónico que años después, mi reencuentro con Blanca, quien es hoy en día mi esposa y madre de mi hijo Joel Alejandro, 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 10 años de investigación y experiencias. Mucho del material que le compone fue escrito durante diferentes etapas de mi ciclo mientras fui propietario y administrador de 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.

Respecto del futuro, 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 LinuxParaTodos.net. Dicho dominio fue tomado hostilmente por mi ex-socio quien se quedó con todo y literalmente me dejó en la calle. Dicha empresa continua comercializando mi trabajo violando la licencia Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1, la cual explícitamente prohíbe la explotación comercial de material sin la autorización del autor.
    - 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.
        - Director de proyecto AL Server.
        - Director de proyecto alDOS.
        - 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.
- Lenguaje HTML 4.0
- Lenguaje CSS 1.0
- Programación BASH
- 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, etc.)

Índice de contenido

1.¿Que es GNU/Linux?....31
1.1.Requerimientos del sistema....32

2.Estándar de Jerarquía de Sistema de Ficheros....33
2.1.Introducción....33
2.2.Estructura de directorios....33
2.3.Particiones recomendadas para instalar GNU/Linux....35

3.Instalación en modo texto de CentOS 5....36
3.1.Procedimientos....36

4.Instalación en modo gráfico de CentOS 5....53
4.1.Procedimientos....53

5.Cómo iniciar el modo de rescate en CentOS....72
5.1.Procedimientos....72

6.Iniciando el sistema en nivel de ejecución 1 (nivel mono-usuario)....78
6.1.Introducción....78
6.2.Procedimientos....78

7.Cómo compilar el núcleo (kernel) de GNU/Linux en CentOS....82
7.1.Introducción....82
7.1.1.Un ejemplo del porque conviene recompilar el núcleo....82
7.2.Procedimientos....83
7.2.1.Determinar el sustento físico y controladores....83
7.2.2.Instalación el equipamiento lógico necesario....85
7.2.3.Obtener el código fuente del núcleo....86
7.2.4.Configuración del núcleo....89

8.Cómo gestionar espacio de memoria de intercambio (swap) en GNU/Linux....95
8.1.Introducción....95
8.1.1.Algo de historia....95
8.1.2.¿Qué es y como funciona el espacio de intercambio?....95
8.1.3.Circunstancias en las que se requiere aumentar la cantidad de memoria de intercambio....95
Procedimientos....96
8.1.4.Cambiar el tamaño de la partición....96
8.1.5.Crear un fichero para memoria de intercambio....96
8.2.Procedimientos....96
8.2.1.Activar una partición de intercambio adicional....96
8.2.2.Utilizar un fichero como memoria de intercambio....97
8.2.3.Optimizando el sistema cambiando el valor de /proc/sys/vm/swappiness....98

9.Procedimientos de emergencia....100
9.1.Introducción....100
9.2.Disco de rescate....100
9.3.Verificación de la integridad del disco....101
9.4.Asignación de formato de las particiones....101

10.Cómo optimizar el sistema de archivos ext3....102
10.1.Introducción....102
10.1.1.Acerca de ext3....102
10.1.2.Acerca del registro por diario (journaling)....102
10.2.Procedimientos....102
10.2.1.Utilizando el mandato e2fsck....103
10.2.2.Opciones de montado....103

11.Cómo configurar y utilizar Sudo....107
11.1.Introducción....107
11.1.1.Historia....107
11.2.Equipamiento lógico necesario....108
11.2.1.Instalación a través de yum....108
11.2.2.Instalación a través de Up2date....108
11.3.Fichero /etc/sudoers....108
11.3.1.Cmnd_Alias....108
11.3.2.User_Alias....109
11.3.3.Host_Alias....109
11.3.4.Runas_Alias....109
11.4.Candados de seguridad....109
11.5.Lo que no se recomienda....110
11.6.Facilitando la vida a través de ~/.bash_profile....110

12.Cómo crear cuentas de usuario....112
12.1.Introducción....112
12.2.Procedimientos....112
12.2.1.Creando una cuenta en el modo de texto: useradd y passwd....112
12.2.2.Eliminar una cuenta de usuario....114
12.3.Manejo de grupos....115
12.3.1.Alta de grupos....115
12.3.2.Alta de grupos de sistema....115
12.3.3.Baja de grupos....115
12.3.4.Asignación de usuarios existentes a grupos existentes....115
12.4.Comentarios finales acerca de la seguridad....115
12.5.Apéndice: Configurando valores predefinidos para el alta de cuentas de usuario....117
12.5.1.Fichero /etc/default/useradd para definir variables utilizadas por el mandato useradd....117
12.5.2.Directorio /etc/skel como molde para crear los directorios de inicio de los usuarios....118
12.6.Apéndice: Ejercicio: Creando cuentas de usuario....119
12.6.1.Introducción....119
12.6.2.Procedimientos....119

13.Breve lección de mandatos básicos....121
13.1.Introducción....121
13.2.Procedimientos....121
13.2.1.Visualizando contenido de ficheros....125
13.2.2.Generación de texto por bucles....126
13.2.3.Bucles....127
13.2.4.Aliases....128
13.2.5.Apagado y reinicio de sistema....128
13.3.Resumen de mandatos básicos....129

14.Funciones básicas de vi....130
14.1.Introducción....130
14.2.Procedimientos....130
14.2.1.Instalación y paquetes adicionales....130
14.3.Conociendo vi....130
14.4.Otras combinaciones de teclas....143

14.5.Más allá de las funciones básicas....144

15.Introducción a sed....145
15.1.Introducción....145
15.1.1.Acerca de sed....145
15.2.Procedimientos....145
15.3.Bibliografía....149

16.Introducción a AWK....150
16.1.Introducción....150
16.1.1.Acerca de AWK....150
16.1.2.Estructura de los programas escritos en AWK....150
16.2.Procedimientos....151

17.Permisos del Sistema de Ficheros....156
17.1.Introducción....156
17.2.Notación simbólica....156
17.3.Notación octal....157
17.3.1.Permisos adicionales....157
17.4.Ejemplos....158
17.4.1.Ejemplos de permisos regulares....158
17.4.2.Ejemplos de permisos especiales....159
17.5.Uso de chmod....159
17.5.1.Opciones de chmod....160
17.5.2.El mandato chmod y los enlaces simbólicos....160

18.Cómo utilizar el mandato chattr....161
18.1.Introducción....161
18.1.1.Acerca del mandato chattr....161
18.2.Opciones....161
18.3.Operadores....161
18.4.Atributos....162
18.5.Utilización....162
18.5.1.Ejemplos....162

19.Creando depósitos yum....164
19.1.Introducción....164
19.2.Procedimientos....164

20.Uso de yum para instalar y desinstalar paquetería y actualizar sistema....166
20.1.Introducción....166
20.2.Procedimientos....166
20.2.1.Actualizar sistema....166
20.2.2.Búsquedas....166
20.2.3.Consulta de información....166
20.2.4.Instalación de paquetes....167
20.2.5.Desinstalación de paquetes....167
20.2.6.Listado de paquetes....167
20.2.7.Limpieza del sistema....168

21.Cómo utilizar RPM....169
21.1.Introducción....169
21.1.1.Acerca de RPM....169
21.2.Procedimientos....169
21.2.1.Reconstrucción de la base de datos de RPM....169

21.2.2.Consulta de paquetería instalada en el sistema....169
21.2.3.Instalación de paquetes....172
21.2.4.Desinstalación de paquetes....178

22.Cómo crear paquetería con rpmbuild....180
22.1.Introducción....180
22.2.Instalación del sustento lógico necesario....180
22.3.Procedimientos....181
22.3.1.Creación de la clave GnuPG....181
22.3.2.Configuración y creación de una jaula para rpmbuild....181
22.3.3.Creación de los ficheros*.spec....183
22.3.4.Uso del mandato rpmbuild....186
22.4.Ejercicios....188
22.4.1.Paquete RPM binario y el paquete *.src.rpm correspondiente creando el fichero *.spec necesario....188
22.4.2.Paquete RPM binario y el paquete *.src.rpm correspondiente realizando limpieza de directorio, firma digital....189

23.Cómo asignar cuotas de disco....190
23.1.Introducción....190
23.2.Equipamiento lógico necesario....190
23.2.1.Instalación a través de yum....190
23.2.2.Instalación a través de Up2date....190
23.3.Procedimientos....190
23.3.1.Edquota....191
23.4.Comprobaciones....193

24.Introducción a TCP/IP....194
24.1.Introducción....194
24.2.Niveles de pila....194
24.2.1.Modelo TCP/IP....195
24.2.2.Modelo OSI....200

25.Introducción a IP versión 4....201
25.1.Introducción....201
25.2.Direcciones....201
25.2.1.Representación de las direcciones....201
25.3.Asignación....202
25.3.1.Bloques reservados....202
25.4.Referencia de sub-redes de IP versión 4....203
25.5.Referencias....204

26.Cómo configurar correctamente los parámetros de red....206
26.1.Introducción....206
26.2.Procedimientos....206
26.2.1.Detección y configuración del sustento físico (hardware)....206
26.2.2.Asignación de parámetros de red....207
26.2.3.Agregar encaminamientos (rutas) adicionales....208
26.2.4.Función de Reenvío de paquetes para IP versión 4....208
26.2.5.Comprobaciones....209
26.2.6.Alta de direcciones IP virtuales....209
26.2.7.La función Zeroconf....210
Desactivando el soporte para IPv6....211
26.3.Ejercicios....211
26.3.1.Encaminamientos estáticos....211
26.3.2.Direcciones IP virtuales....214

27.Cómo configurar acoplamiento de tarjetas de red (bonding).....218
27.1.Introducción.....218
27.2.Procedimientos.....218
27.2.1.Fichero de configuración /etc/modprobe.conf.....218
27.2.2.Fichero de configuración /etc/sysconfig/network-scripts/bond0.....220
27.2.3.Iniciar, detener y reiniciar el servicio network.....221
27.3.Comprobaciones.....221
27.4.Bibliografía.....222

28.Cómo conectarse a una red Wifi desde la terminal.....223
28.1.Introducción.....223
28.1.1.Preparativos.....223
28.1.2.Autenticando en el punto de acceso.....224
28.1.3.Asigando parámetros de red a la interfaz.....225

29.Cómo utilizar lsof.....226
29.1.Introducción.....226
29.1.1.Acerca de lsof.....226
29.2.Procedimientos.....226

30.Cómo utilizar Netcat (nc).....229
30.1.Introducción.....229
30.1.1.Acerca de Netcat.....229
30.2.Equipamiento lógico necesario.....229
30.2.1.Instalación a través de yum.....229
30.2.2.Instalación a través de Up2date.....229
30.3.Procedimientos.....229
30.3.1.Conexiones simples.....229
30.3.2.Revisión de puertos.....230
30.3.3.Creando un modelo cliente servidor.....231
30.3.4.Transferencia de datos.....231

31.Como utilizar Netstat.....232
31.1.Introducción.....232
31.1.1.Acerca de Netstat.....232
31.2.Procedimientos.....232

32.Cómo utilizar ARP.....237
32.1.Introducción.....237
32.1.1.Acerca de ARP.....237
32.2.Procedimientos.....237

33.Introducción a IPTABLES.....240
33.1.Introducción.....240
33.1.1.Acerca de Iptables y Netfilter.....240
33.2.Equipamiento lógico necesario.....240
33.2.1.Instalación a través de yum.....240
33.2.2.Instalación a través de up2date.....240
33.3.Procedimientos.....241
33.3.1.Cadenas.....241
33.3.2.Reglas de destino.....241
33.3.3.Políticas por defecto.....241
33.3.4.Limpieza de reglas específicas.....241
33.3.5.Reglas específicas.....241
Ejemplos de reglas.....242
33.3.6.Eliminar reglas.....243

33.3.7.Mostrar la lista de cadenas y reglas....243
33.3.8.Iniciar, detener y reiniciar el servicio iptables....245
33.3.9.Agregar el servicio iptables al arranque del sistema....245
33.4.Bibliografía....246

34.Cómo utilizar CBQ....247
34.1.Introducción....247
34.1.1.Acerca de cbq....247
34.2.Comprendiendo la velocidad binaria (bit rate)....247
34.3.Equipamiento lógico necesario....248
34.3.1.Instalación a través de yum....248
34.3.2.Instalación a través de up2date....248
34.4.Preparativos....248
34.4.1.Parámetro DEVICE....248
34.4.2.Parámetro de clase WEIGHT....249
34.4.3.Parámetro de clase PRIO....249
34.4.4.Parámetro de clase PARENT....249
34.4.5.Parámetro de clase LEAF....250
34.4.6.Parámetro de clase BOUNDED....250
34.4.7.Parámetro de clase ISOLETED....251
34.4.8.Parámetros de filtración....251
34.5.Procedimientos....253
34.5.1.CBQ sin compartir ancho de banda entre clases....254
34.5.2.CBQ compartiendo ancho de banda entre clases....255
34.5.3.Iniciar, detener y reiniciar el servicio cbq....255
34.5.4.Agregar el servicio cbq al arranque del sistema....256

35.Introducción a SELinux en CentOS 5 y Fedora....257
35.1.Introducción....257
35.2.¿Qué es SELinux?....257
35.3.Mandato getsebool....257
35.4.Mandato setsebool....258
35.4.1.Servicios de FTP....258
35.4.2.OpenVPN....259
35.4.3.Apache....259
35.4.4.Samba....259
35.4.5.Otros servicios....260

36.Cómo configurar un servidor DHCP en una LAN....262
36.1.Introducción....262
36.1.1.Acerca del protocolo DHCP....262
36.1.2.Acerca de dhcp por Internet Software Consortium, Inc....262
36.2.Equipamiento lógico necesario....263
36.2.1.Instalación a través de yum....263
36.2.2.Instalación a través de up2date....263
36.3.Procedimientos....263
36.3.1.SELinux y el servicio dhcpd....263
36.3.2.Fichero de configuración /etc/dhcpd.conf....263
36.3.3.Fichero de configuración /etc/sysconfig/dhcpd....264
36.3.4.Iniciar, detener y reiniciar el servicio dhcpd....265
36.3.5.Agregar el servicio dhcpd al arranque del sistema....265
36.4.Comprobaciones desde cliente DHCP....265
36.5.Modificaciones necesarias en el muro cortafuegos....266

37.Cómo configurar vsftpd (Very Secure FTP Daemon)....267
37.1.Introducción....267
37.1.1.Acerca del protocolo FTP....267
37.1.2.Acerca del protocolo FTPS....267

37.1.3.Acerca de RSA....267
37.1.4.Acerca de OpenSSL....268
37.1.5.Acerca de X.509....268
37.1.6.Acerca de vsftpd....268
37.2.Equipamiento lógico necesario....268
37.2.1.Instalación a través de yum....268
37.2.2.Instalación a través de up2date....268
37.3.Ficheros de configuración....268
37.4.Procedimientos....269
37.4.1.SELinux y el servicio vsftpd....269
37.4.2.Fichero /etc/vsftpd/vsftpd.conf....269
37.4.3.Parámetro anonymous_enable....269
37.4.4.Parámetro local_enable....269
37.4.5.Parámetro write_enable....270
37.4.6.Parámetro anon_upload_enable....270
37.4.7.Parámetro anon_mkdir_write_enable....270
37.4.8.Parámetro ftpd_banner....270
37.4.9.Estableciendo jaulas para los usuarios: parámetros chroot_local_user y chroot_list_file....270
37.4.10.Control del ancho de banda....271
37.4.11.Soporte SSL/TLS para VFSTPD....271
37.4.12.Iniciar, detener y reiniciar el servicio vsftpd....273
37.4.13.Agregar el servicio al arranque del sistema....273
37.5.Modificaciones necesarias en el muro cortafuegos....273
37.6.Ejercicio VSFTPD....274

38.Cómo configurar pure-ftpd....276
38.1.Introducción....276
38.1.1.Acerca del protocolo FTP....276
38.1.2.Acerca de pure-ftpd....276
38.2.Equipamiento lógico necesario....276
38.2.1.Instalación a través de yum....276
38.3.Procedimientos....277
38.3.1.Fichero de configuración /etc/pure-ftpd/pure-ftpd.conf....277
38.3.2.Agregar el servicio al arranque del sistema....280
38.3.3.Iniciar, detener y reiniciar servicio....280
38.4.Modificaciones necesarias en el muro cortafuegos....280

39.Cómo configurar OpenSSH....281
39.1.Introducción....281
39.1.1.Acerca de SSH....281
39.1.2.Acerca de SFTP....281
39.1.3.Acerca de SCP....281
39.1.4.Acerca de OpenSSH....281
39.2.Equipamiento lógico necesario....282
39.3.Ficheros de configuración....282
39.4.Procedimientos....282
39.4.1.Parámetro Port....282
39.4.2.Parámetro ListenAddress....282
39.4.3.Parámetro PermitRootLogin....282
39.4.4.Parámetro X11Forwarding....283
39.4.5.Parámetro AllowUsers....283
39.5.Aplicando los cambios....283
39.6.Probando OpenSSH....284
39.6.1.Acceso a través de intérprete de mandatos....284
39.6.2.Transferencia de ficheros a través de SFTP....284
39.6.3.Transferencia de ficheros a través de SCP....285
39.7.Modificaciones necesarias en el muro cortafuegos....286

40.Cómo utilizar OpenSSH con autenticación a través de clave pública....287

40.1.Introducción....287
40.2.Procedimientos....287
40.2.1.Modificaciones en el Servidor....287
40.2.2.Modificaciones en el Cliente....287
40.2.3.Comprobaciones....288

41.Cómo configurar OpenSSH con Chroot....289
41.1.Introducción....289
41.2.Equipamiento lógico necesario....289
41.3.Procedimientos....291
41.3.1.Componentes mínimos para la jaula....291
41.3.2.Ficheros /etc/passwd y /etc/group....292
41.3.3.Dispositivos de bloque....292
41.4.Ejemplo práctico....292
41.4.1.Crear las cuentas de los usuarios....292
41.4.2.Ejemplo aplicado a sitio de red virtual con Apache....293

42.Cómo configurar NTP....295
42.1.Introducción....295
42.1.1.Acerca de NTP....295
42.1.2.Acerca de UTC....296
42.2.Equipamiento lógico necesario....296
42.2.1.Instalación a través de yum....296
42.2.2.Instalación a través de up2date....296
42.3.Procedimientos....296
42.3.1.Herramienta ntpdate....296
42.3.2.Fichero de configuración /etc/ntp.conf....296
42.3.3.Iniciar, detener y reiniciar el servicio ntpd....297
42.3.4.Agregar el servicio ntpd al arranque del sistema....298
42.4.Modificaciones necesarias en el muro cortafuegos....298

43.Cómo configurar Clamd....299
43.1.Introducción....299
43.2.Instalación de equipamiento lógico necesario....299
43.3.Procedimientos....299
43.3.1.SELinux y el servicio clamd....299
43.3.2.Configuración de Clamd....300

44.Cómo configurar el sistema para sesiones gráficas remotas....304
44.1.Introducción....304
44.2.Sesión gráfica remota con GDM....304
44.2.1.Procedimiento....304

45.Cómo configurar un servidor NFS....307
45.1.Introducción....307
45.2.Procedimientos....307
45.2.1.Instalación del sustento lógico necesario....307
45.3.Configurando la seguridad....307
45.3.1.Compartir un volumen NFS....308
45.3.2.Configurando las máquinas clientes....309
45.4.Instalación de GNU/Linux a través de un servidor NFS....310

46.Cómo configurar Samba básico....312
46.1.Introducción....312
46.1.1.Acerca del protocolo SMB....312
46.1.2.Acerca de Samba....312

46.2.Equipamiento lógico necesario....312
46.2.1.Instalación a través de yum....313
46.2.2.Instalación a través de up2date....313
46.3.Procedimientos....313
46.3.1.SELinux y el servicio smb....313
46.3.2.Alta de cuentas de usuario....314
46.3.3.El fichero lmhosts....314
46.3.4.Parámetros principales del fichero smb.conf....314
46.3.5.Parámetro remote announce....315
46.3.6.Impresoras en Samba....316
46.3.7.Compartiendo directorios a través de Samba....316
46.4.Iniciar el servicio y añadirlo al arranque del sistema....319
46.5.Comprobaciones....319
46.5.1.Modo texto....319
46.5.2.Modo gráfico....321

47.Cómo configurar Samba denegando acceso a ciertos ficheros....322
47.1.Introducción....322
47.2.Procedimientos....322
47.3.Aplicando los cambios....322
47.4.Comprobaciones....323

48.Cómo configurar Samba con Papelera de Reciclaje....324
48.1.Introducción....324
48.2.Procedimientos....324
48.3.Aplicando los cambios....326
48.4.Comprobaciones....326

49.Cómo instalar y configurar Samba-Vscan en CentOS 5....329
49.1.Introducción....329
49.2.Acerca de Samba-Vscan....329
49.3.Instalación de equipamiento lógico necesario....329
49.4.Procedimientos....329

50.Cómo configurar Samba como cliente o servidor WINS....333
50.1.Introducción....333
50.2.Procedimientos....333
50.2.1.Parámetros wins server y wins support....333
50.2.2.Parámetro name resolve order....334
50.2.3.Parámetro wins proxy....334
50.2.4.Parámetro dns proxy....334
50.2.5.Parámetro max ttl....334
50.2.6.Parámetros max wins ttl y min wins ttl....334
50.3.Aplicando los cambios....335

51.La ingeniería social y los [incorrectos] hábitos del usuario....336
51.1.Recomendaciones para evitar ser víctimas de la ingeniería social a través del correo electrónico....337

52.Configuración básica de Sendmail....338
52.1.Introducción....338
52.1.1.Acerca de Sendmail....338
52.1.2.Acerca de Dovecot....338
52.1.3.Acerca de SASL y Cyrus SASL....338
52.1.4.Protocolos utilizados....339
52.2.Equipamiento lógico necesario....341

52.2.1.Instalación a través de yum....342
52.2.2.Instalación a través de Up2date....342
52.3.Procedimientos....342
52.3.1.Alta de cuentas de usuario y asignación de claves de acceso....342
52.3.2.Dominios a administrar....343
52.3.3.Control de acceso....344
52.3.4.Alias de la cuenta de root....345
52.3.5.Configuración de funciones de Sendmail....345
52.3.6.Usuarios Virtuales....347
52.3.7.Control del correo chatarra (Spam) a través de DNSBLs....348
52.3.8.Protocolos para acceder hacia el correo....348
52.3.9.Reiniciando servicio....349
52.4.Encaminamiento de dominios....349
52.4.1.Redundancia del servidor de correo....349
52.4.2.Servidor de correo intermediario....350
52.5.Verificando el servicio....351
52.6.Pruebas para el envío de correo....352
52.6.1.Utilizando telnet....352
52.6.2.Utilizando mutt....354
52.7.Referencias....354

53.Opciones avanzadas de seguridad para Sendmail....356
53.1.Introducción....356
53.2.Funciones....356
53.2.1.confMAX_RCPTS_PER_MESSAGE....356
53.2.2.confBAD_RCPT_THROTTLE....356
53.2.3.confPRIVACY_FLAGS....356
53.2.4.confMAX_HEADERS_LENGTH....357
53.2.5.confMAX_MESSAGE_SIZE....357
53.2.6.confMAX_DAEMON_CHILDREN....357
53.2.7.confCONNECTION_RATE_THROTTLE....357

54.Cómo configurar Sendmail y Dovecot con soporte SSL/TLS....358
54.1.Introducción....358
54.1.1.Acerca de DSA....358
54.1.2.Acerca de RSA....358
54.1.3.Acerca de X.509....358
54.1.4.Acerca de OpenSSL....359
54.2.Procedimientos....359
54.2.1.Sendmail. 359
54.2.2.Dovecot. 361
54.2.3.Configuración de GNOME Evolution....363
54.2.4.Modificaciones necesarias en el muro cortafuegos....366

55.Cómo configurar Cyrus IMAP....368
55.1.Introducción....368
55.2.Equipamiento lógico necesario....368
55.2.1.Instalación a través de yum....368
55.2.2.Instalación a través de up2date....368
55.3.Procedimientos....369
55.3.1.Alta de cuentas de usuario y asignación de claves de acceso....369
55.3.2.Iniciar, detener y reiniciar el servicio cyrus-imapd....370
55.3.3.Agregar el servicio cyrus-imapd al arranque del sistema....370
55.3.4.Integración con Sendmail....370
55.4.Comprobaciones....370

56.Instalación y configuración de SquirrelMail (correo a través de interfaz HTTP)... 373

56.1.Introducción....373
56.2.Procedimientos....373
56.2.1.Instalación del sustento lógico necesario....373
56.2.2.Configuración de SquirrelMail....373
56.3.Finalizando configuración....376
56.4.Ajustes en php.ini para optimizar el uso de Squirrelmail....377

57.Cómo instalar GroupOffice en CentOS....379
57.1.¿Qué es Group Office?....379
57.2.Equipamiento lógico necesario....380
57.2.1.Configuración de depósitos YUM para CentOS 5 y Red Hat Enterprise Linux 5....380
57.3.Procedimientos....380
57.3.1.Ajustes posteriores a la instalación....383

58.Apéndice: Enviar correo a todos los usuarios del sistema....390
58.1.Procedimientos....390
58.2.Acerca de la seguridad....390

59.Cómo instalar y configurar el programa vacation para responder avisos automáticos en vacaciones....391
59.1.Intrucción....391
59.2.Equipamiento lógico necesario....391
59.2.1.Instalación a través de yum....391
59.2.2.Instalación a través de up2date....391
59.3.Procedimientos....392

60.Cómo configurar clamav-milter....394
60.1.Introducción....394
60.1.1.Acerca de clamav-milter....394
60.1.2.Acerca de ClamAV....394
60.2.Equipamiento lógico necesario....394
60.2.1.Instalación a través de yum....395
60.3.Procedimientos....395
60.3.1.SELinux y el servicio clamav-milter....395
60.3.2.Requisitos previos....395
60.3.3.Fichero /etc/mail/sendmail.mc....395
60.3.4.Configuración....396
60.3.5.Iniciar, detener y reiniciar el servicio clamav-milter....396

61.Cómo configurar spamass-milter....397
61.1.Introducción....397
61.1.1.Acerca de spamass-milter....397
61.1.2.Acerca de SpamAssassin....397
61.2.Equipamiento lógico necesario....397
61.2.1.Instalación a través de yum....397
61.3.Procedimientos....398
61.3.1.SELinux y el servicio spamass-milter....398
61.3.2.Requisitos previos....398
61.3.3.Fichero /etc/mail/sendmail.mc....398
61.3.4.Configuración....398
61.3.5.Fichero /etc/sysconfig/spamass-milter....399
61.3.6.Fichero /etc/procmailrc....400
Fichero /etc/sysconfig/spamassassin....401
61.3.7.Iniciar, detener y reiniciar el servicio spamass-milter....401

62.Cómo configurar un servidor NIS....402

62.1.Introducción....402
62.2.Procedimientos....402
Instalación del equipamiento lógico necesario en el servidor NIS....402
62.2.2.Configuración del servidor NIS....403
62.2.3.Instalación del equipamiento lógico necesario en el cliente NIS....405
62.2.4.Configuración del cliente NIS....405

63.Cómo configurar OpenLDAP como servidor de autenticación....408
63.1.Introducción....408
63.2.Equipamiento lógico necesario....408
63.2.1.Instalación a través de yum....408
63.2.2.Instalación a través de up2date....408
63.3.Procedimientos....409
63.3.1.SELinux y el servicio ldap....409
63.3.2.Creación de directorios....409
63.3.3.Generación de claves de acceso para LDAP....409
63.3.4.Fichero de configuración /etc/openldap/slapd.conf....409
63.3.5.Inicio del servicio ldap....410
63.3.6.Migración de cuentas existentes en el sistema....410
63.4.Comprobaciones....411
63.5.Configuración de clientes....412
63.5.1.authconfig (modo-texto)....413
63.5.2.authconfig-tui (modo texto)....413
63.5.3.authconfig-gtk (modo gráfico)....414
63.6.Administración....415
63.7.Respaldo de datos....415
63.8.Restauración de datos....416
63.9.Modificaciones necesarias en el muro cortafuegos....416

64.Cómo configurar OpenLDAP como libreta de direcciones....417
64.1.Introducción....417
64.2.Equipamiento lógico necesario....417
64.2.1.Instalación a través de yum....417
64.2.2.Instalación a través de up2date....417
64.3.Procedimientos....417
64.3.1.SELinux y el servicio ldap....417
64.3.2.Creación de directorios....418
64.3.3.Generación de claves de acceso para LDAP....418
64.3.4.Fichero de esquemas....418
64.3.5.Fichero de configuración /etc/openldap/slapd.conf....418
64.3.6.Inicio del servicio ldap....419
64.3.7.Añadir datos al directorio....419
64.4.Configuración de clientes....421
64.4.1.Novell Evolution....421
64.4.2.Mozilla Thunderbird....423
64.4.3.Squirrelmail....424
64.5.Administración....424
64.6.Respaldo de datos....424
64.7.Restauración de datos....425
64.8.Modificaciones necesarias en el muro cortafuegos....425

65.Cómo configurar OpenLDAP con soporte SSL/TLS....426
65.1.Introducción....426
65.1.1.Acerca de LDAP en modo SSL/TLS....426
65.1.2.Acerca de RSA....426
65.1.3.Acerca de X.509....426
65.1.4.Acerca de OpenSSL....427
65.2.Procedimientos....427

65.2.1.Generando clave y certificado....427
65.2.2.Parámetros de /etc/openldap/slapd.conf....428
65.2.3.Comprobación....428
65.2.4.Configuración de GNOME Evolution....428
65.2.5.Configuración de Mozilla Thunderbird....429
65.2.6.Configuración LDAP Browser....430
65.2.7.Configuración LDAP Administration Tool....430
65.3.Modificaciones necesarias en el muro cortafuegos....431

66.Cómo instalar y configurar MySQL™....432
66.1.Introducción....432
66.1.1.Acerca de MySQL™....432
66.2.Equipamiento lógico necesario....432
66.2.1.Instalación a través de yum....432
66.2.2.Instalación a través de up2date....432
66.3.Procedimientos....433
66.3.1.SELinux y el servicio mysqld....433
66.3.2.Iniciar, detener y reiniciar el servicio mysqld....433
66.3.3.Agregar el servicio mysqld al arranque del sistema....433
66.3.4.Asignación de clave de acceso al usuario root....433
66.4.Creando y destruyendo bases de datos....435
66.5.Otorgando permisos a los usuarios....435
66.6.Modificaciones necesarias en el muro cortafuegos....436

67.Configuración básica de Apache....438
67.1.Introducción....438
67.1.1.Acerca del protocolo HTTP....438
67.1.2.Acerca de Apache....438
67.2.Equipamiento lógico necesario....438
67.2.1.Instalación a través de yum....438
67.2.2.Instalación a través de Up2date....439
67.3.Iniciar servicio y añadir el servicio al arranque del sistema....439
67.4.Procedimientos....440
67.4.1.SELinux y Apache....440
67.4.2.UTF-8 y codificación de documentos....441
67.4.3.Ficheros de configuración....442
67.4.4.Directorios virtuales....442
67.4.5.Redirección de directorios....443
67.4.6.Tipos de MIME....443
67.4.7.Soporte para CGI con extensión *.cgi....443
67.4.8.Robo de imágenes....445
67.5.Modificaciones necesarias en el muro cortafuegos....445
67.6.Apéndice: Configuración de Sitios de Red virtuales en Apache....445

68.Cómo habilitar los ficheros .htaccess y SSI)Server Side Includes) en Apache 2.x....447
68.1.Introducción....447
68.2.Procedimientos....447
68.2.1.Autenticación de directorios....447
68.2.2.Asignación de directivas para PHP....448

69.Cómo configurar Apache con soporte SSL/TLS. 451
69.1.Introducción....451
69.1.1.Acerca de HTTPS....451
69.1.2.Acerca de RSA....451
69.1.3.Acerca de Triple DES....451
69.1.4.Acerca de X.509....452
69.1.5.Acerca de OpenSSL....452

69.1.6.Acerca de mod_ssl....452
69.2.Requisitos....452
69.3.Equipamiento lógico necesario....452
69.3.1.Instalación a través de yum....452
69.3.2.Instalación a través de Up2date....453
69.4.Procedimientos....453
69.4.1.Generando clave y certificado....453
69.4.2.Configuración de Apache....455
69.4.3.Comprobación....456
69.4.4.Modificaciones necesarias en el muro cortafuegos....456

70.Cómo configurar un servidor de nombres de dominio (DNS)....457
70.1.Introducción....457
70.1.1.Bind (Berkeley Internet Name Domain)....457
70.1.2.DNS (Domain Name System)....457
70.1.3.NIC (Network Information Center)....457
70.1.4.FQDN (Fully Qualified Domain Name)....458
70.1.5.Componentes de un DNS....458
70.1.6.Herramientas de búsqueda y consulta....460
70.2.Equipamiento lógico necesario....462
70.2.1.Instalación a través de yum....462
70.2.2.Instalación a través de Up2date....462
70.3.Procedimientos....462
70.3.1.SELinux y el servicio named....462
70.3.2.Preparativos....463
70.3.3.Creación de los ficheros de zona....464
70.3.4.Seguridad adicional en DNS para uso público....467
70.3.5.Seguridad adicional en DNS para uso exclusivo en red local....471
70.3.6.Las zonas esclavas....471
70.3.7.Seguridad adicional para transferencias de zona....472
70.3.8.Reiniciar servicio y depuración de configuración....475

71.Cómo configurar Squid: Parámetros básicos para Servidor Intermediario (Proxy)....477
71.1.Introducción....477
71.1.1.¿Qué es Servidor Intermediario (Proxy)?....477
71.1.2.Acerca de Squid....478
71.2.Equipamiento lógico necesario....479
71.2.1.Instalación a través de yum....479
71.2.2.Instalación a través de up2date....479
71.2.3.Otros componentes necesarios....479
71.3.SELinux y el servicio squid....480
71.4.Antes de continuar....480
71.5.Configuración básica....480
71.5.1.Parámetro http_port: ¿Que puerto utilizar para Squid?....481
71.5.2.Parámetro cache_mem....482
71.5.3.Parámetro cache_dir: ¿Cuanto desea almacenar de Internet en el disco duro?....482
71.5.4.Parámetro ftp_user....483
71.5.5.Controles de acceso....483
71.5.6.Aplicando Listas y Reglas de control de acceso....484
71.5.7.Parámetro chache_mgr....486
71.5.8.Parámetro cache_peer: caches padres y hermanos....486
71.6.Caché con aceleración....487
71.6.1.Proxy Acelerado: Opciones para Servidor Intermediario (Proxy) en modo convencional....487
71.6.2.Proxy Acelerado: Opciones para Servidor Intermediario (Proxy) Transparente....488
71.6.3.Proxy Acelerado: Opciones para Servidor Intermediario (Proxy) Transparente para redes con Internet Exlorer 5.5 y versiones anteriores....488
71.7.Estableciendo el idioma de los mensajes mostrados por de Squid hacia el usuario....489
71.8.Iniciando, reiniciando y añadiendo el servicio al arranque del sistema....489
71.9.Depuración de errores....489

71.10.Ajustes para el muro corta-fuegos....490
71.10.1.Re-direccionamiento de peticiones a través de iptables y Firestarter....490
71.10.2.Re-direccionamiento de peticiones a través de la opción REDIRECT en Shorewall....490

72.Cómo configurar Squid: Acceso por autenticación....492
72.1.Introducción....492
72.2.Equipamiento lógico necesario....492
72.3.Eligiendo el módulo de autenticación....492
72.3.1.Autenticación a través del módulo LDAP....492
72.3.2.Autenticación a través del módulo NCSA....493
72.4.Listas y reglas de control de acceso....494
72.4.1.Finalizando procedimiento....495

73.Cómo configurar Squid: Restricción de acceso a Sitios de Red....496
73.1.Introducción....496
73.2.Equipamiento lógico necesario....496
73.3.Definiendo patrones comunes....496
73.4.Parámetros en /etc/squid/squid.conf....497
73.4.1.Permitiendo acceso a sitios inocentes incidentalmente bloqueados....497
73.4.2.Finalizando procedimiento....498

74.Cómo configurar Squid: Restricción de acceso a contenido por extensión....499
74.1.Introducción....499
74.2.Software requerido....499
74.3.Definiendo elementos de la Lista de Control de Acceso....499
74.4.Parámetros en /etc/squid/squid.conf....500
74.4.1.Finalizando procedimiento....501

75.Cómo configurar Squid: Restricción de acceso por horarios....502
75.1.Introducción....502
75.2.Equipamiento lógico necesario....502
75.3.Procedimientos....502
75.3.1.Más ejemplos....503
75.3.2.Finalizando procedimiento....504

76.Cómo configurar squid con soporte para direcciones MAC....505
76.1.Introducción....505
76.1.1.Acerca de Squid....505
76.2.Equipamiento lógico necesario....505
76.2.1.Instalación a través de yum....505
76.3.Procedimientos....506
Fichero /etc/squid/listas/macsredlocal....506
76.3.1.Fichero /etc/squid/squid.conf....507
76.4.Iniciar, detener y reiniciar el servicio squid....507

77.Cómo instalar y configurar la herramienta de reportes Sarg....509
77.1.Introducción....509
77.2.Equipamiento lógico necesario....509
77.3.Procedimientos....509

78.Apéndice: Listas y reglas de control de acceso para Squid....513
78.0.1.Reglas aplicadas....513

79.Cómo configurar un muro cortafuegos con Shorewall y tres interfaces de red....

515
79.1.Introducción....515
79.1.1.Acerca de Shorewall....515
79.1.2.Acerca de Iptables y Netfilter....515
79.1.3.Acerca de Iproute....515
79.1.4.Requisitos....516
79.2.Conceptos requeridos....516
79.2.1.¿Qué es una zona desmilitarizada?....516
79.2.2.¿Que es una Red Privada?....516
79.2.3.¿Qué es un NAT?....517
79.2.4.¿Qué es un DNAT?....517
79.3.Procedimientos....517
79.3.1.Equipamiento lógico necesario....517
79.3.2.Fichero de configuración /etc/shorewall/shorewall.conf....517
79.3.3.Fichero de configuración /etc/shorewall/zones....518
79.3.4.Fichero de configuración /etc/shorewall/interfaces....518
79.3.5.Fichero de configuración /etc/shorewall/policy....519
79.3.6.Fichero de configuración /etc/shorewall/masq....520
79.3.7.Fichero de configuración /etc/shorewall/rules....520
79.4.Iniciar el cortafuegos y añadirlo a los servicios de arranque del sistema....523

80.Cómo configurar un servidor de OpenVPN en CentOS 5....524
80.1.Introducción....524
80.1.1.Acerca de OpenVPN....524
80.1.2.Breve explicación de lo que se logrará con este documento....524
80.2.Instalación del equipamiento lógico necesario....525
80.2.1.Instalación en CentOS 5....525
80.3.Procedimientos....526
80.3.1.Configuración de muro cortafuegos con Shorewall....529
80.3.2.Configuración de clientes Windows....530
80.3.3.Clientes GNU/Linux....533
80.4.Bibiliografía....539

81.Cómo configurar SNMP....540
81.1.Introducción....540
81.1.1.Acerca de SNMP....540
81.1.2.Acerca de Net-SNMP....540
81.2.Equipamiento lógico necesario....540
81.2.1.Instalación a través de yum....540
81.2.2.Instalación a través de up2date....540
81.3.Procedimientos....541
Fichero de configuración /etc/snmp/snmpd.conf....541
81.3.2.Un ejemplo funcional de configuración....542
81.3.3.Iniciar, detener y reiniciar el servicio snmpd....543
81.3.4.Agregar el servicio snmpd al arranque del sistema....544
81.4.Comprobaciones....544
81.5.Modificaciones necesarias en el muro cortafuegos....544

82.Cómo configurar MRTG....545
82.1.Introducción....545
82.1.1.Acerca de MRTG....545
82.2.Equipamiento lógico necesario....545
82.2.1.Instalación a través de yum....545
82.2.2.Instalación a través de up2date....545
82.3.Procedimientos....545
82.4.Comprobaciones....546

83.Cómo instalar Java 1.5 en CentOS 5....548

83.1.Introducción....548
83.2.Instalación del equipamiento lógico necesario....548
83.2.1.Instalación a través de yum....548
83.3.Procedimientos....548
83.3.1.Creación de usuario para utilizar rpmbuild....548
83.3.2.Creación de estructura de directorios para rpmbuild....548

84.Cómo instalar la complemento (plug-in) Flash Player para Firefox y otros navegadores....551
84.1.Introducción....551
84.2.Procedimientos....551
84.2.1.Fedora, CentOS 5 y Red Hat Enterprise Linux 5....551
84.2.2.CentOS 4 y Red Hat Enterprise Linux 4....552
84.3.Comprobaciones....552

85.Cómo configurar escáner en red....554
85.1.Introducción....554
85.1.1.Acerca de SANE....554
85.1.2.Acerca de Xsane....554
85.2.Equipamiento lógico necesario....555
85.2.1.Instalación del servicio saned....555
85.2.2.Instalación del cliente Xsane....555
85.3.Procedimientos....555
85.3.1.Configuración del servicio saned....555
85.3.2.Configuración del cliente Xsane....557

86.Usando Smartd para anticipar los desastres de disco duro....558
86.1.Introducción....558
86.2.Procedimientos....558

87.Cómo crear un disco con instalación personalizada de CentOS 5....560
87.1.Instalación de equipamiento lógico necesario....560
87.2.Procedimientos....560
87.2.1.Creación de fichero de configuración de instalación personalizada....560
87.2.2.Creación del directorio de trabajo y contenido del mismo....561
87.2.3.Añadir equipamiento lógico adicional....563
87.2.4.Creación de la imagen ISO....564

88.Ejercicios....566
88.1.Ejercicio NFS....566
88.1.1.Introducción....566
88.1.2.Procedimientos....566
88.2.Ejercicio SAMBA....568
88.2.1.Procedimientos....568
88.3.Ejercicio Apache® y VSFTPD....571
88.3.1.Procedimientos....571
88.3.2.Comprobaciones....572
88.4.Ejercicio: Cuotas de disco, Apache, VSFTPD y DNS....574
88.4.1.Procedimientos....574
88.4.2.Comprobaciones....578
88.5.Ejercicio: Servidor Intermediario (Proxy)....580
88.5.1.Introducción....580
Procedimientos....580

89.Ejercicio: Servidor DNS dinámico, servidor DHCP, Servidor Intermediario (Proxy) y Shorewall....586

89.1.Introducción....586
89.1.1.Política: cerrar todo y abrir solo lo necesario....586
89.2.Equipamiento lógico necesario....586
89.3.Procedimientos....587
89.3.1.Modificación de la interfaz de acceso hacia Internet....587
Configuración de servidor DNS....588
Configuración de servidor DHCP....591
Configuración de Squid....593
Configuración de Shorewall....598
Instalar y configurar la herramienta de reportes Sarg....602

90.Ejercicio: configuración del sistema para Linux, Apache, PHP y MySQL....603

91.Ejercicio: Configuración del sistema como estación de trabajo....606

Notas....609

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.

La información contenida en este manual se distribuye con la esperanza de que sea de utilidad, y se proporciona tal cual es pero **SIN GARANTÌA ALGUNA**, aún sin la garantía implícita de comercialización o adecuamiento para un propósito en particular, y el autor o autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de esta.

1. ¿Que es GNU/Linux?

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

Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.1

GNU es un acrónimo recursivo que significa **GNU No es Unix** (**G**NU is **N**ot **U**nix). Este proyecto fue iniciado por **Richard Stallman**, y anunciado el 27 de septiembre de 1983, con el objetivo de crear un sistema operativo completamente libre.

GNU/Linux® es un poderoso y sumamente versátil sistema operativo con licencia libre y que implemente 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. En 1992, el núcleo **Linux**> fue combinado con el sistema **GNU**. El Sistema Operativo formado por esta combinación se conoce como **GNU/Linux**.

GNU/Linux es **equipamiento lógico libre** o *Software Libre*. Esto significa que el usuario tiene la libertad de redistribuir y modificar a 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 equipamiento lógico 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 equipamiento lógico gratuito** (comúnmente denominado como Freeware), se trata de **equipamiento lógico libre** o *Software Libre*. Cuando nos referirnos a *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 equipamiento lógico (y cobrar por el servicio si así lo desea). La **GPL** tiene como objetivo garantizar al usuario la libertad de compartir y cambiar **equipamiento lógico libre**, es decir, asegurarse de que el equipamiento lógico siempre permanezca libre para todos los usuarios. La **GPL** es aplicable a la mayoría del equipamiento lógico de la Free Software Foundation así como a cualquier otro programa cuyos autores se comprometan a usarlo.

GNU/Linux® es también de la mejor alternativa de siglo XXI para los usuarios que no solo desean libertad, sino que también desean 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 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

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

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 (**FHS** 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 procesos de desarrollar un estándar de sistema de ficheros jerárquico inició en Agosto de 1993 con un esfuerzo para reestructurar la 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 el desarrollar una versión de **FSSTND** más detallada y dirigida no solo hacia Linux sino también hacia otros sistemas operativos similares a Unix. Como uno de los resultados el estándar cambió de nombre a **FHS** o **F**ilesystem **H**ierarchy **S**tandard.

El **FHS** es mantenido por **Free Standards Group**, una organización sin fines de lucro constituida por compañías que manufacturan equipamiento físico (Hardware) y lógico (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 FHS 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 inicios 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 (super-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 solo 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 solo 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 de 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 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.

Directorio.	Descripción
/var/tmp/	Ficheros temporales preservados entre reinicios.

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

2.3. Particiones recomendadas para instalar GNU/Linux.

Como mínimo se requieren tres particiones:

/boot	Requiere al menos 75 MB. Asignar más espacio puede considerarse desperdicio.
/	Requiere de 512 a 1024 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	Requiere al menos 1.5 GB en instalaciones básicas. Debe considerarse el equipamiento 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.

3. Instalación en modo texto de CentOS 5.

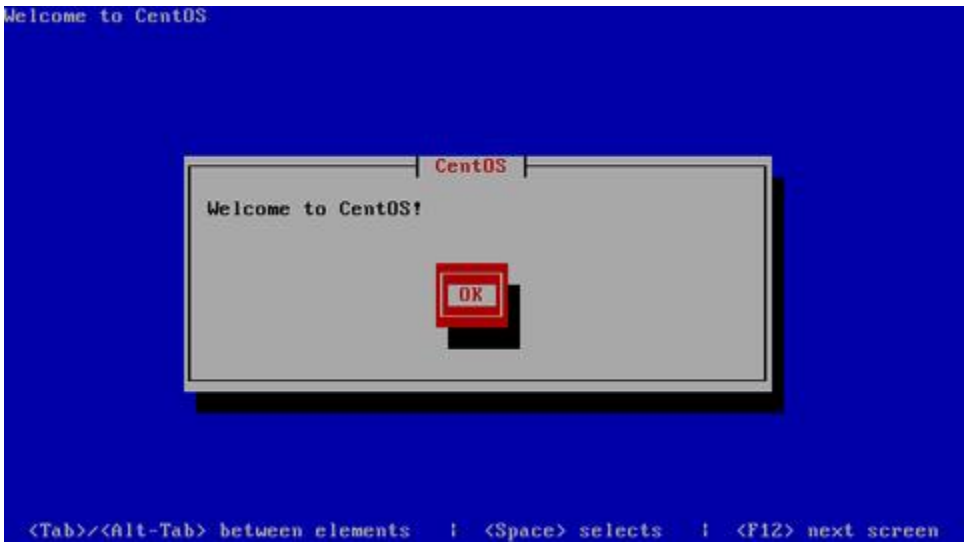
Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*

3.1. 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.

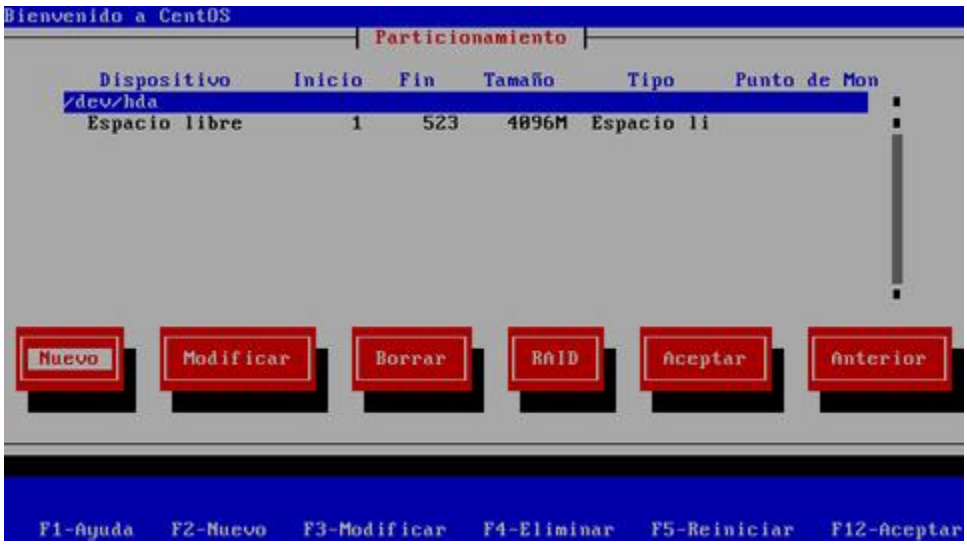
Si se trata de un **disco duro nuevo y/o sin particiones**, el sistema le advertirá que es necesario inicializar la unidad. Seleccione **«Si»** y pulse la tecla **ENTER** para realizar la operación.

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.

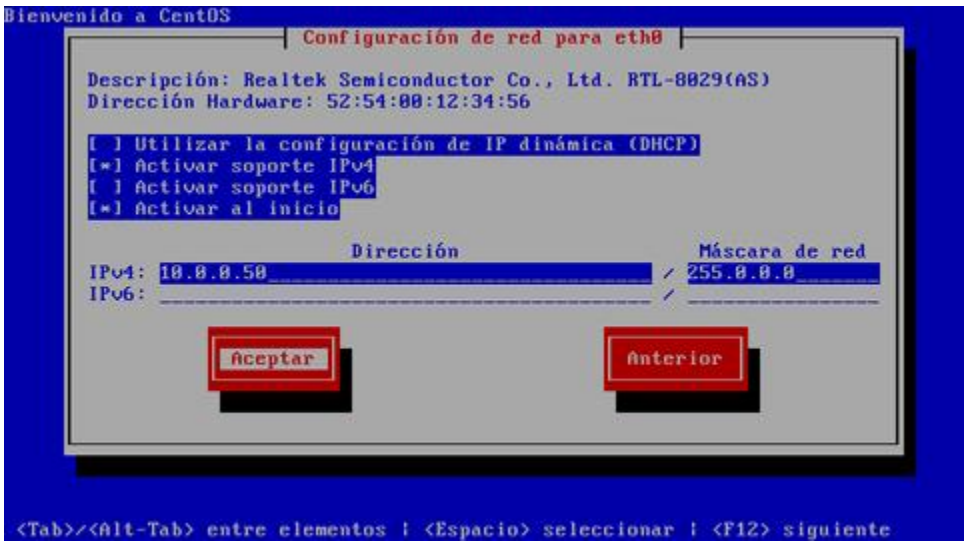
Si necesita pasar algún parámetro en particular al núcleo (kernel), como por ejemplo **acpi=off** o **nolapic** cuando hay problemas de compatibilidad de sustento físico, ingrese en el campo correspondiente aquello que sea necesario. **En la mayoría de los casos no necesitará ingresar parámetro alguno**.

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 ejecución 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.

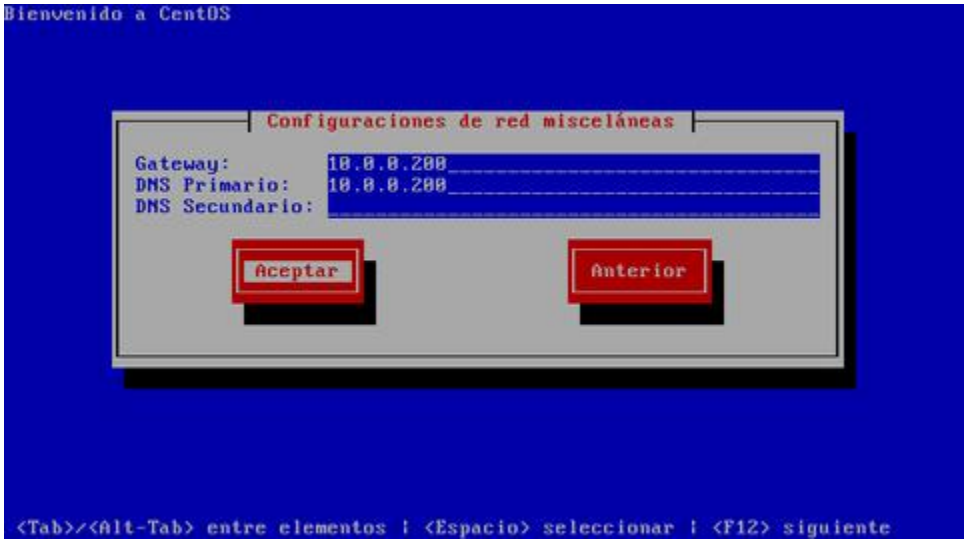
De haber otro sistema operativo instalado en el sistema, seleccione el que utilizará para iniciar de forma predeterminada. Si solo está instalando Linux, solo pulse la tecla **ENTER** para saltar a la siguiente pantalla.

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.

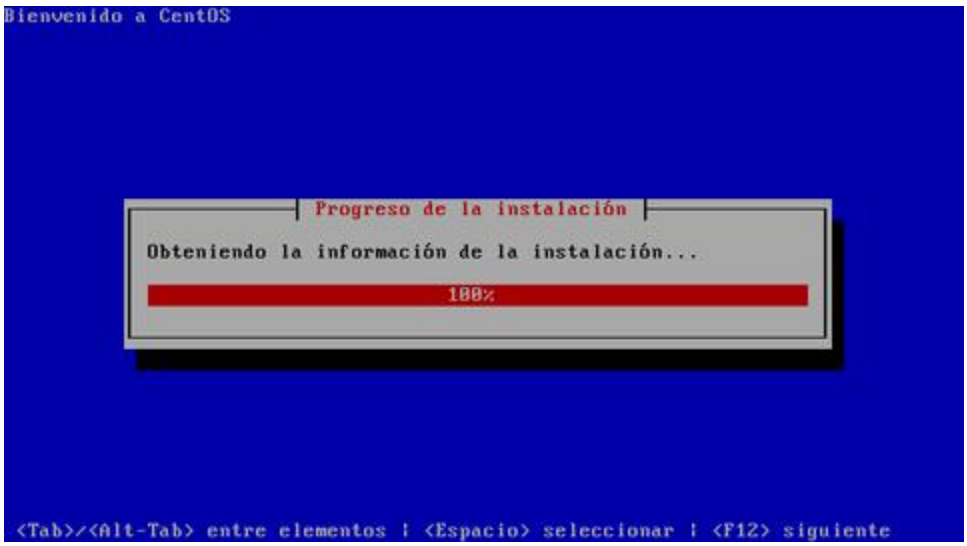


Asigne un nombre de anfitrión (HOSTNAME) para el sistema. Se recomienda que dicho nombre sea un **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) resuelto al menos en un DNS local. Si desconoce que dato ingresar, defina éste como **localhost.localdomain**. Al terminar, pulse la tecla **ENTER** para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

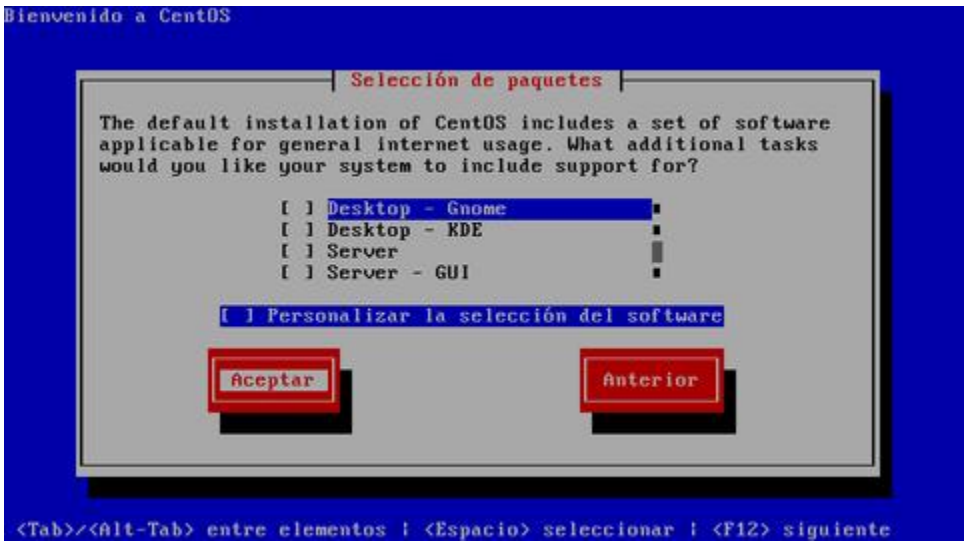
Seleccione la casilla **«System clock uses UTC»**, que significa que el reloj del sistema utilizará **UTC** (**T**iempo **U**niversal **C**oordinado), que es el sucesor de **GMT** (b>Greenwich **M**ean **T**ime, que significa Tiempo Promedio de Greenwich), y es la zona horaria de referencia respecto 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.



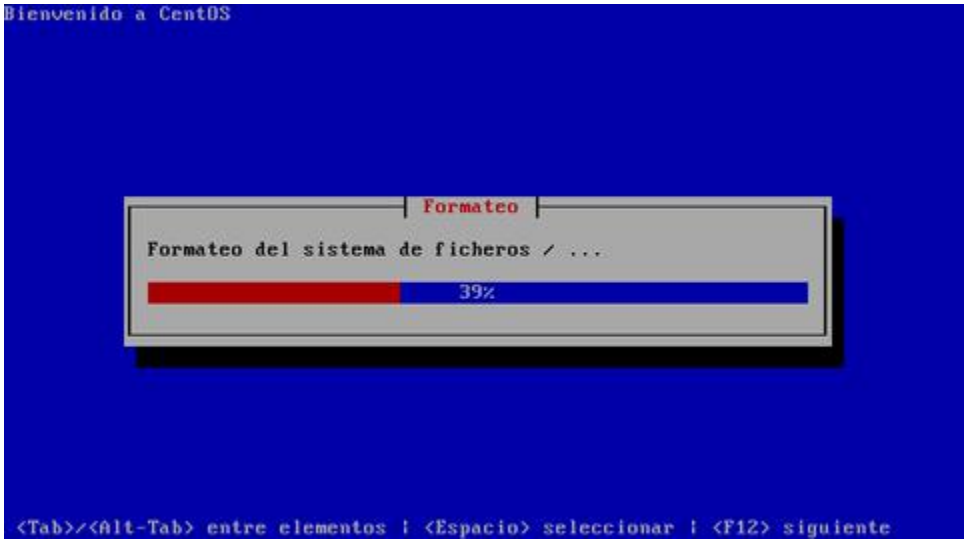
Realice una instalación con el mínimo de paquetes, desactivando todas las casillas de cada grupo de paquetes. El objeto de esto es solo instalar lo mínimo necesario para el funcionamiento del sistema operativo, y permitir instalar, posteriormente, **solo aquello que realmente se requiera** de acuerdo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

4. 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/*

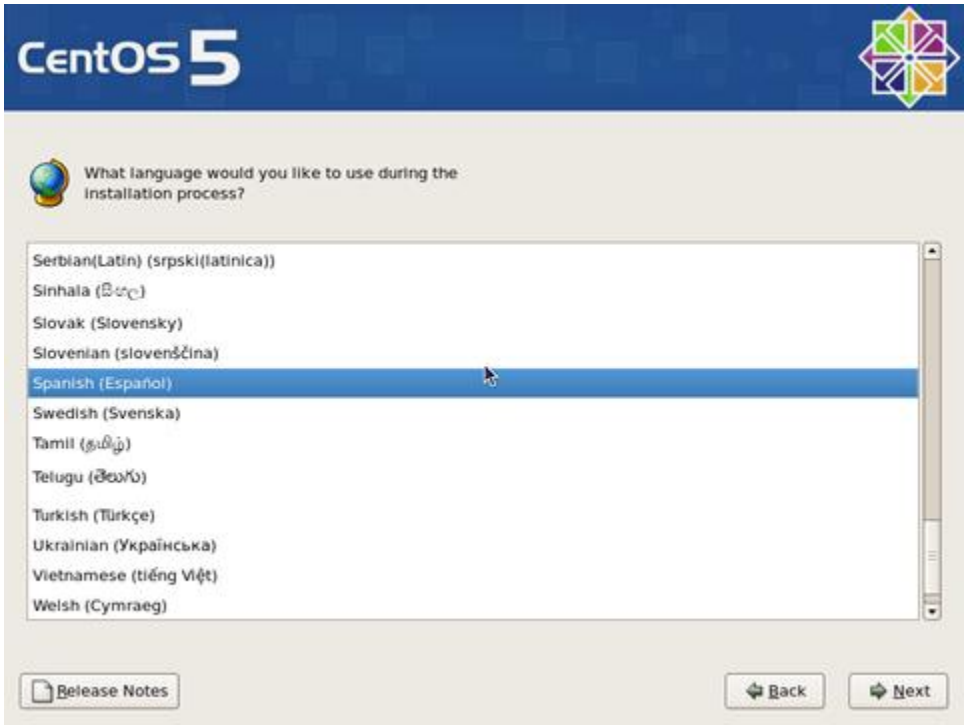
4.1. Procedimientos.

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.

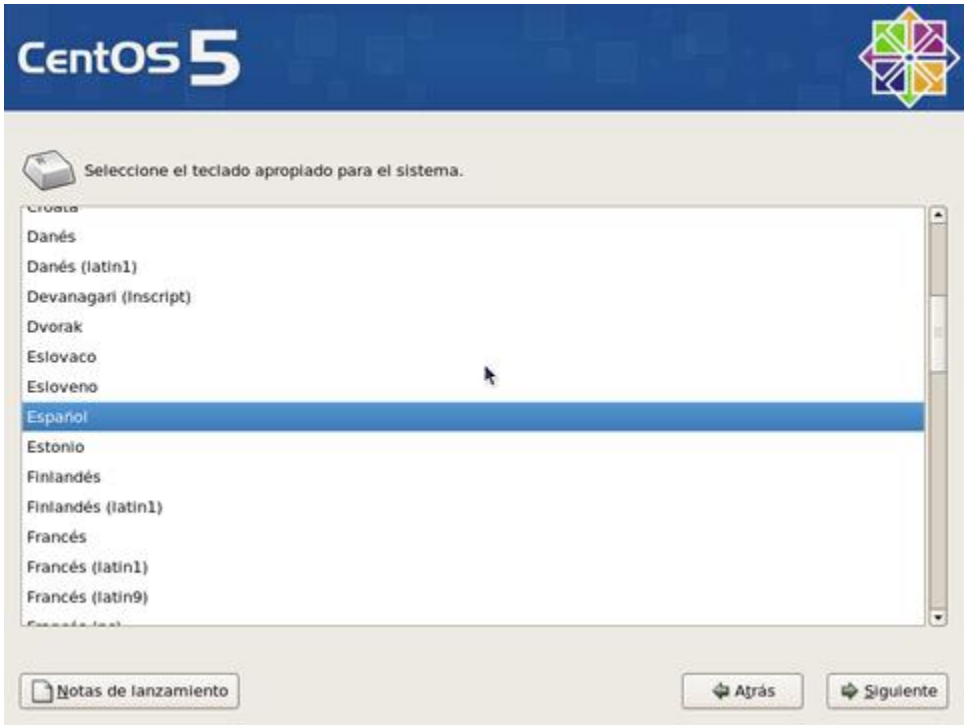
Si desea verificar la integridad del disco a partir del cual se realizará la instalación, seleccione **«OK»** y pulse la tecla **ENTER**, considere que esto puede demorar varios minutos. Si está seguro de que el disco o discos a partir de los cuales se realizará la instalación están en buen estado, seleccione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



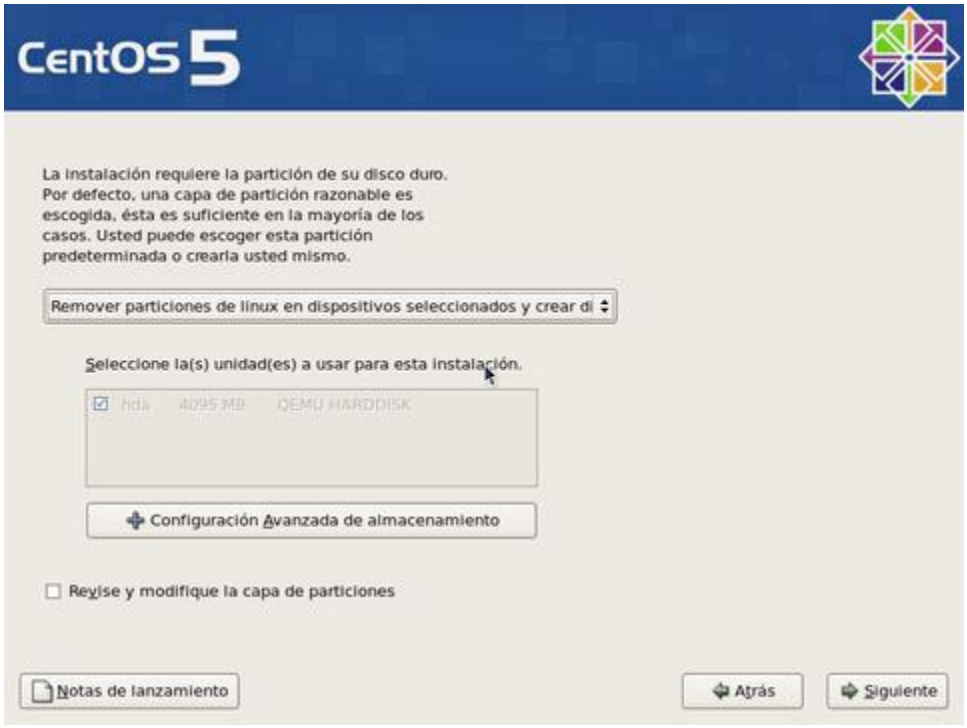
Seleccione el mapa de teclado que corresponda al dispositivo utilizado. El mapa **«Español»** o bien **«Latinoamericano»** de acuerdo a lo que corresponda. Al terminar, haga clic sobre el botón **«Siguiente»**.



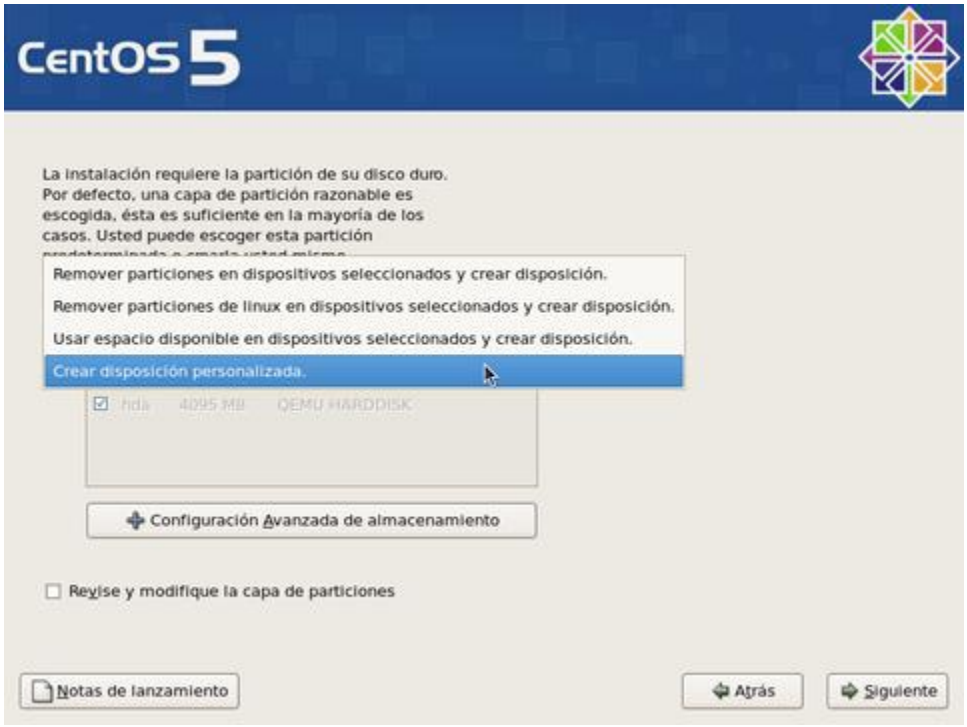
Salvo que exista una instalación previa que se desee actualizar (no recomendado), deje seleccionado **«Instalar CentOS»** y haga clic en el botón **«Siguiente»** a fin de realizar una instalación nueva.

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

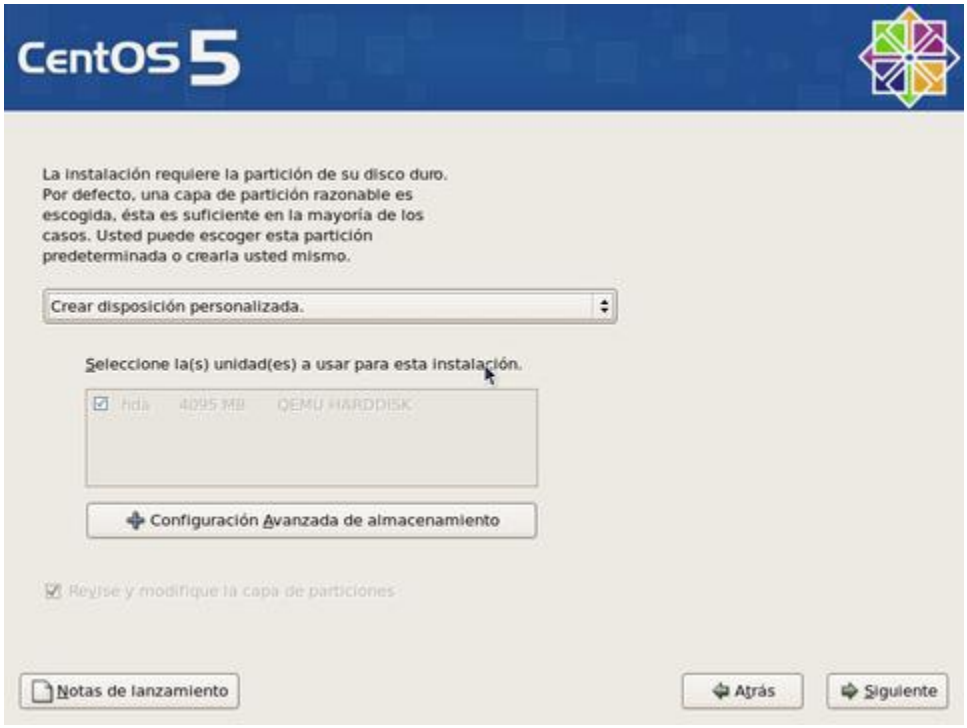
- «**Remover particiones en dispositivos seleccionados y crear disposición», lo cual eliminaría cualquier partición de cualquier otro sistema operativo presente**, y creará de forma automática las particiones necesarias.
- «**Remover particiones de linux en dispositivos seleccionados y crear disposición»,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



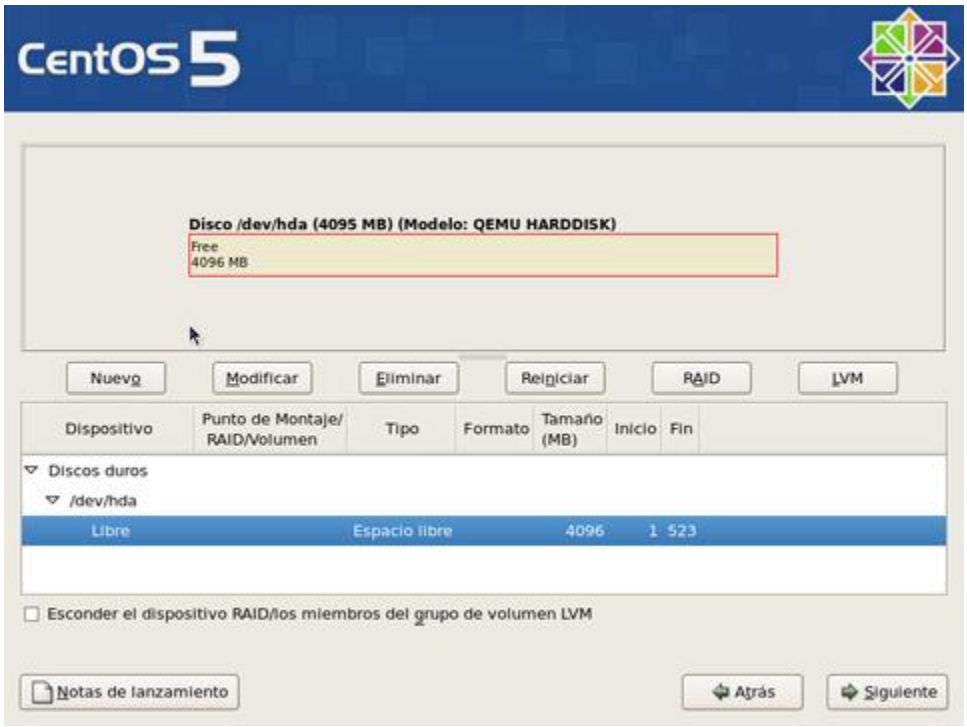
Conviene crear una disposición que permita un mayor control. Seleccione **«Crear disposición personalizada»**.



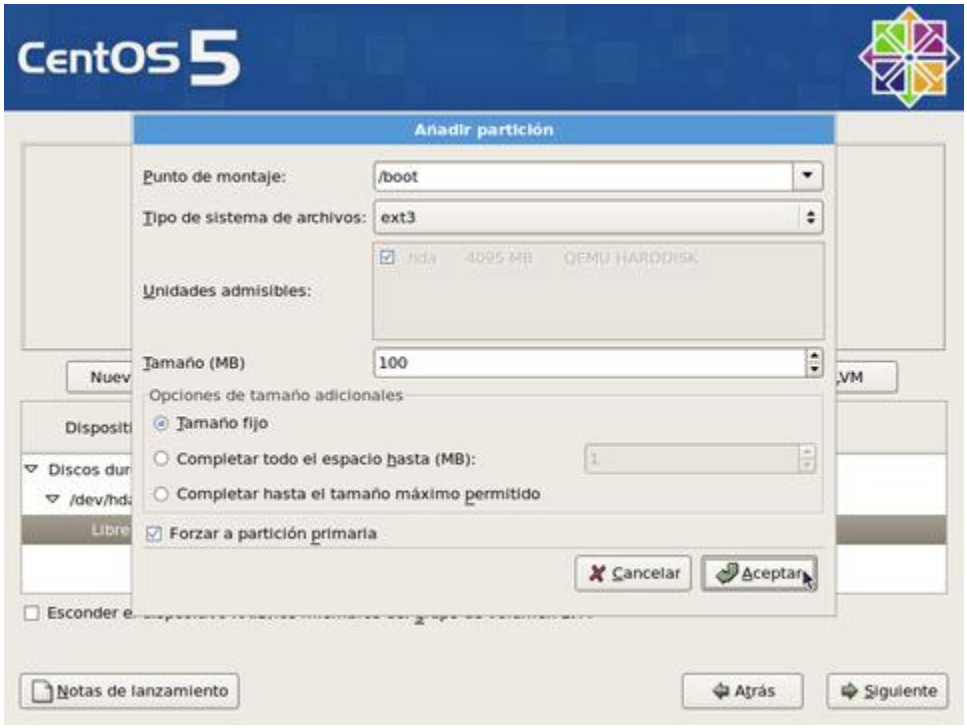
Una vez seleccionado **«Crear disposición personalizada»**, haga clic sobre el botón **«Siguiente»**.



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

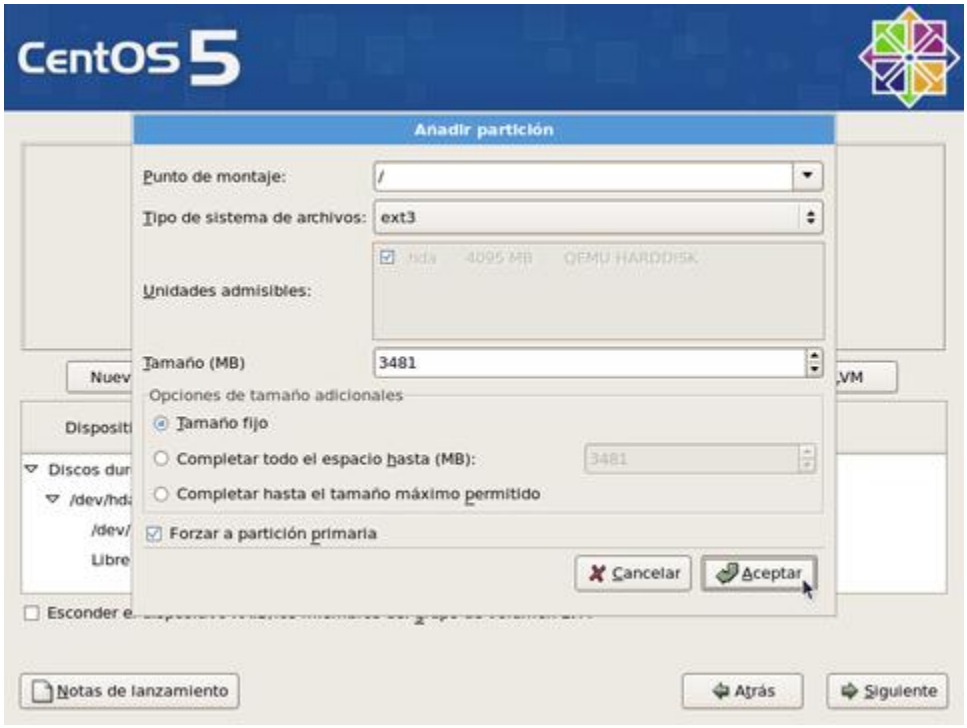


Asigne 100 MB a la partición /boot y defina ésta como partición primaria, siempre que la tabla de particiones lo permita.



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.

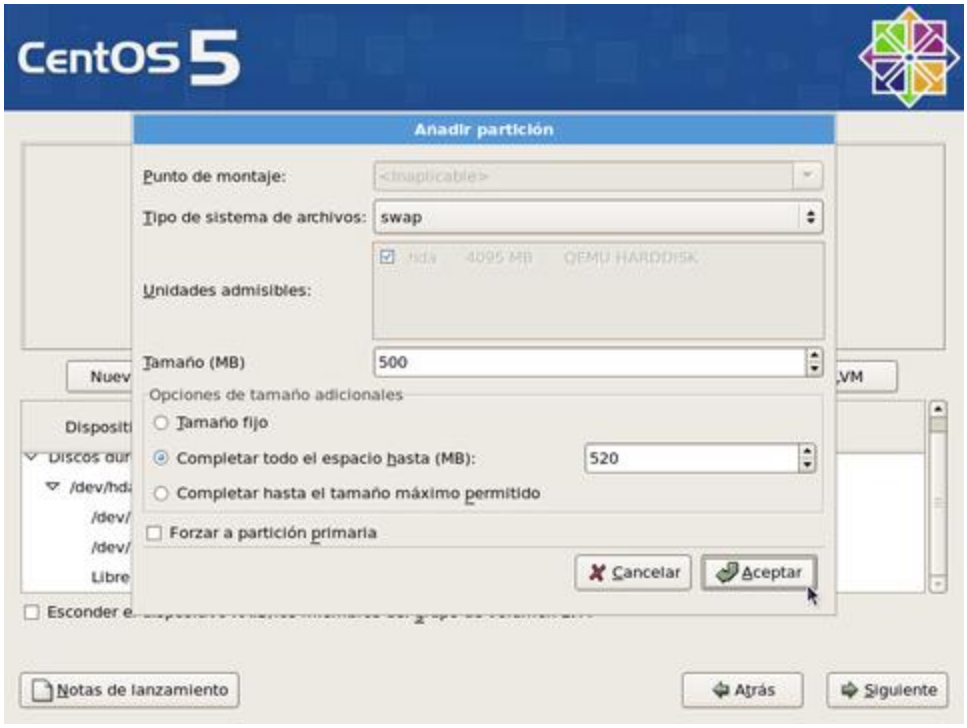


Si está conforme, haga clic otra vez en el botón **«Nuevo»** y proceda a crear la siguiente partición.

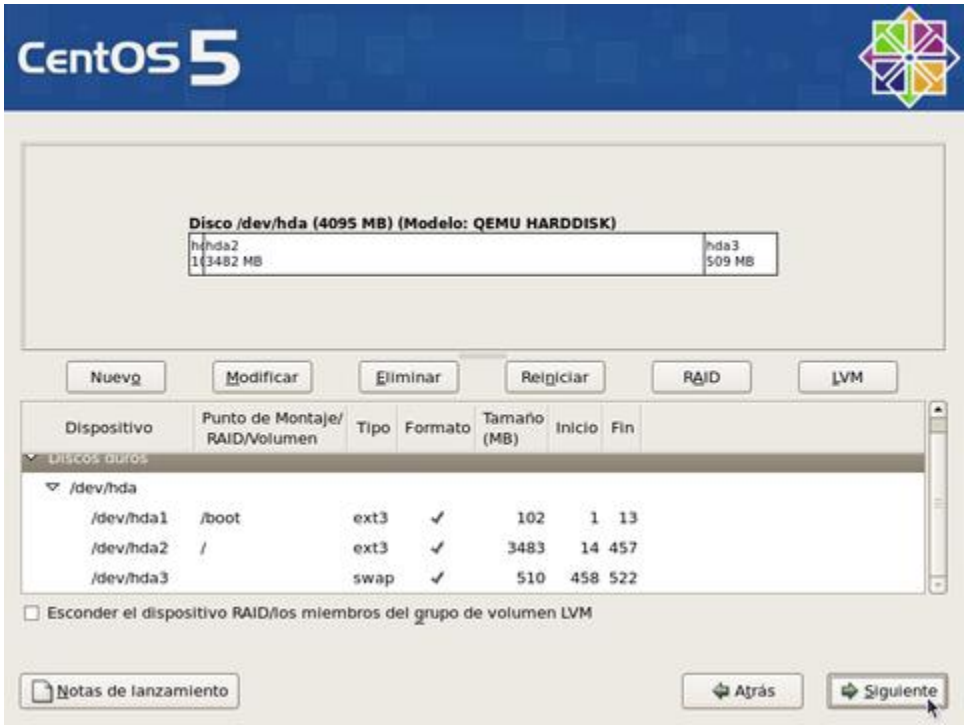
La partición para la memoria de intercambio no requiere punto de montaje. Seleccione en el campo de **«Tipo de sistema de archivos»** la opción **«swap»**, asigne el 200% de la memoria física (o cuanto basta para 2 GB). Por tratarse de la última partición de la tabla, es buena idea asignarle el espacio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

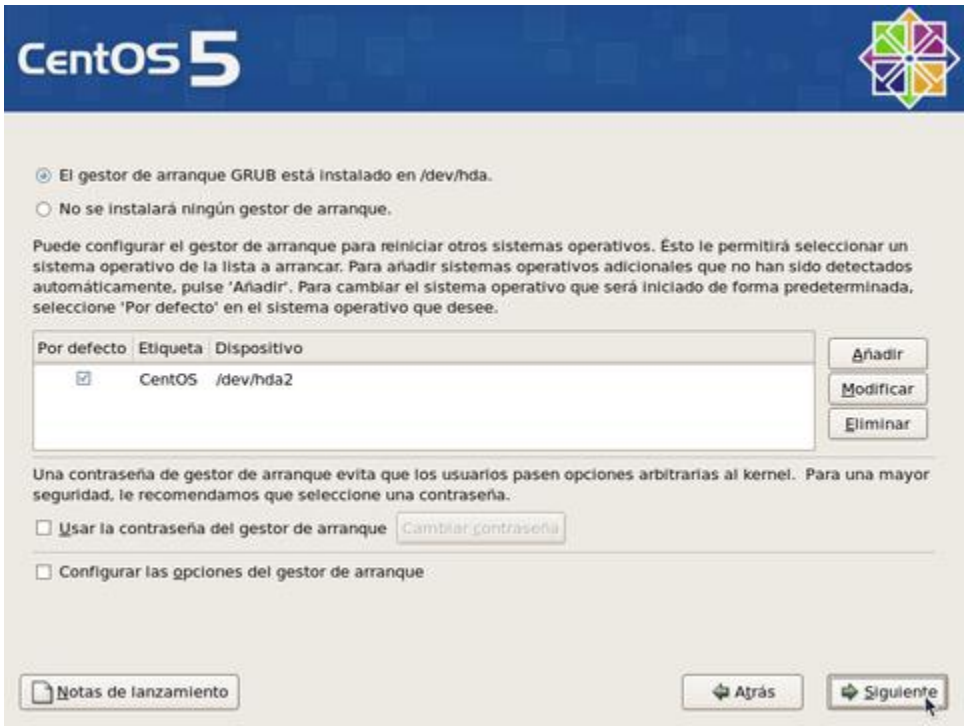
`/usr`	Requiere al menos 1.5 GB en instalaciones básicas. Debe considerarse el sustento lógico a utilizar a futuro. Para uso general, se recomiendan no menos de 5 GB y, de ser posible, considere un tamaño óptimo de hasta 8 GB en instalaciones promedio.
`/tmp`	Requiere al menos 350 MB y puede asignarse 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.



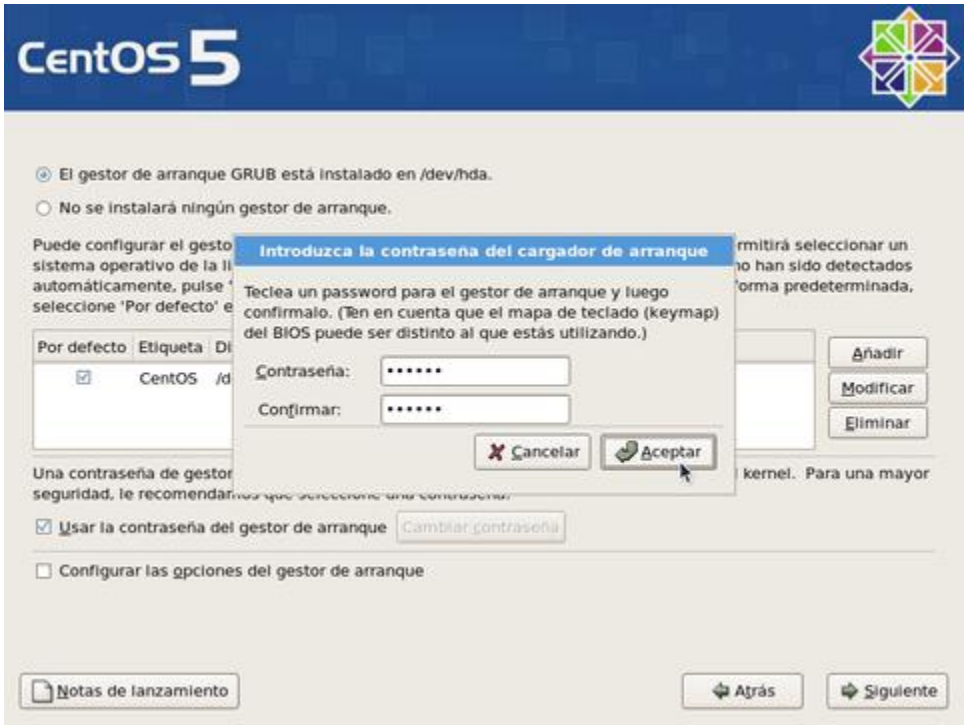
Si está conforme con la tabla de particiones creada, haga clic sobre el botón **«siguiente»** para pasar a la siguiente pantalla.



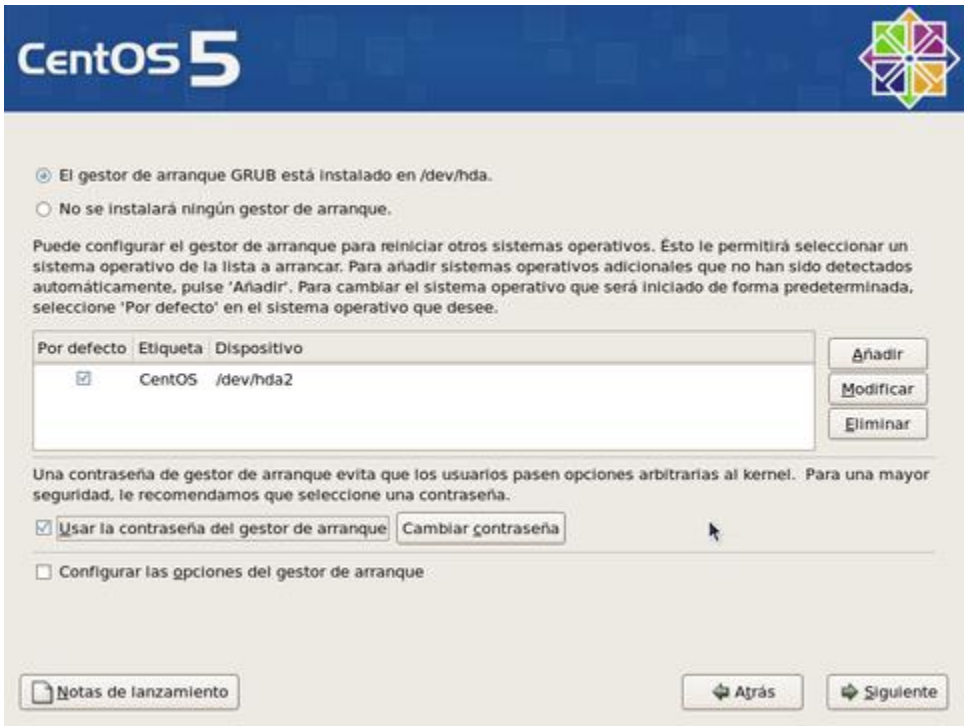
Ingresará a la configuración del gestor de arranque. Por motivos de seguridad, y principalmente con la finalidad de impedir que alguien sin autorización y con acceso físico al sistema pueda iniciar el sistema en nivel de ejecución 1, o cualquiera otro, haga clic en la casilla **«Usar la contraseña del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

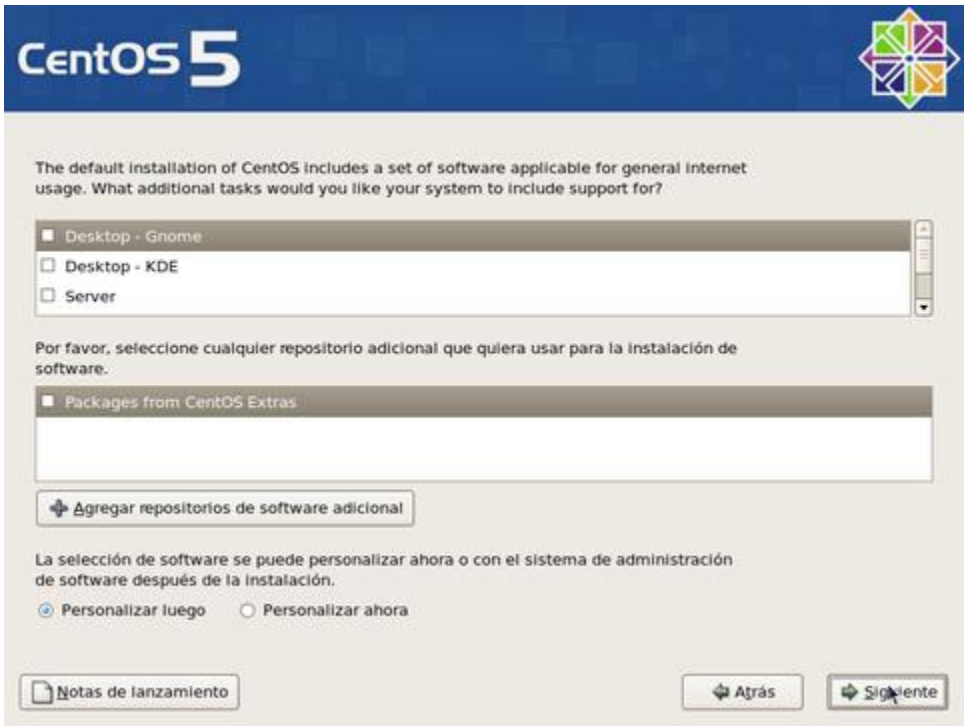
un **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) resuelto al menos en un DNS local. Defina, además, en esta misma pantalla, la dirección IP de la puerta de enlace y las direcciones IP de los servidores DNS de los que disponga. Si desconoce que dato ingresar, defina éste como **localhost.localdomain**. 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.

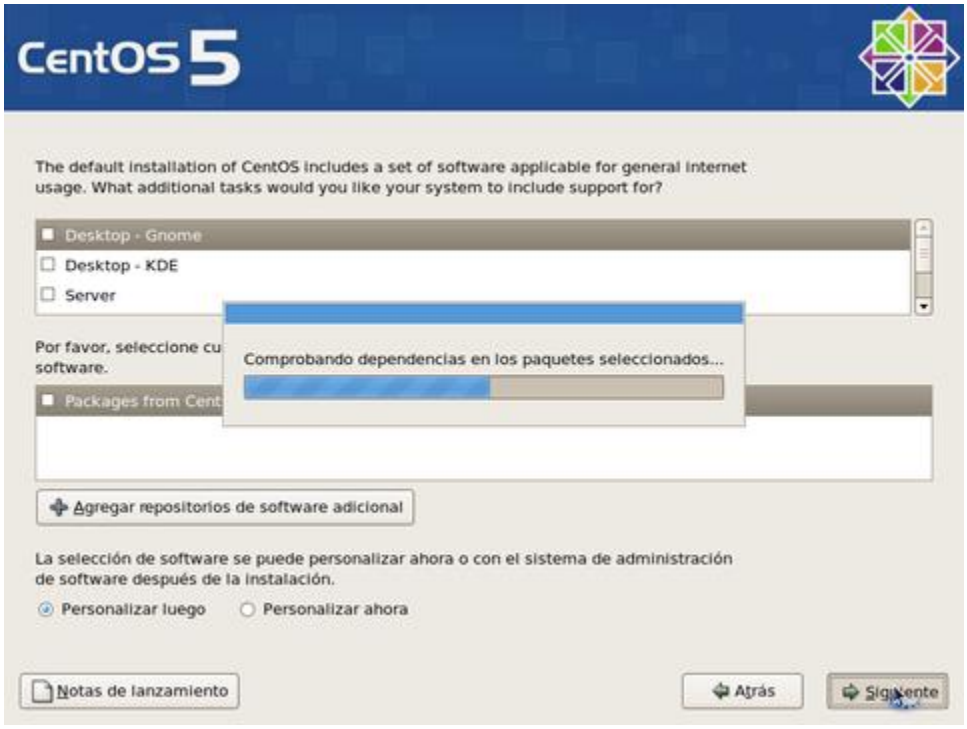
Asigne una clave de acceso al usuario **root**. Debe escribirla dos veces a fin de verificar que está coincide con lo que realmente se espera. Por razones de seguridad, se recomienda asignar una clave de acceso que evite utilizar palabras provenientes de cualquier diccionario, en cualquier idioma, así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

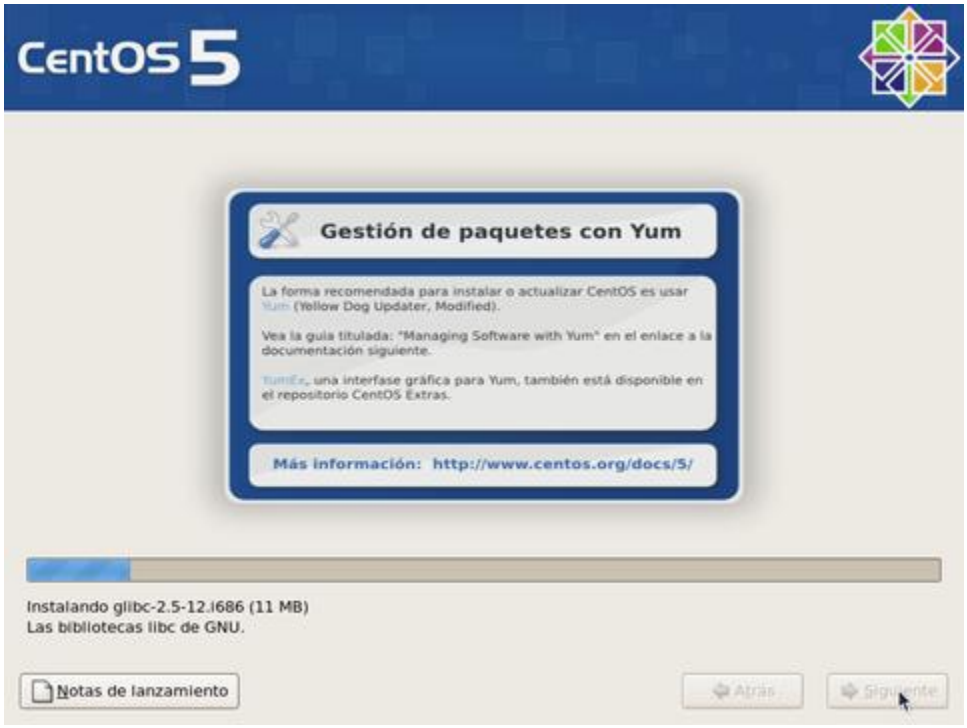
Si iniciará de forma automática el proceso de formato de las particiones que haya creado para instalar el sistema operativo. Dependiendo de la capacidad del disco duro, este proceso puede demorar algunos minutos.

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**».

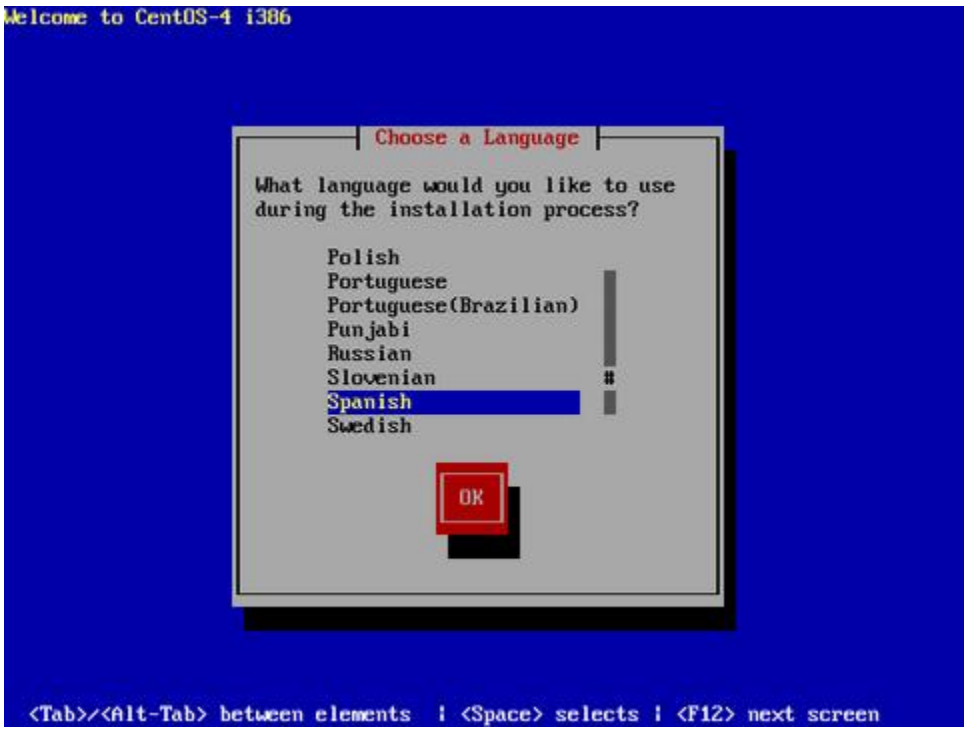
5. Cómo iniciar el modo de rescate en CentOS.

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

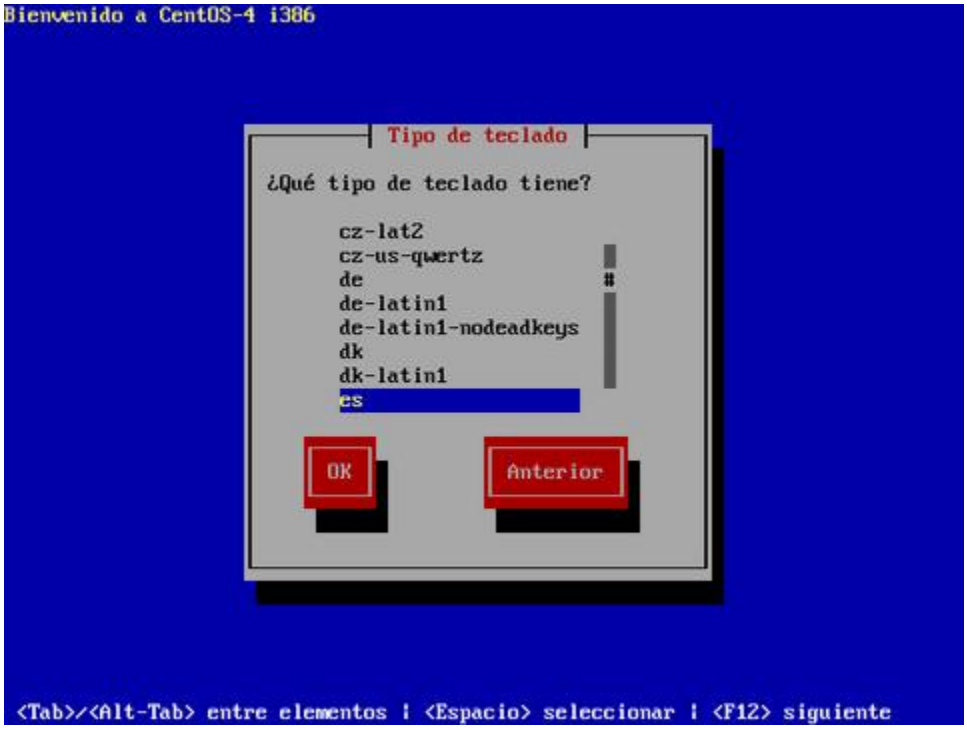
5.1. Procedimientos.

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.

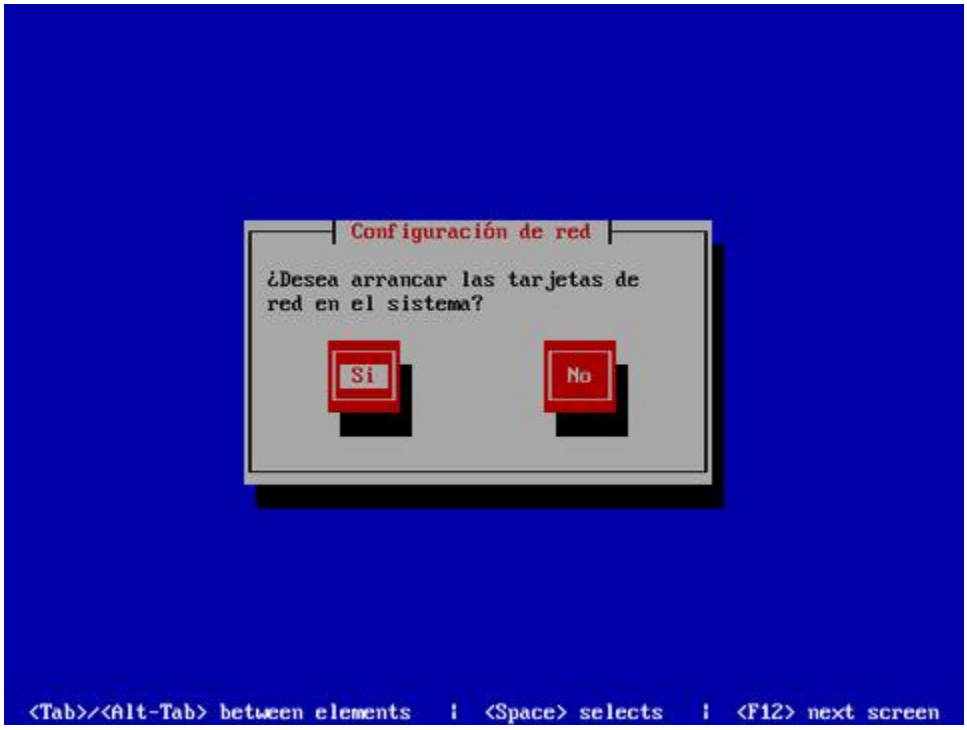
En cuanto inicie el programa, elija **«Spanish»** (español) como el idioma a utilizar.



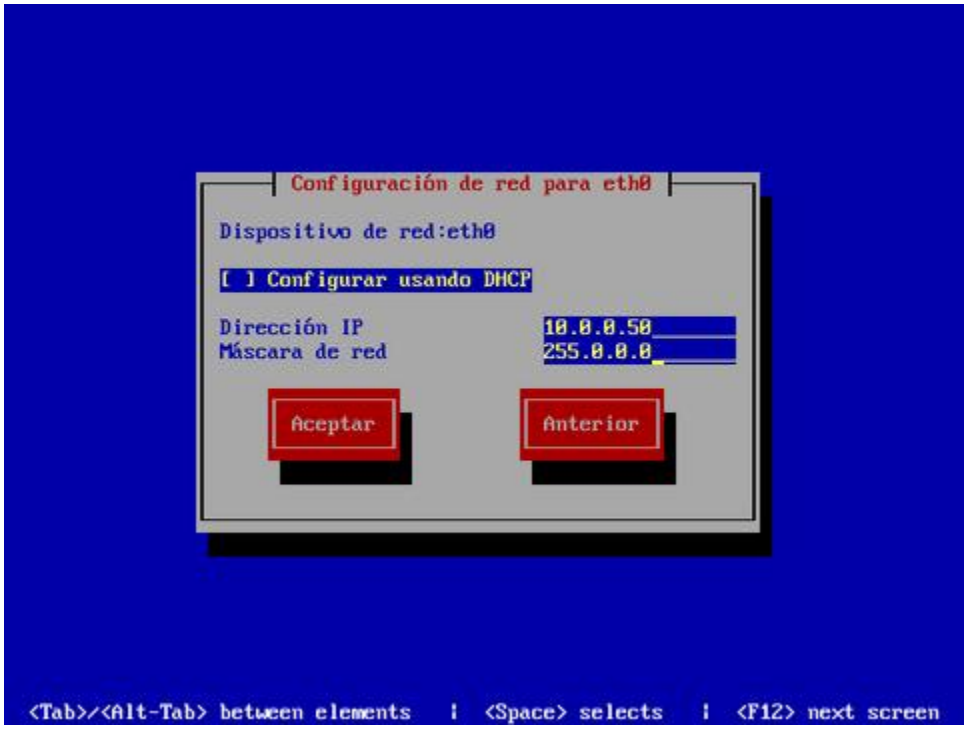
Seleccione el mapa de teclado que corresponda al dispositivo utilizado. El mapa **«es»** corresponde a la disposición del teclado Español España. El mapa **«latin-1»** corresponde a la disposición del teclado Español Latino Americano.



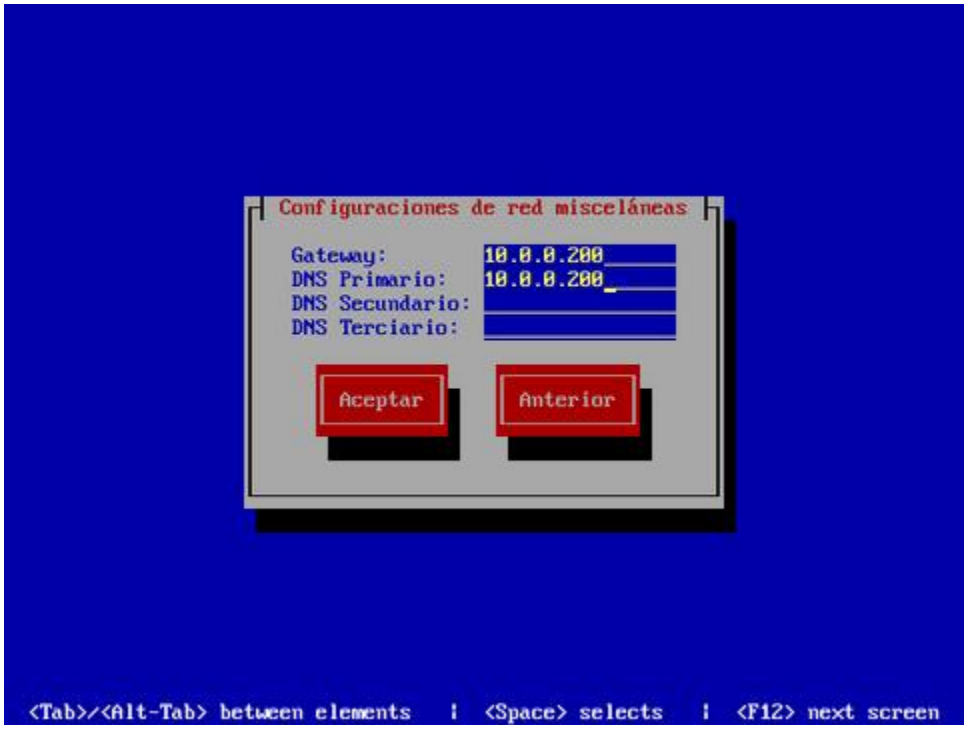
El programa preguntará si desea activar las tarjetas de red presentes en el sistema. Responda que **si**. Resulta muy conveniente, para algunas tareas de mantenimiento y reparaciones, contar con conectividad.



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.

6. Iniciando el sistema en nivel de ejecución 1 (nivel mono-usuario).

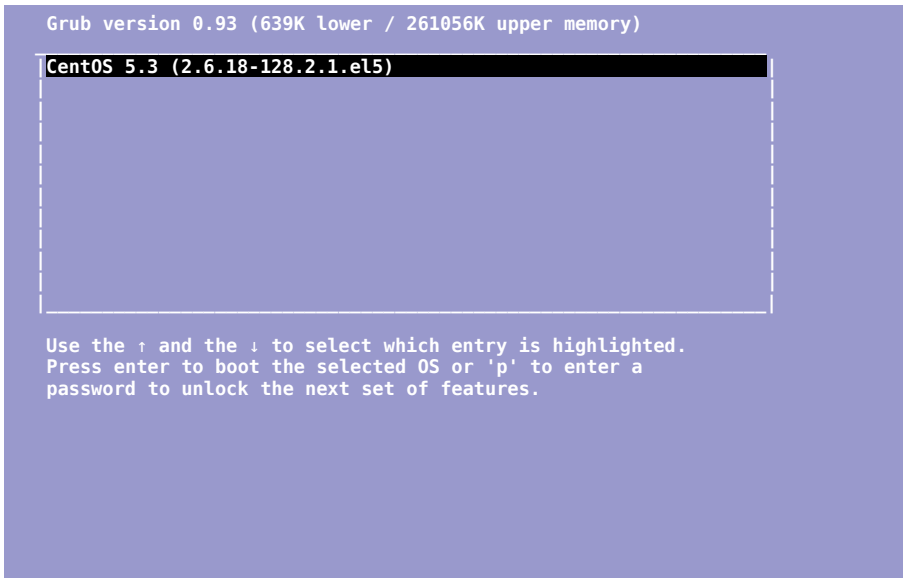
Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.org/

6.1. Introducción.

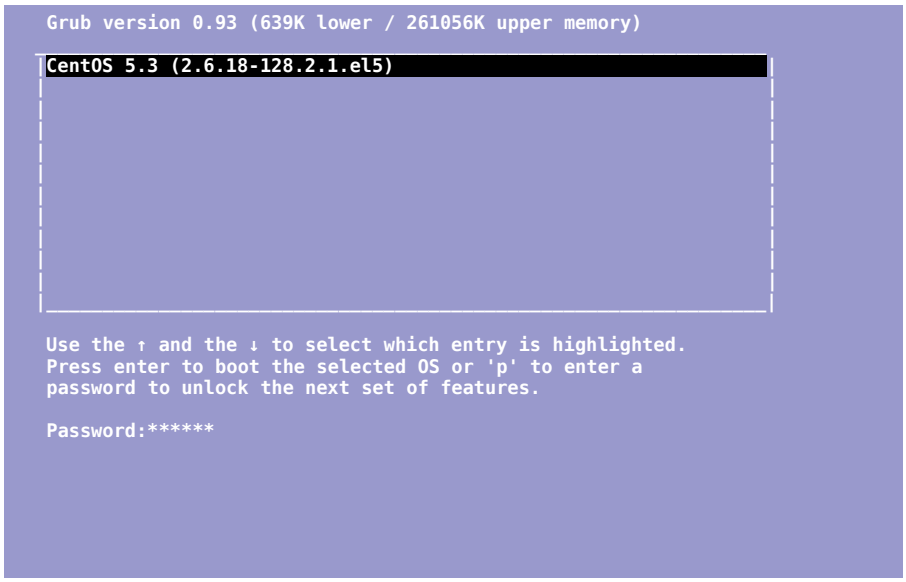
Existen situaciones en las cuales se puede requerir el inicio del sistema en nivel de ejecución 1 o nivel mono-usuario a fin de realizar tareas de mantenimiento o, en su defecto, reparaciones.

6.2. 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:

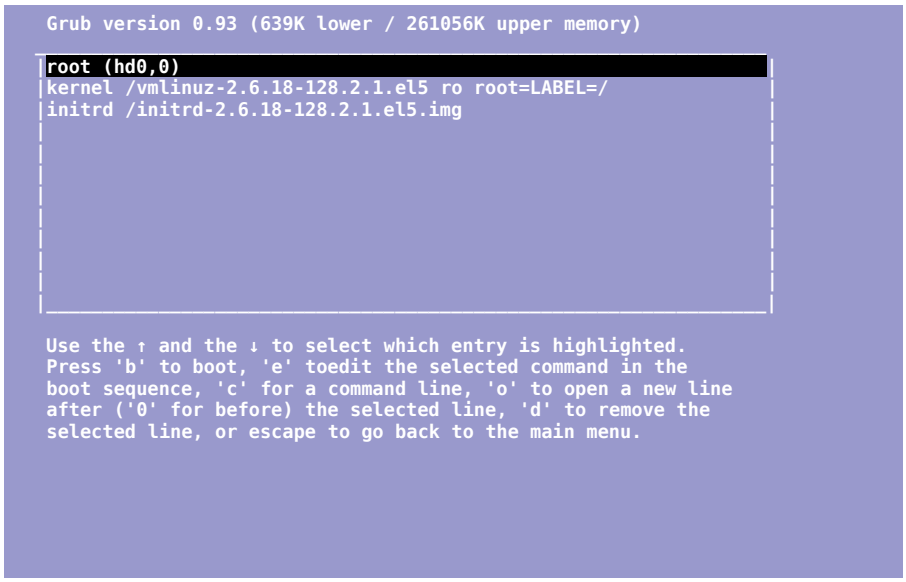


Pulse la tecla 'p' e ingrese la clave de acceso definida desde el programa de instalación del sistema operativo:

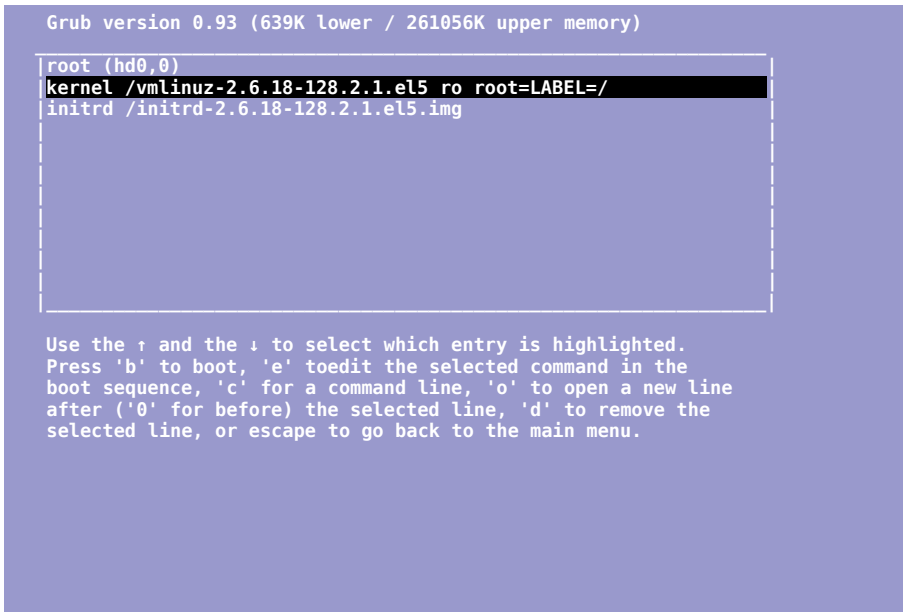


El texto de opciones cambiará después de ingresar la clave de acceso correcta:

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

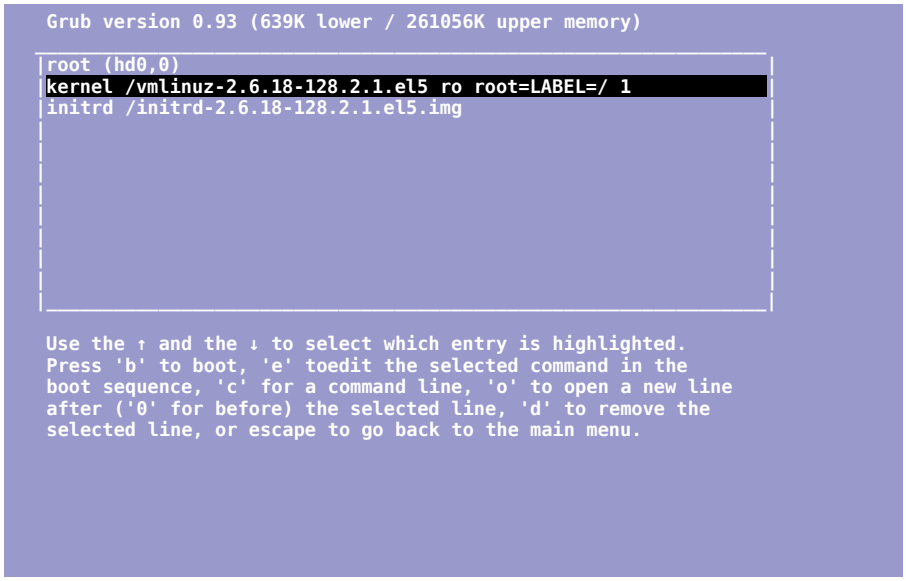


Seleccione la línea referente al núcleo y vuelva a pulsar la tecla 'e' a fin de modificar dicha línea:



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 ejecución 1:



7. Cómo compilar el núcleo (kernel) de GNU/Linux en CentOS.

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

7.1. Introducción.

Una de las grandes ventajas de que el núcleo (*kernel*) **GNU/Linux** sea equipamiento lógico libre (*Software Libre*) es el poder descargar el código fuente del núcleo, configurar éste para compilar específicamente con opciones adecuadas a necesidades particulares o con controladores específicos para un sustento físico (*hardware*) en particular, compilarlo y obtener como resultado mejoras en el desempeño.

La gran variedad de distribuciones de **GNU/Linux** instalan un núcleo (*kernel*) que fue configurado y compilado con opciones genéricas y que permiten utilizar éste en una gran variedad de dispositivos y computadoras. Esto facilita la vida a los desarrolladores y empaquetadores que trabajan para cada distribución pues de esta forma con cuatro o cinco versiones del paquete de núcleo abarcan la mayoría de los sustentos físicos en el mercado. Ésto elimina la necesidad de los usuarios por compilar el núcleo.

Por mencionar un ejemplo, el paquete del núcleo de **CentOS 5** y **Red Hat Enteprise Linux 5** que se distribuye para arquitecturas **i686** incluye opciones y optimizaciones genéricas que permiten utilizar un mismo paquete **RPM** del núcleo para una amplia variedad de sistemas. Éste incluye el soporte para ser utilizado con microprocesadores como **Pentium Pro**, **Pentium II**, **Pentium III**, **Pentium 4**, **Pentium M**, **Celeron**, **Athlon**, **Duron**, **Cyrix i686**, etc. Evidentemente este soporte genérico impide poder explotar todo el potencial e instrucciones de un modelo de microprocesador en particular.

7.1.1. Un ejemplo del porque conviene recompilar el núcleo.

Si, por ejemplo, se dispone una computadora portátil (*Laptop*) **Compaq Armada M300** con microprocesador **Pentium III** (**Coppermine**) de 500 MHz, con **320 MB RAM**, circuitos integrados **Intel PIIX4**, tarjeta de audio **ESS Technology ES1978**, tarjeta de red **Ethernet Pro 100** y otros ciertos dispositivos en particular, el núcleo genérico incluido en la instalación funcionará bien, pero se tendrá un desempeño inferior. Configurar y compilar el núcleo específicamente para las características de este modelo de computadora portátil, excluyendo de la configuración funciones que jamás se utilizarán en este sistema, mejorará su desempeño significativamente.

En sistemas caseros y computadoras portátiles con cierta antigüedad, pueden excluirse funciones como el soporte para más de 4 GB de RAM, soporte genérico para arquitectura **ix86**, soporte para otros modelos de computadoras portátiles, soporte para más de un microprocesador, soporte para **IPv6** y otras opciones que solo serían útiles en otro tipo de sistemas como servidores.

Puede agregarse soporte para más periféricos, como por ejemplo más dispositivos **USB**, y compilar algunos controladores (cómo el soporte para **LVM**) dentro del núcleo en lugar de hacerlo como módulos a fin de mejorar el desempeño durante el arranque del sistema.

En un servidor se puede mejorar mucho el desempeño configurando y compilando exclusivamente las opciones y módulos específicos para la configuración de sustento físico (*hardware*) y funciones requeridas para los servicios a brindar.

7.2. Procedimientos.

7.2.1. Determinar el sustento físico y controladores.

Este procedimiento es complicado e implica contar con un cierta experiencia y conocimientos generales acerca del sustento físico (*hardware*).

7.2.1.1. Módulos utilizados por el sistema.

Utilizando el mandato **lsmod** es posible determinar que controladores se están utilizando en el sistema. Esta lista de controladores debe tomarse muy en cuenta a fin de evitar excluir alguno de éstos. Utilice el mandato de la siguiente forma:

```
/sbin/lsmod
```

Lo anterior puede devolver una salida similar a la siguiente, que dependerá del sustento físico del sistema:

```
Module                  Size  Used by
nls_utf8                1888  1
vfat                   12768  1
fat                    50268  1 vfat
sg                     35536  0
sd_mod                 28112  2
usb_storage            46848  1
scsi_mod              148044  3 sg,sd_mod,usb_storage
i2c_dev                 7492  0
dm_multipath           18856  0
backlight               5220  0
snd_es1968             28192  1
gameport               13608  1 snd_es1968
snd_ac97_codec         97760  1 snd_es1968
ac97_bus                1728  1 snd_ac97_codec
snd_seq_dummy           3556  0
snd_seq_oss            30976  0
snd_seq_midi_event      7008  1 snd_seq_oss
snd_seq                47856  5 snd_seq_dummy,snd_seq_oss,snd_seq_midi_event
snd_pcm_oss            41184  0
snd_mixer_oss          16192  1 snd_pcm_oss
battery                12932  0
ac                      5796  0
snd_pcm                72168  3 snd_es1968,snd_ac97_codec,snd_pcm_oss
button                  7984  0
parport_pc             27524  0
snd_timer              22148  2 snd_seq,snd_pcm
snd_page_alloc         10216  2 snd_es1968,snd_pcm
parport                35400  1 parport_pc
snd_mpu401_uart         7872  1 snd_es1968
```

```
snd_rawmidi            23392  1 snd_mpu401_uart
joydev                 11232  0
snd_seq_device          8044  4 snd_seq_dummy,snd_seq_oss,snd_seq,snd_rawmidi
snd                    52068  13 snd_es1968,snd_ac97_codec,snd_seq_oss,snd_seq,
                              snd_pcm_oss,snd_mixer_oss,snd_pcm,snd_timer,
                              snd_mpu401_uart,snd_rawmidi,snd_seq_device
e100                   34220  0
soundcore               7264  1 snd
mii                     5440  1 e100
i2c_piix4               8780  0
pcspkr                  2624  0
i2c_core               24432  2 i2c_dev,i2c_piix4
serio_raw               6500  0
floppy                 55652  0
dm_snapshot            17472  0
dm_zero                 1920  0
dm_mirror              25568  0
ext3                  132488  2
jbd                    42100  1 ext3
uhci_hcd               23696  0
ohci_hcd               22916  0
ehci_hcd               33740  0
```

7.2.1.2. Tipo de microprocesador.

La información del microprocesador se puede consultar leyendo el contenido del fichero virtual **/proc/cpuinfo** utilizando el mandato **less** del siguiente modo:

```
less /proc/cpuinfo
```

Lo anterior puede devolver una salida similar a la siguiente, que dependerá del tipo de microprocesador del que se disponga:

```
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 8
model name      : Pentium III (Coppermine)
stepping        : 3
cpu MHz         : 498.164
cache size      : 256 KB
fdiv_bug        : no
hlt_bug         : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level     : 2
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 sep
mtrr pge mca cmov pat pse36 mmx fxsr sse
bogomips        : 996.86
clflush size    : 32
```

7.2.1.3. Dispositivos PCI.

El mandato **lspci** permite determinar los dispositivos **PCI** (**P**eripheral **C**omponent **I**nterconnect o Interconexión de Componentes Periféricos) presentes en el sistema.

```
/sbin/lspci
```

Lo anterior puede devolver una salida similar a la siguiente, que dependerá de los dispositivos **PCI** de los que que se disponga:

```
00:00.0 Host bridge: Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX Host bridge
(AGP disabled) (rev 03)
00:04.0 CardBus bridge: Texas Instruments PCI1211
00:05.0 VGA compatible controller: ATI Technologies Inc 3D Rage LT Pro (rev dc)
00:07.0 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ISA (rev 02)
00:07.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
00:07.2 USB Controller: Intel Corporation 82371AB/EB/MB PIIX4 USB (rev 01)
00:07.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 03)
00:08.0 Multimedia audio controller: ESS Technology ES1978 Maestro 2E (rev 10)
00:09.0 Ethernet controller: Intel Corporation 82557/8/9/0/1 Ethernet Pro 100 (rev
09)
00:09.1 Serial controller: Agere Systems LT WinModem
01:00.0 Ethernet controller: 3Com Corporation 3CRPAG175 Wireless PC Card (rev 01)
```

7.2.1.4. Dispositivos USB.

De manera similar al mandato **lspci**, el mandato **lsusb** permite determinar los dispositivos **USB** (**U**niversal **S**erial **B**us o Transporte Universal en Serie) presentes en el sistema. Conecte a las ranuras **USB** del sistema los dispositivos **USB** más frecuentemente utilizados y utilice el mandato **lsusb**.

```
/sbin/lsusb
```

Lo anterior puede devolver una salida similar a la siguiente, que dependerá del tipo de dispositivos **USB** de los que se disponga:

```
Bus 001 Device 005: ID 0457:0151 Silicon Integrated Systems Corp. Super Flash
1GB / GXT  64MB Flash Drive
Bus 001 Device 004: ID 05ac:0201 Apple, Inc. USB Keyboard [Alps or Logitech,
M2452]
Bus 001 Device 003: ID 05ac:1001 Apple, Inc. Keyboard Hub [ALPS]
Bus 001 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
```

7.2.2. Instalación el equipamiento lógico necesario.

Para **CentOS**, a fin de disponer de los paquetes **RPM** de fuentes, se debe configurar primero los depósitos **yum** de los paquetes **RPM** fuentes (.src.rpm) como el **nuevo** fichero **/etc/yum.repos.d/CentOS-Sources.repo**, con el siguiente contenido:

```
#source packages
[sources]
name=CentOS-$releasever - Sources
baseurl=http://mirror.centos.org/centos/$releasever/os/SRPMS/
gpgcheck=1
enabled=1
gpgkey=http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-5
#source packages
[sources-updates]
name=CentOS-$releasever - Sources Updates
baseurl=http://mirror.centos.org/centos/5/updates/SRPMS/
gpgcheck=1
enabled=1
```

```
gpgkey=http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-5
```

Al terminar se continúa con la instalación de los paquetes **RPM** binarios de el compilador **gcc**, cabeceras de desarrollo para el lenguaje de programación **C**, paquete de desarrollo de **ncurses**, para construir la herramienta de configuración del núcleo, y el paquete para creación de paquetería **RPM**:

```
yum -y install gcc glibc-devel ncurses-devel rpm-build
```

Si se va a utilizar la herramienta de configuración gráficos, hay que instalar además los paquetes **qt-devel** y **gcc-c++** del siguiente modo:

```
yum -y install qt-devel gcc-c++
```

7.2.3. Obtener el código fuente del núcleo.

7.2.3.1. A partir de los depósitos de la distribución utilizada.

Utilizar el paquete fuente de la distribución de **GNU/Linux** utilizada garantiza que se utilizará la misma versión oficial de núcleo para producción del distribuidor, la cual seguramente incluye parches específicos para funcionar con la instalación de esa distribución de **GNU/Linux**. Esto garantiza que se mantendrá la compatibilidad de los **API** (**A**pplication **P**rogramming **I**nterface o Interfaz de Programación de Aplicaciones) requeridos por aplicaciones de terceros.

Primero se instala el paquete **yum-utils** de la siguiente forma:

```
yum -y install yum-utils
```

El paquete **yum-utils** incluye la herramienta **yumdownloader**, misma que se utilizará para descargar el paquete fuente del paquete **RPM** del kernel, del siguiente modo:

```
yumdownloader --source kernel
```

Suponiendo que se tiene instalado el paquete del núcleo denominado **kernel-2.6.18-92.1.6.el5**, lo anterior descargara desde los depósitos de equipamiento lógico en Internet el paquete **kernel-2.6.18-92.1.6.el5.src.rpm** dentro del directorio de trabajo actual.

Se procede a instalar el paquete fuente **kernel-2.6.18-92.1.6.el5.src.rpm** de la siguiente forma:

```
rpm -ivh kernel-*.src.rpm
```

Esto instalará los fuentes y parches para el núcleo en el directorio **/usr/src/redhat/SOURCES/** y el fichero de especificación para construir el paquete binario **RPM** como **/usr/src/redhat/SPECS/kernel-2.6.spec**.

Para poder utilizar el código fuente, hay que descomprimir y aplicar los parches incluidos por el distribuidor. Esto se consigue utilizando el mandato **rpmbuild** con las opciones -**bp** y **--target=[arquitectura]**, donde **[arquitectura]**representa la arquitectura genérica del microprocesador. En el caso de **CentOS 5**, están disponibles las configuraciones genéricas para

i586, **i686**, **x86_64**, **ia64**, **ppc**, **ppc64**, **s390** y **s390x**, y las variantes **i686-PAE**, para equipos , **i686-xen**, **ia64-xen** y **x86_64-xen**, para utilizar las funciones de **Xen** que permiten utilizar paravirtualización.

Las opciones **-bp** inician parcialmente el la construcción del paquete (*build*) pero solo hasta la sección **%prep** (preparativos) del fichero de especificación, lo que significa que se descomprimirá el fuente del núcleo y se aplicarán los parches.

Se debe acceder al directorio **/usr/src/redhat/SPECS/**.

```
cd /usr/src/redhat/SPECS/
```

Posteriormente se procede a descomprimir fuentes y aplicar parches. La opción **--target=i686** se utilizará en ejemplo a continuación para que se instale un fichero previamente configurado con **opciones genéricas** para la arquitectura **i686**.

```
rpmbuild -bp --target=i686 kernel-2.6.spec
```

Considerando en el ejemplo que se instaló el paquete fuente **RPM kernel-2.6.18-92.1.6.el5.src.rpm**, solo resta es acceder al directorio **/usr/src/redhat/BUILD/kernel-2.6.18/linux-2.6.18.i686/** para configurar las opciones que se utilizarán.

```
cd ../BUILD/kernel-2.6.18/linux-2.6.18.i686/
```

Dentro del paquete **RPM** se incluyen varios ficheros con configuraciones genéricas de acuerdo a la arquitectura, los cuales se instalan dentro del directorio **/usr/src/redhat/SOURCES/**. Uno de estos ficheros se selecciona y copia automáticamente dentro del directorio **/usr/src/redhat/BUILD/kernel-2.6.18/linux-2.6.18.i686/** cuando se define la arquitectura con la opción **--target** del mandato **rpmbuild**.

kernel-2.6.18-i586.config	Configuración genérica para arquitectura **i586** (Pentium, Pentium MMX, AMD K5, AMD K6, AMD K6 II, AMD K6 III).
kernel-2.6.18-i686.config	Configuración genérica para arquitectura **i686** (Pentium Pro, Pentium II, Pentium III, Pentium 4, Pentium M, Xeon, Celeron, AMD K7, AMD Athlon XP, AMD Duron).
kernel-2.6.18-i686-debug.config	Configuración genérica para arquitectura **i686**, con opciones de depuración. Solo recomendado para desarrolladores y escenarios donde se requiere diagnóstico.
kernel-2.6.18-i686-PAE.config	Configuración genérica para arquitectura **i686**, con soporte **PAE** (**P**hysical **A**ddress **E**xtension) que añade capacidades para utilizar mayor espacio de intercambio (*swapspace*). Utilizado en sistemas con más de 4 GB de RAM.
kernel-2.6.18-i686-xen.config	Configuración genérica para arquitectura **ia64** (Intel Itanium), con soporte para Xen. Permite utilizar paravirtualización a través de Xen.
kernel-2.6.18-ia64.config	Configuración genérica para arquitectura **ia64**.
kernel-2.6.18-ia64-debug.config	Configuración genérica para arquitectura **ia64**, con opciones de depuración. Solo recomendado para desarrolladores y escenarios donde se requiere diagnóstico.
kernel-2.6.18-ia64-xen.config	Configuración genérica para arquitectura **ia64**, con soporte para Xen. Permite utilizar paravirtualización a través de Xen.

kernel-2.6.18-ppc64.config	Configuración genérica para arquitectura **PPC** de 64 bit (G5).
kernel-2.6.18-ppc64-debug.config	Configuración genérica para arquitectura **PPC** de 64 bit, con opciones de depuración. Solo recomendado para desarrolladores y escenarios donde se requiere diagnóstico.
kernel-2.6.18-ppc.config	Configuración genérica para arquitectura **PPC** de 32 bit (G3 y G4).
kernel-2.6.18-ppc-smp.config	Configuración genérica para arquitectura **PPC** de 32 bit, con soporte de Multi-Procesamiento Simétrico (**SMP**).
kernel-2.6.18-s390.config	Configuración genérica para arquitectura **s390**.
kernel-2.6.18-s390x.config	Configuración genérica para arquitectura **s390x**.
kernel-2.6.18-s390x-debug.config	Configuración genérica para arquitectura **s390**, con opciones de depuración. Solo recomendado para desarrolladores y escenarios donde se requiere diagnóstico.
kernel-2.6.18-x86_64.config	Configuración genérica para arquitectura **x86_64** (AMD K8, AMD Athlon 64, AMD Opteron).
kernel-2.6.18-x86_64-debug.config	Configuración genérica para arquitectura **x86_64**, con opciones de depuración. Solo recomendado para desarrolladores y escenarios donde se requiere diagnóstico.
kernel-2.6.18-x86_64-xen.config	Configuración genérica para arquitectura **x86_64**, con soporte para Xen. Permite utilizar paravirtualización a través de Xen.

7.2.3.2. Descargar desde kernel.org

La principal ventaja de descargar el núcleo desde **kernel.org** es que se contará con la más reciente versión, mejoras y más dispositivos soportados. El inconveniente es que puede perderse la estandarización con la distribución utilizada o bien la compatibilidad con algunas aplicaciones de terceros que dependen directa o indirectamente de una versión en particular del núcleo, o un **API** incluido en alguna versión en particular del núcleo.

Se accede hacia **http://www.kernel.org/** y se descarga, desde la parte inferior de la portada del sitio, la versión más reciente del núcleo.

```
wget \
http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.25.10.tar.bz2
```

Lo anterior descargará el paquete **linux-2.6.25.10.tar.bz2**.

Se procede a descomprimir **linux-2.6.25.10.tar.bz2** utilizando lo siguiente:

```
tar jxvf linux-2.6.25.10.tar.bz2
```

Lo anterior descomprimirá el contenido en un directorio denominado **linux-2.6.25.10**. Solo resta es acceder hacia este directorio para configurar las opciones que se utilizarán.

```
cd linux-2.6.25.10
```

7.2.4. Configuración del núcleo.

Se puede utilizar el mandato **make** con la opción **config** de la siguiente forma:

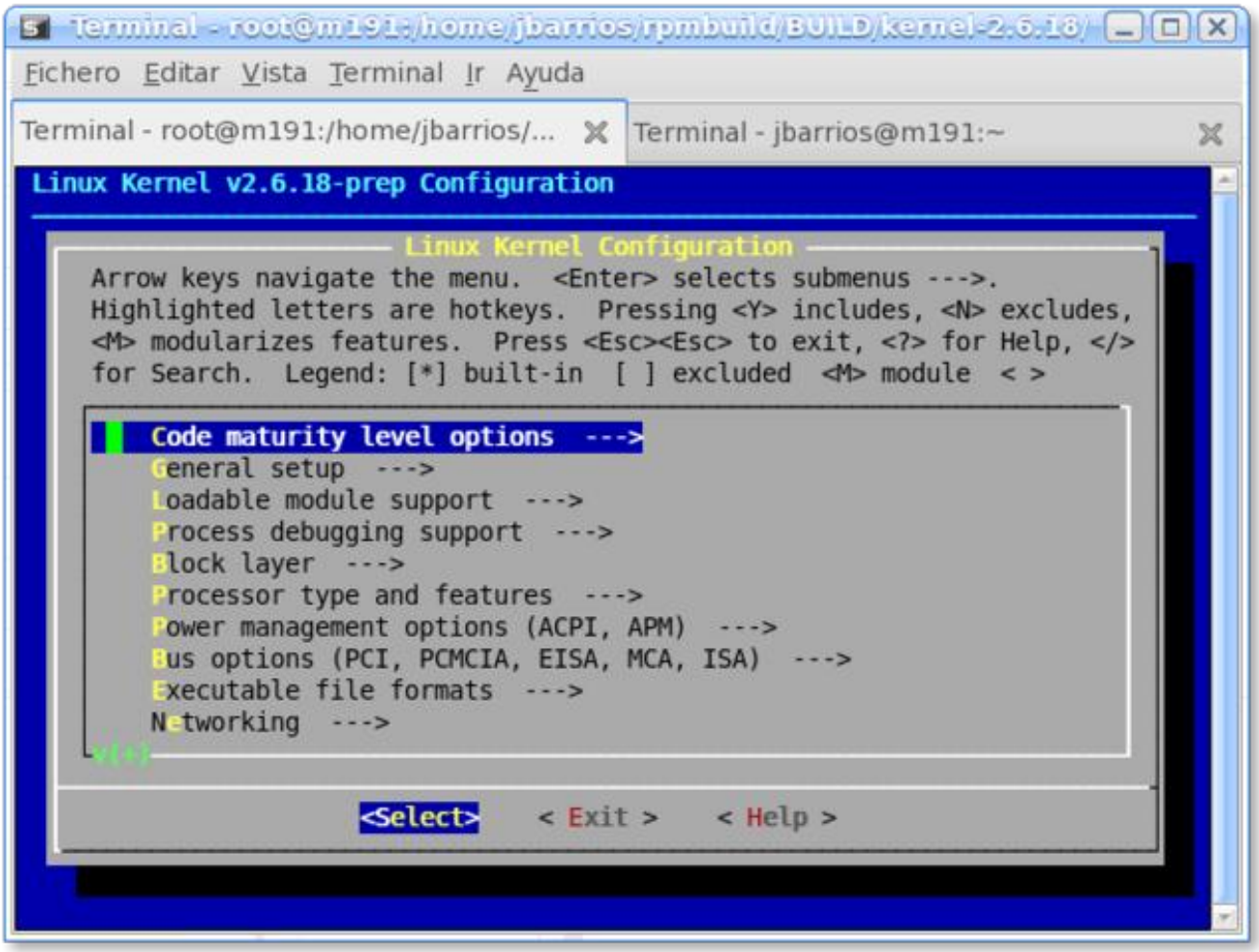
```
make config
```

El inconveniente de ésto es que se tendrá que responder una a una cada una de las opciones del núcleo. Solo se recomienda para usuario muy experimentados.

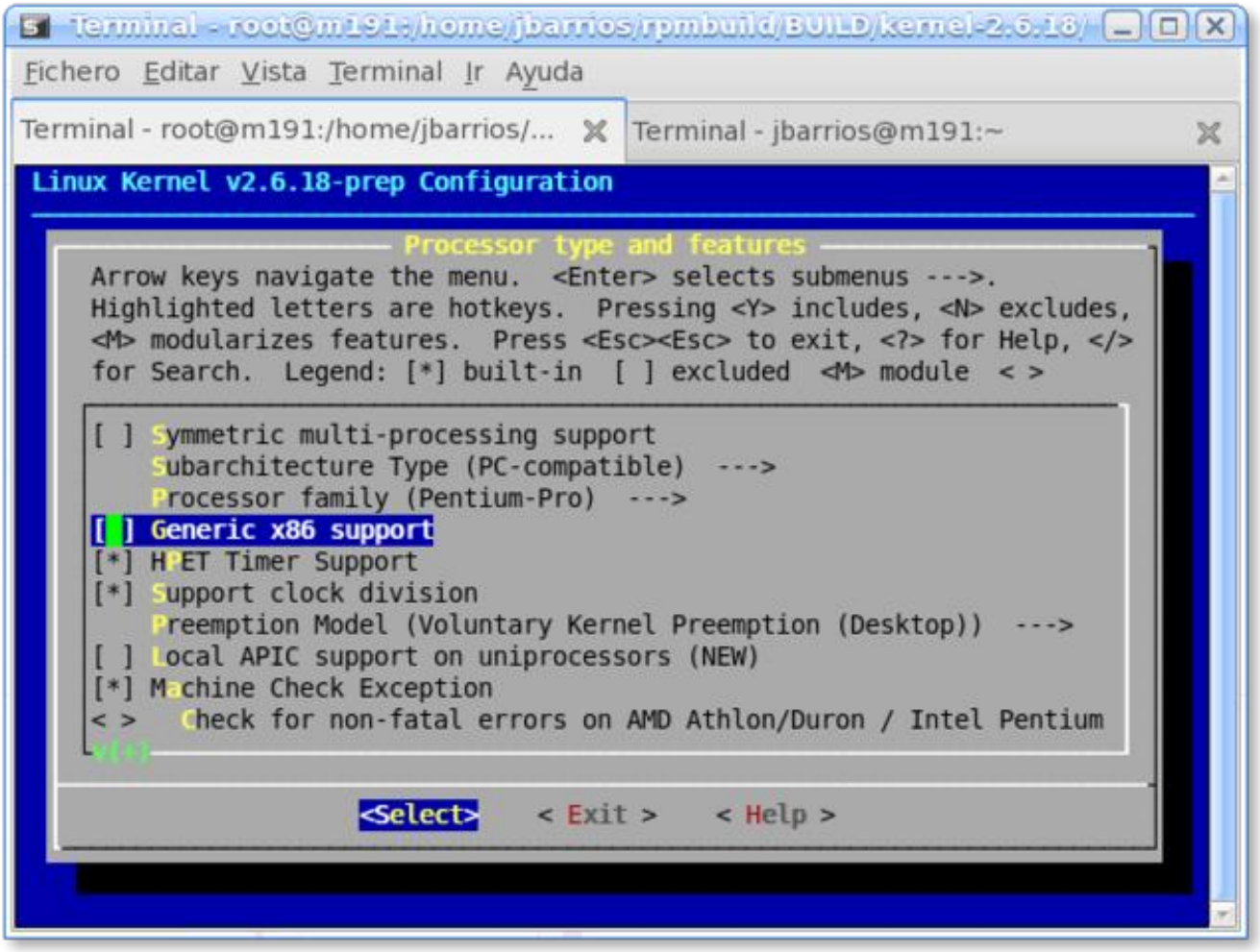
Se puede utilizar el mandato **make** con la opción **menuconfig de** la siguiente forma:

```
make menuconfig
```

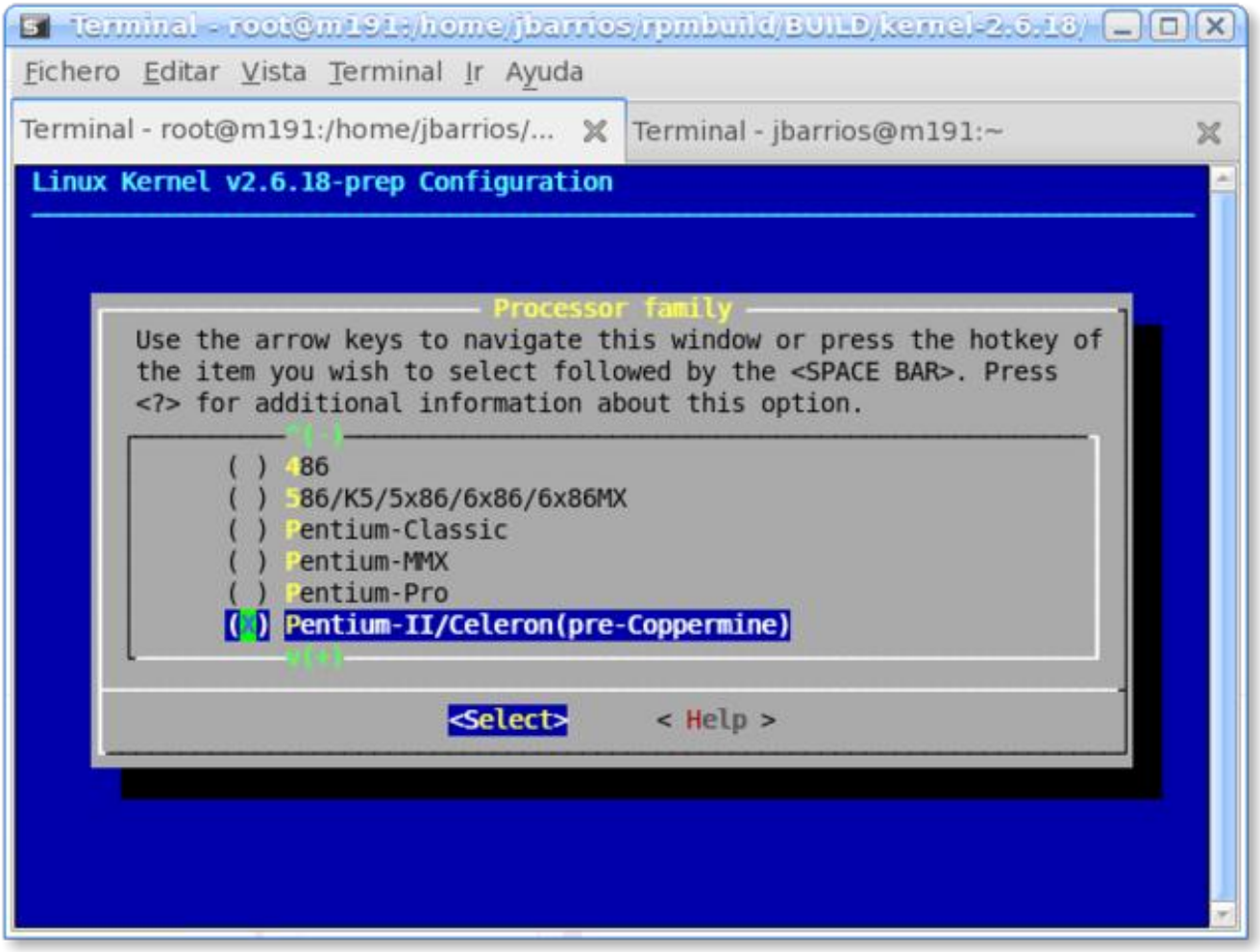
Lo anterior compilará y ejecutará una interfaz hecha en **ncurses** que permitirá examinar el árbol de opciones y habilitar y deshabilitar de una forma más amistosa, pues cada opción incluye una ayuda que explica para que sirve y si es seguro incluirla, compilarla como módulo o excluirla.



En general, se puede empezar excluyendo las optimizaciones genéricas y funciones que nunca se utilizarán en el sistema como el multiprocesamiento simétrico y soporte para más de 4 GB de RAM.



Y luego seleccionado el tipo exacto de microprocesador y excluir las funciones genéricas.



Pueden habilitarse o excluirse funciones y módulos, de acuerdo a las necesidades y el sustento físico determinado previamente con los mandatos **lsmod**, **lspci** y **lsusb**, en el resto de las opciones del árbol de configuración de **menuconfig**.

En general se puede compilar dentro del núcleo lo siguiente:

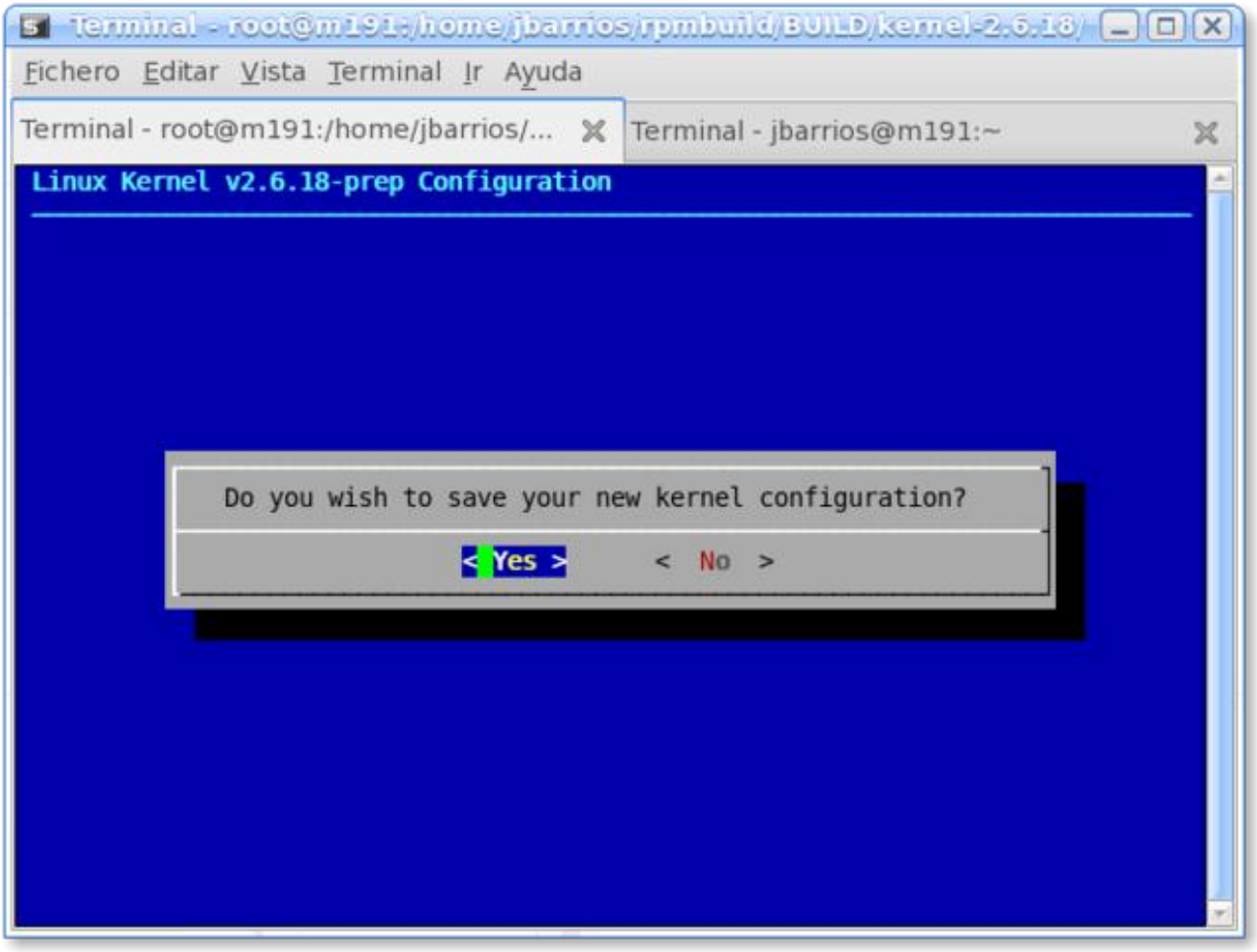
- Controladores para dispositivos integrados en la tarjeta madre que sean de uso continuo.
- Controladores de dispositivos de uso continuo, como controladores de disco y transportes (*buses*) **SCSI** (**S**mall **C**omputers **S**ystem **I**nterface o Sistema de Interfaz para Pequeñas Computadoras), **ATA** (**A**dvanced **T**echnology **A**ttachment), **PATA** (**P**arallel **A**dvanced **T**echnology **A**ttachment), **SATA** (**S**erial **A**dvanced **T**echnology **A**ttachment), **RAID** (**R**edundant **A**rray of **I**nexpensive **D**isks o conjunto redundante de discos independientes), etc.
- Soporte de **LVM** (**L**ogical **V**olume **M**anager o Gestor de Volúmenes Lógicos).
- Controladores para sistemas de ficheros (**ext3**).

En general se debe evitar incluir dentro del kernel y solo compilar como módulo lo siguiente:

- Controladores de dispositivos periféricos (como los controladores para cámaras digitales).
- Controladores para cualquier dispositivo que se pueda remover del sistema (es decir dispositivos **USB**, **Firewire**, **Bluetotooth**, etc.).
- Controladores de dispositivos que se intercambien con frecuencia.

La regla general es **mantener el núcleo lo más pequeño posible** y evitar incluir dentro de éste demasiados controladores. Si se compila un controlador dentro del núcleo y el dispositivo es retirado del sistema o éste sufre algún tipo de daño que afecte su funcionamiento, el núcleo puede sufrir conflictos con el resto de los controladores, o bien sufrir un fallo. Es preferible compilar como módulos los controladores de todo aquello que se pueda remover del sistema, incluyendo los dispositivos que utilicen ranuras **PCI**.

Al terminar de configurar lo anterior, simplemente se sale de **menuconfig** para guardar los cambios.



7.2.4.1. Compilación del núcleo.

La compilación se inicia utilizando el mandato **make**.

```
make
```

7.2.4.2. Instalación del núcleo.

Después de varios minutos, dependiendo de la capacidad del sistema, se procede a instalar primero los módulos:

```
make modules_install
```

Al concluir el procedimiento, se instala el núcleo.

```
make install
```

Lo anterior instalará el núcleo en el directorio **/boot**, creará el fichero **system.map** correspondiente, creará la imagen del disco RAM correspondiente y añadirá una entrada en el fichero **/boot/grub/grub.conf**, respetando los núcleos previamente instalados al colocarse como opción de arranque secundaria.

Simplemente reinicie y pruebe el nuevo núcleo. Si todo parece funcionar correctamente, puede editar el fichero **/boot/grub/grub.conf** y colocar el nuevo núcleo como predeterminado.

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol00
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.25.10)
        root (hd0,0)
        kernel /vmlinuz-2.6.25.10 ro root=/dev/VolGroup00/LogVol00
        initrd /initrd-2.6.25.10.img
title CentOS (2.6.18-92.1.6.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-92.1.6.el5 ro root=/dev/VolGroup00/LogVol00
        initrd /initrd-2.6.18-92.1.6.el5.img
```

NOTA: Es muy importante siempre conservar una copia del núcleo que viene con la distribución utilizada en caso de presentarse problemas.

7.2.4.3. Creando paquete RPM.

Se puede crear un paquete **RPM** a partir de los binarios recién compilados. Acceda de nuevo hacia el directorio del núcleo recién compilado y utilice el mandato **make** con la opción **binrpm-pkg** de la siguiente forma:

```
make binrpm-pkg
```

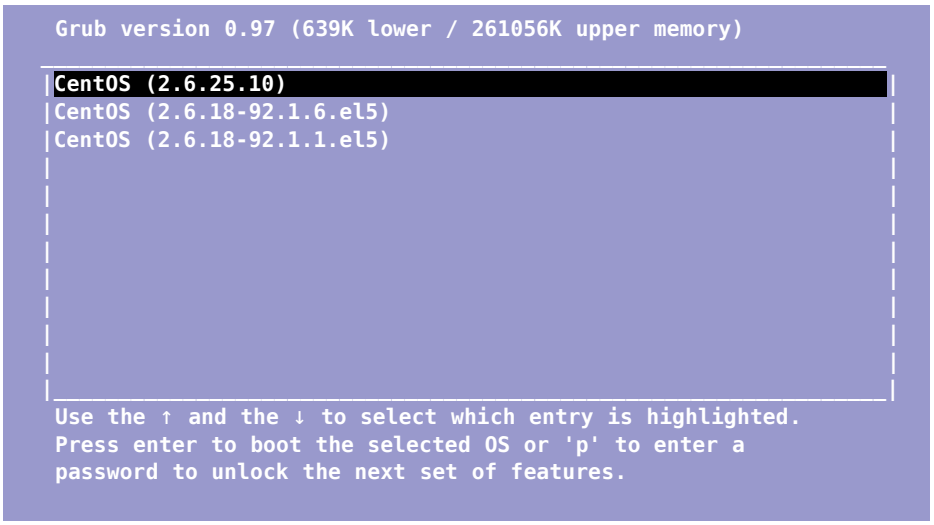
Si desea crear un paquete **RPM** compilando todo de nuevo, puede utilizar el mandato **make** con la opción **rpm-pkg** de la siguiente forma:

```
make rpm-pkg
```

La instalación del paquete resultante se realiza utilizando el mandato **rpm** con las opciones **-ivh** (instalar, descriptivo y mostrar barra de progreso), a fin de que se mantengan instalados los paquetes del núcleo existentes en el sistema y estos coexistan, permitiendo elegir con cual iniciar el sistema desde el arranque con **Grub**.

```
rpm -ivh /usr/src/redhat/RPMS/i386/kernel-2.25.10-2.i386.rpm
```

Lo anterior instalará el paquete **RPM** del núcleo recién creado, sin afectar a otras versiones de paquetes del núcleo que estén previamente instaladas. Al terminar, solo será necesario eligir desde **Grub** el núcelo con el cual se iniciará el sistema.



8. Cómo gestionar espacio de memoria de intercambio (swap) en GNU/Linux.

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

8.1. Introducción.

8.1.1. Algo de historia.

Hace muchos años, **GNU/Linux**, en los tiempos del núcleo versión 2.0, se encontraba limitado a utilizar una sola partición de memoria de intercambio de un máximo de 128 MB, siendo esto una de los principales argumentos utilizados por sus detractores. Por fortuna las cosas han cambiado, y hoy en día ya no existe dicho límite, y es posible además utilizar cuanta memoria de intercambio sea requerida para satisfacer las necesidades de cualquier sistema.

8.1.2. ¿Qué es y como funciona el espacio de intercambio?

El espacio de memoria de intercambio o **Swap**, es lo que se conoce como **memoria virtual**. La diferencia entre la memoria real y la virtual es que está última utiliza espacio en el disco duro en lugar de un módulo de memoria. Cuando la memoria real se agota, el sistema copia parte del contenido de esta directamente en este espacio de memoria de intercambio a fin de poder realizar otras tareas.

Utilizar memoria virtual tiene como ventaja el proporcionar la memoria adicional necesaria cuando la memoria real se ha agotado y se tiene que realizar un proceso. El inconveniente radica en que, como consecuencia de utilizar espacio en el disco duro, la utilización de esta es mucho muy lenta. Uno puede percatarse de esto cuando el disco duro empieza a trabajar repentinamente hasta por varios minutos después de abrir varias aplicaciones.

¿Cuanto espacio para memoria de intercambio se debe asignar al sistema?

Menos de 1 GB de RAM	Misma cantidad de memoria RAM total
2-4 GB de RAM	50% de memoria RAM total
Más de 4 Gbytes de RAM	2 GB

8.1.3. Circunstancias en las que se requiere aumentar la cantidad de memoria de intercambio.

Contar con mayor espacio para utilizar memoria virtual puede ser práctico en los siguientes casos:

- Sistemas en donde adquirir memoria adicional está fuera de toda discusión.
- En equipos con trabajo intensivo que consume mucha memoria (diseño gráfico, por

ejemplo).
- Servidores de alto desempeño en donde se desea contar con un amplio margen de espacio Swap para satisfacer las demandas de servicios.
- Sistemas que actualizaron desde una versión de núcleo 2.2 a una versión de núcleo 2.4 o 2.6.
- Sistemas donde se aumentó la cantidad de memoria RAM y se encuentran con la problemática de cubrir la cuota mínima de espacio de memoria de intercambio.

Procedimientos.

Todos los procedimientos listados a continuación requieren hacerse como el usuario **root** o bien utilizando el mandato **sudo**.

8.1.4. Cambiar el tamaño de la partición.

Cambiar el tamaño de las particiones el disco duro y cambiar las dimensiones una partición de memoria de intercambio adicional es el método más efectivo.Sin embargo,ésto representa un riesgo, debido que podría ocurrir un error durante el procesos de repartición que podría desencadenar en pérdida de datos en un disco duro. Si se utiliza este método, es importante disponer de un respaldo de todos los datos importantes antes de comenzar el proceso.

8.1.5. Crear un fichero para memoria de intercambio.

Otro método más sencillo y sin riesgo alguno, consiste en utilizar un archivo de intercambio de forma similar a como se hace en otros sistemas operativos.

Ante todo, la mejor solución siempre será adquirir más RAM.

8.2. Procedimientos.

8.2.1. Activar una partición de intercambio adicional.

Si se cambio la tabla de particiones del disco duro y se ha creado una nueva partición de memoria de intercambio, se le da formato de la siguiente forma con el mandato **mkswap**, donde la opción **-c** indica se verifiquen sectores del disco duro buscando bloques dañados a fin de marcar estos y evitar utilizarlos:

```
/sbin/mkswap -c [dispositivo]
```

En el siguiente ejemplo se dará formato como partición de memoria de intercambio a la partición **/dev/hda8** de 256 MB, verificando sectores en busca de bloques dañados:

```
/sbin/mkswap -c /dev/hda8
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Settting up Swapspace version 0, size=262144 bytes
```

Para activar la partición y que sea utilizada inmediatamente por el sistema operativo, se utiliza el mandato **swapon** de la siguiente forma:

```
swapon [dispositivo]
```

En el siguiente ejemplo se activa como partición de memoria de intercambio a la partición **/dev/hda8**:

```
/sbin/swapon /dev/hda8
```

Para corroborar que la nueva partición de memoria de intercambio está siendo utilizada por el sistema operativo, se utiliza el el mandato **free**, que puede devolver una salida similar a la siguiente:

```
             total       used       free     shared    buffers     cached
Mem:        321364     312576       8788          0        940      63428
-/+ buffers/cache:     248208      73156
Swap:       639984     105740     534244
```

Para que esta partición se utilice como memoria de intercambio automáticamente en el siguiente arranque del sistema, debe agregarse la línea correspondiente en el fichero **/etc/fstab** del siguiente modo:

```
[partición]             swap    swap    defaults        0 0
```

En el siguiente ejemplo se definirá como partición de memoria de intercambio a la partición **/dev/hda8** en el fichero **/etc/fstab**:

```
/dev/hda8               swap    swap    defaults        0 0
```

8.2.2. Utilizar un fichero como memoria de intercambio.

Este método no requiere hacer cambios en la tabla de particiones del disco duro. Es idóneo para usuarios poco experimentados, para quienes desean evitar tomar riesgos al cambiar la tabla de particiones el disco duro, o bien para quienes requieren más de memoria de intercambio ocasional o circunstancialmente.

Considerando que el fichero de memoria de intercambio puede ser colocado en cualquier directorio del disco duro, se utiliza el mandato **dd**, especificando que se escribirán ceros (**if=/dev/zero**) para crear el fichero **/swap** (**of=/swap**), en bloques de 1024 bytes hasta completar una cantidad en bytes determinada (**count=[cantidad en bytes]**). En el siguiente ejemplo se realiza lo anterior hasta completar **262144 bytes** (**count=262144**), que equivalen a **256 MB**:

```
dd if=/dev/zero of=/swap bs=1024 count=262144
```

Se requiere darle formato de memoria de intercambio al fichero creado con el mandato **mkswap**. En el siguiente ejemplo se dará formato fichero **/swap** para ser utilizado como memoria de intercambio especificando que éste será de **262144 bytes**:

```
/sbin/mkswap /swap 262144
```

Lo anterior puede devolver una salida similar a la siguiente:

```
Settting up Swapspace version 0, size=262144 bytes
```

p>Para activar la partición y que sea utilizada inmediatamente por el sistema operativo, se utiliza el mandato **swapon**. En el siguiente ejemplo se activa como partición de memoria de intercambio a el fichero **/swap**:

```
/sbin/swapon /swap
```

Para corroborar que nuevo fichero de memoria de intercambio está siendo utilizada por el sistema operativo, se utiliza el el mandato **free**, que puede devolver una salida similar a la siguiente:

```
             total       used       free     shared    buffers     cached
Mem:        321364     312576       8788          0        940      63428
-/+ buffers/cache:     248208      73156
Swap:       639984     105740     534244
```

Para que este fichero se utilice como memoria de intercambio automáticamente en el siguiente arranque del sistema, debe agregarse la línea correspondiente en el fichero **/etc/fstab** del siguiente modo:

```
/swap           swap    swap    defaults        0 0
```

8.2.3. Optimizando el sistema cambiando el valor de /proc/sys/vm/swappiness

El núcleo de **GNU/Linux** permite cambiar con que frecuencia las aplicaciones y programas son movidas de la memoria física hacia la memoria de intercambio. El valor predeterminado es 60, como puede observarse al mirar el contenido de **/proc/sys/vm/swappiness** de la siguiente forma:

```
cat /proc/sys/vm/swappiness
```

Pueden establecerse valores entre 0 y 100, donde el valor más bajo establece que se utilice menos la memoria de intercambio, lo cual significa que se reclamará en su lugar el caché de la memoria. El valor predeterminado de 60 fue establecido teniendo en mente a los desarrolladores del núcleo de GNU/Linux a fin de permitir realizar pruebas y diagnósticos.

Para la mayoría de los casos, conviene cambiar este valor por uno más bajo a fin de que el sistema utilice menos la memoria de intercambio y utilice más la **memoria cache**. Ésta es una clase de memoria RAM estática de acceso aleatorio (**SRAM** o **S**tatic **R**andom **A**ccess **M**emory). Se sitúa entre la **Unidad Central de Procesamiento** (**CPU**) y la memoria RAM y se presenta de forma temporal y automática para el usuario proporcionado acceso rápido a los datos de uso más frecuente.

Un valor apropiado y que funcionará para la mayoría de los sistemas en producción es **10**. En el siguiente ejemplo se aplica el valor **10** para el fichero **/proc/sys/vm/swappiness**.

```
echo 10 > /proc/sys/vm/swappiness
```

Para lo anterior, también se puede utilizar el mandato **sysctl** de la siguiente forma:

```
sysctl -w vm.swappiness=10
```

Lo anterior devuelve una salida similar a la siguiente, confirmando que se ha aplicado el cambio:

```
[root@mlocalhost ~]# sudo -w sysctl vm.swappiness=10
vm.swappiness = 10
```

Este cambio en las variables del sistema de forma aplica inmediata hasta el siguiente reinicio del sistema. Para hacer que el cambio sea permanente, se edita el fichero **/etc/sysctl.conf** y se añade la siguiente línea:

```
vm.swappiness = 10
```

9. Procedimientos de emergencia

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: http://www.alcancelibre.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 optimizar el sistema de archivos ext3.

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

10.1. Introducción.

Cuando se trabaja con servidores y estaciones de trabajo con instalaciones de **Ubuntu**, **CentOS**, **Red Hat** o **Fedora** y se busca optimizar el uso del disco duro de sistemas de archivos ext3, hay ajustes que pueden mejorar el desempeño significativamente.

10.1.1. Acerca de ext3.

ext3 (*third extended filesystem* o tercer sistema de archivos extendido) es el sistema de archivo más utilizado por las distribuciones de **GNU/Linux** y. Se diferencia de **ext2** en que trabaja con registro por diario (*journaling*) y porque utiliza un árbol binario balanceado (árbol **AVL**, creado por los matemáticos rusos Georgii **A**delson-**V**elskii y Yevgeniy **L**andis) y también por incorporar el método **Orlov** de asignación para bloques de disco (el mismo que se gestiona a través de los mandatos **lsattr** y **chattr**). Además **ext3** permite ser montado y utilizado como si fuera **ext2** y actualizar desde **ext2** hacia **ext3** sin necesidad de formatear la partición y, por tanto, sin perder los datos almacenados en ésta.

10.1.2. Acerca del registro por diario (journaling).

El registro por diario (*journaling*) es un mecanismo por el cual un sistema de archivos implementa transacciones. Consiste en un registro en el que se almacena la información necesaria para restablecer los datos dañados por una transacción en caso de que ésta falle, como puede ocurrir durante una interrupción de energía.

10.2. Procedimientos

Para determinar que dispositivos corresponden a las particiones en el disco duro, se utiliza el mandato **df**. Ejemplo:

```
[root@m064 ~]# df
S.ficheros         Bloques de 1K   Usado    Dispon Uso% Montado en
/dev/hda2            19283024  17279260   1207584  94% /
/dev/sda1               77749     21905     51830  30% /boot
/dev/sdb1            17496684  10618980   5988912  64% /home
/dev/hda5            54158844  41284544  11223624  79% /var/ftp
/dev/sda2            15352348   4874232   9698164  34% /home/rpmbuild
tmpfs                  777732         0    777732   0% /dev/shm
```

Una vez determinados que dispositivos corresponden a las diferentes particiones, pueden aplicarse varios métodos de optimización.

10.2.1. Utilizando el mandato e2fsck.

El mandato **e2fsck** se utiliza regularmente para revisar y reparar particiones con formato **ext2** y **ext3**. Incluye la opción **-D** que realiza la optimización de directorios en el sistema de archivos. La optimización de todos los directorios de una partición consiste en volver a posicionar (*reindexing*) los directorios, cuando el sistema de archivos incluye soporte para tal, o volviendo a acomodar y comprimiendo directorios. La opción **-D** se debe utilizar junto con la opción **-f** para forzar la verificación de la partición del disco duro.

Para optimizar una partición en formato **ext3**, es indispensable que ésta esté desmontada. Para poder desmontar una partición es indispensable que el sistema funcione sin procesos haciendo uso de contenidos en dicha partición. Puede utilizarse el mandato **lsof** para determinar esto y así definir que es lo que se debe detener momentáneamente. Si el sistema funciona sin procesos haciendo uso de contenidos en la partición, se puede seguir el procedimiento ejemplificado a continuación con el dispositivo **/dev/sda3** que en este particular ejemplo corresponde a la partición para **/home**:

```
umount /home
e2fsck -f -D /dev/sda3
```

La salida puede devolver algo similar a lo siguiente:

```
[root@m100 SPECS]# e2fsck -D -f /dev/sda3
e2fsck 1.39 (29-May-2006)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 3A: Optimizing directories
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/home: ***** FILE SYSTEM WAS MODIFIED *****
/home: 13/5244736 files (7.7% non-contiguous), 208319/5243214 blocks
```

Una vez terminado el procedimiento, se pueden volver a montar las particiones optimizadas.

En el caso de tratarse de particiones que sea imposible desmontar por encontrarse en uso, puede utilizarse el disco de instalación de CentOS, Fedora o Red Hat en modo de rescate (**boot: linux rescue**), o un Disco Vivo (*LiveCD*), en el caso de **Ubuntu**, y desmontando las particiones que se quiera optimizar antes de utilizar el mandato **e2fsck -f -D**.

10.2.2. Opciones de montado.

Los sistemas de archivos ext3 permiten tres opciones que particularmente son útiles. Todas se especifican en la columna de opciones de los dispositivos en el fichero **/etc/fstab**.

10.2.2.1. Opción noatime (no tiempos de acceso).

Es la forma más rápida y fácil de lograr mejoras en el desempeño. Esta opción impide se actualice los tiempos de acceso de los inodos (nodos índice), los cuales realmente son poco utilizados por la mayoría de los usuarios. Esto permite mejor desempeño en servidores de noticias y **HTTP** pues

permite un más rápido acceso hacia el sistema de archivos. Es particularmente útil en computadoras portátiles pues reduce considerablemente la cantidad de procesos de **E/S** o **E**ntrada y **S**alida (**I/O** o **I**nput/**O**utput) del disco duro. Equivale a utilizar **chattr +A**, pero aplicado a todos los datos de la partición.

En el siguiente ejemplo, se configurará la opción **noatime** para la partición **/var/www** en el fichero **/etc/fstab** de un servidor HTTP.

```
LABEL=/var/www      /var/www      ext3      defaults,noatime      1 2
```

10.2.2.2. Opción commit (consignación de cambios).

Esta opción controla el tiempo que se utilizará entra cada operación sincronización (**sync**) de datos y metadatos en una partición. El **tiempo predeterminado** es de **5 segundos**. Puede incrementarse ligeramente para mejorar el desempeño, tomando en cuenta que si se específica demasiado tiempo y ocurre una interrupción de energía antes de hacer una operación de sincronización (**sync**), se perderán los datos más recientes con los que se haya trabajado. Esta opción **solo se recomienda si se dispone de un sistema de respaldo de energía confiable**.

En el siguiente ejemplo, se configurará la opción **commit** con el valor equivalente a **8 segundos** para la partición **/var/www** en el fichero **/etc/fstab** de un servidor HTTP.

```
LABEL=/var/www      /var/www      ext3      defaults,commit=8      1 2
```

10.2.2.3. Opción data (datos).

Nota: Debido a que se debe desmontar y volver a montar, las modificaciones de esta opción requieren que la partición esté sin utilizar. Por lo cual se recomienda realizar este procedimiento desde un disco de rescate o bien iniciando el sistema en nivel de ejecución 1 (monousuario).

Esta opción permite tres posibles valores:

- **ordered**: Es el valor predeterminado. Escribe los datos asociados a los metadatos primero en el sistema de archivos antes de hacerlo en el registro por diario. Si es prioritario garantizar la integridad de datos o bien se carece de un sistema de respaldo de energía confiable, es la opción que debe utilizarse.

- **writeback**: Hace que el sistema de archivos se comporte de manera similar a **XFS**. Sin preservar el ordenamiento al escribir en el disco, de modo que las **consignaciones de cambios** (*commits*) en el registro por diario puede ocurrir antes de la escritura en el sistema de archivos. Este método es **el más rápido** porque solo los metadatos se almacenan en el registro por diario, pero puede hacer que se muestren datos viejos después de una falla del sistema o interrupción de energía. **Solo se recomienda si se dispone de un sistema de respaldo de energía confiable**.

- **journal**: Es lo opuesto a **ordered**. Obliga a escribir primero los datos en el registro por diario y luego en el sistema de archivos, por lo cual utiliza un registro por diario más grande y que por lo tanto demora más tiempo en recuperarse en caso de una falla del sistema o interrupción de energía. Este es evidentemente el método más lento en la mayoría de los casos, salvo que se realicen operaciones de lectura y escritura al mismo tiempo, como ocurre con las bases de datos.

En el siguiente ejemplo se configurará en el fichero **/etc/fstab** de un servidor **HTTP** y **base de**

datos la partición **/var/www** con la opción data con el valor **writeback** y la partición **/var/lib** con la opción **data** y el valor **journal**:

```
LABEL=/var/www      /var/www      ext3      defaults,data=writeback    1 2
LABEL=/var/lib      /var/lib      ext3      defaults,data=journal      1 2
```

Antes de desmontar y volver a montar o reiniciar el sistema, hay que convertir los registros de diarios a **writeback** o bien **journal**, dependiendo el caso. Para tal fin se utiliza el mandato **tune2fs** del siguiente modo, en el caso donde se desea cambiar al modo **writeback** el registro por diario de la partición **LABEL=/var/www**:

```
tune2fs -o journal_data_writeback LABEL=/var/www
```

En el caso donde se desea cambiar al modo **journal** el registro por diario de la partición **LABEL=/var/lib**, se utiliza lo siguiente:

```
tune2fs -o journal_data LABEL=/var/lib
```

Para revertir el cambio y volver a utilizar el modo **ordered**, se puede utilizar el mandato **tune2fs** con la opción **-o journal_data**.

Para aplicar los cambios, sin correr el riesgo de reiniciar con errores de sintaxis en el fichero **/etc/fstab** que impedirían montar las particiones configuradas, se puede utilizar el mandato **umount** para desmontar la partición a modificar, y posteriormente el mandato **mount** para volver a desmontarlas. Ejemplos:

```
umount /var/www
umount /var/lib
mount /var/www
mount /var/lib
```

Utilizar el mandato **mount** cn la opción **-o remount** siempre devolverá un error de opción incorrecta. Esta es la razón por la cual se desmontan y montan las particiones para cambiar el tipo de registro por diario de las particiones.

Si lo anterior devuelve el símbolo de sistema sin errores, significa que las opciones **se aplicaron correctamente** y que el sistema puede ser reiniciado con toda seguridad en el momento que se considere apropiado.

Para regresar todo a como estaba originalmente, se edita el fichero **/etc/fstab** y se quitando las opciones **data=valor** previamente configuradas:

```
LABEL=/var/www      /var/www      ext3      defaults    1 2
LABEL=/var/lib      /var/lib      ext3      defaults      1 2
```

Se desmontan las particiones:

```
umount /var/lib
umount /var/www
```

Y con el mandato **tune2fs** se define nuevamente el formato **ordered**:

```
tune2fs -o journal_data_ordered LABEL=/var/lib
tune2fs -o journal_data_ordered LABEL=/var/www
```

Y finalmente se vuelven a montar las particiones:

```
mount /var/lib
mount /var/www
```

Si lo anterior devuelve el símbolo de sistema sin errores, significa que las opciones **fueron revertidas y aplicadas correctamente** y que el sistema puede ser reiniciado con toda seguridad en el momento que se considere apropiado.

11. Cómo configurar y utilizar Sudo

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

11.1. 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 realizar ésta.

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).

11.1.1. 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 la 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.

11.2. Equipamiento lógico necesario.

11.2.1. Instalación a través de yum.

Si se utiliza de CentOS 5, Red Hat™ Enterprise Linux 5 o White Box Enterprise Linux 5, o versiones posteriores, se puede instalar lo necesario utilizando lo siguiente:

```
yum -y install sudo
```

11.2.2. 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 sudo
```

11.3. 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.

11.3.1. 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.

11.3.2. 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.

11.3.3. 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**.

11.3.4. 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).

11.4. 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
```

11.5. 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
```

11.6. 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.

12. Cómo crear cuentas de usuario

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

12.1. 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.

12.2. 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.

12.2.1. 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.

12.2.1.1. 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
```

12.2.1.2. 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.

12.2.1.3. 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.

12.2.2. 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
```

12.3. Manejo de grupos

12.3.1. Alta de grupos

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

12.3.2. 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
```

12.3.3. Baja de grupos

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

12.3.4. Asignación de usuarios existentes a grupos existentes

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

12.4. 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.

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

12.5.1. 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.

12.5.1.1. 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/`.

12.5.1.2. 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.

12.5.2. 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
```

12.6. Apéndice: Ejercicio: Creando cuentas de usuario

12.6.1. Introducción

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

12.6.2. 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 /sbin/nologin -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
```

13. Breve lección de mandatos básicos.

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

13.1. Introducción.

Por favor **siga los procedimientos al pie de la letra**. En varios ejemplos utilizará el carácter ~ (tilde), que es una forma de abreviar el directorio de inicio del usuario con el que se ha ingresado al sistema.

13.2. 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, en este caso su directorio de inicio. El mandato **pwd**, por tanto, sirve para mostrar la ruta del directorio de trabajo actual (***p****ath of* ***w****orking* ***d****irectory*).

Realice lo siguiente:

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

Lo anterior lo cambiará al directorio **/usr/local** y le mostrará la ruta actual. El mandato **cd**, por tanto, sirve para cambiar de directorio de trabajo (***c****hange* ***d****irectory*).

Realice lo siguiente:

```
cd
pwd
```

Lo anterior lo regresará al directorio de inicio (~) y le mostrará que ahora se localiza dentro de éste.

Realice lo siguiente:

```
ls /usr/local
```

Lo anterior mostrará el contenido del directorio **/usr/local** y además le demostrará que es innecesario cambiarse a un directorio en particular para ver su contenido. El mandato **ls**, por tanto, sirve para mostrar la lista de contenido de directorios (***l****i****s****t***)

Realice lo siguiente:

```
ls
ls -a
```

Lo anterior primeramente mostrará que aparentemente no hay contenido en el directorio de inicio (~); 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 su directorio de inicio (~) 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
```

13.2.1. 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
```

13.2.2. 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
```

13.2.3. 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
```

13.2.4. 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
```

13.2.5. Apagado y reinicio de sistema.

Finalmente, y para concluir la breve lección de mandatos, es importante conocer que en

GNU/Linux se desempeñan varios procesos en el trasfondo. Estos servicios deben ser finalizados apropiadamente. El sistema operativo es muy diferente a MS-DOS, en donde se podía apagar el sistema en cualquier momento. Hay que cerrar el sistema apropiadamente, terminando servicios, guardar en disco el contenido del almacenamiento previo de la memoria (buffer) que lo requiera, y desmontar todos los sistemas de ficheros. Para tal fin se utilizan los mandatos **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
```

13.3. 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 pulse la tecla **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 se pueden utilizar como **root**)

14. Funciones básicas de vi

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

```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"holamundo.txt" [Fichero nuevo]                 0,0-1         Todo
```

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

```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERTAR --                                  0-1         Todo
```

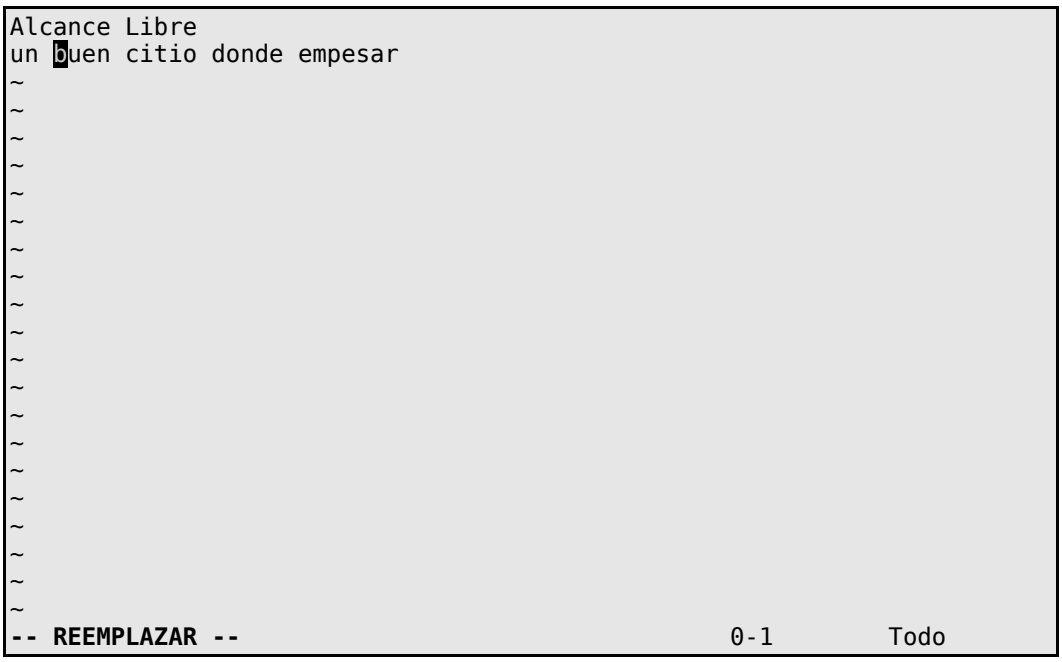
Note que en la parte inferior de la pantalla aparece la palabra «**INSERTAR**». Esto significa que, al igual que cualquier otro editor de texto conocido, puede comenzar a insertar texto en el fichero. Escriba la frase «Alcance Libre», pulse la tecla <ENTER> y **escriba** de forma propositiva la frase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

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

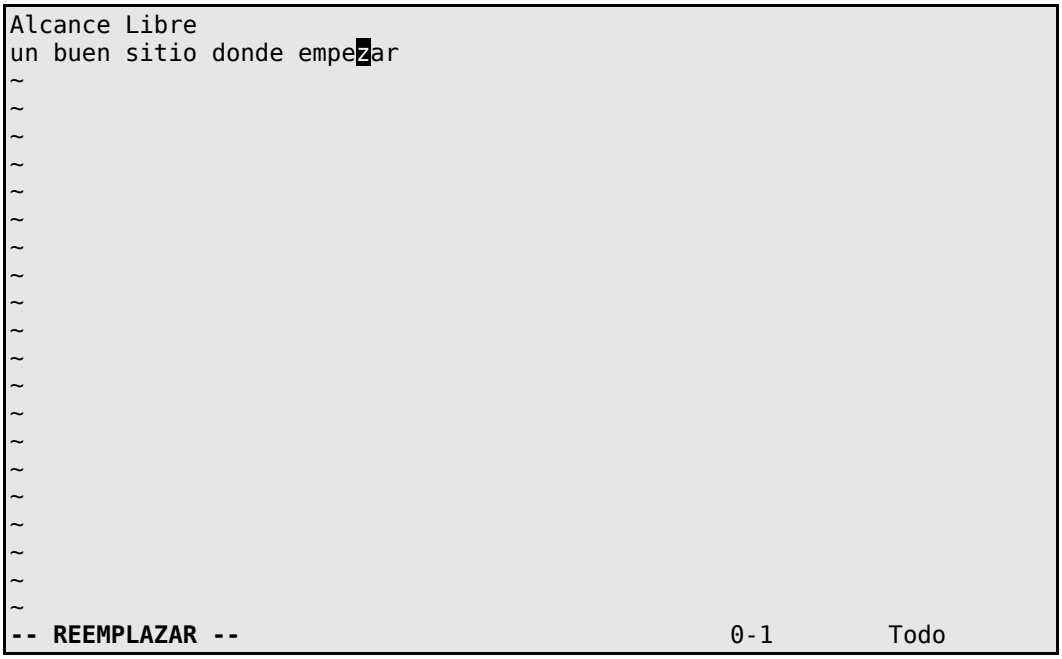
Posicione el cursor del teclado justo por debajo de la «v» de la palabra «vuen» y pulse de nuevo la tecla <INSERT> del teclado. Notará que ahora aparece la palabra «REEMPLAZAR»:

```
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
```

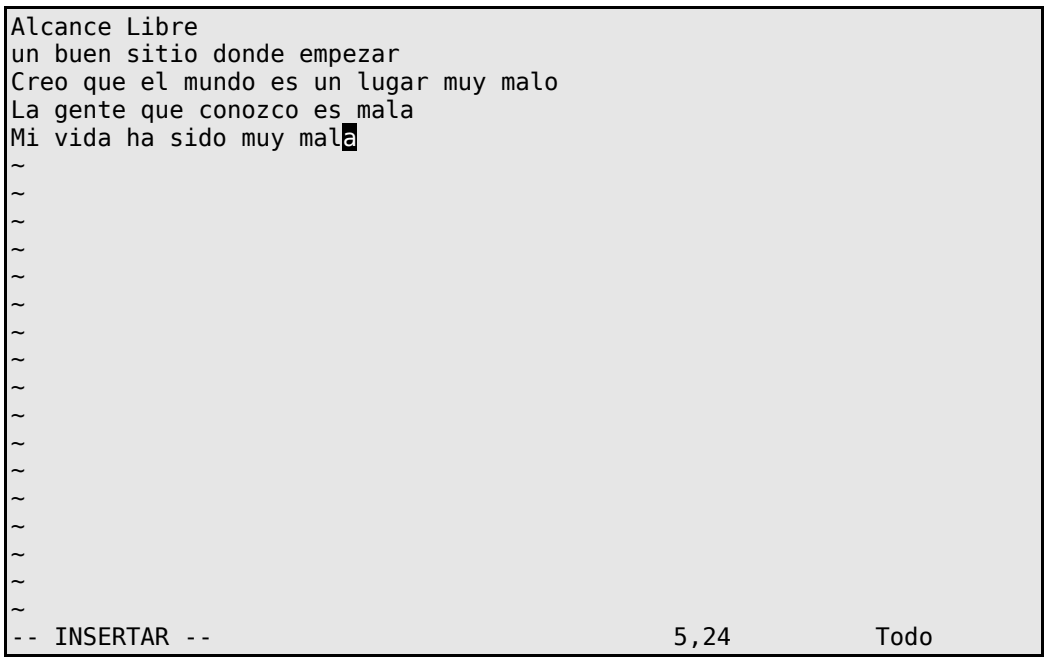
Vuelva a pulsar la tecla **:** (dos puntos) e inmediatamente escriba «saveas adiosmundo.txt»:

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

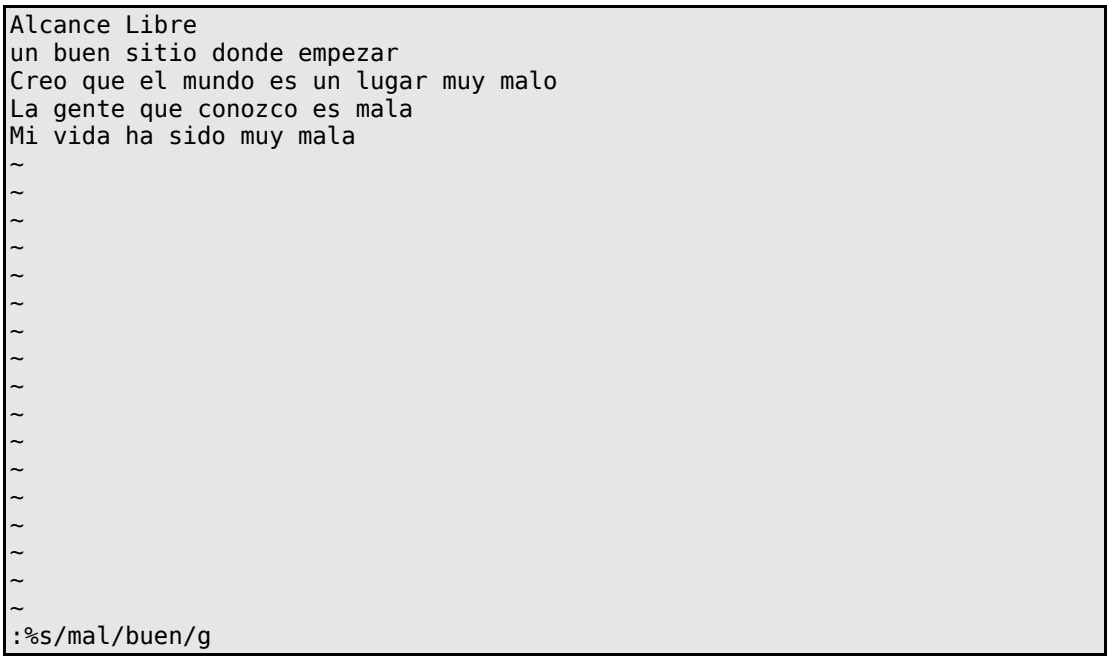
Pulse nuevamente la tecla <ENTER> y observe el mensaje en la parte inferior de la pantalla que indica que el fichero acaba de ser guardado como adiosmundo.txt:

```
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:



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:



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:

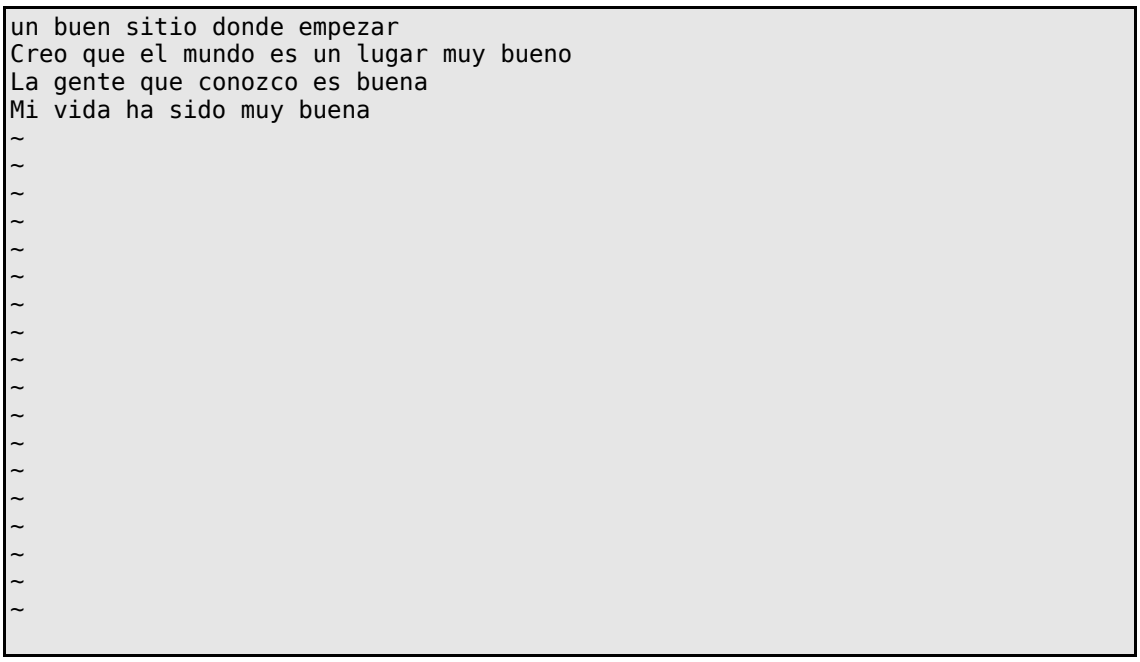
```
Alcance Libre
un buen sitio donde empezar
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
3 sustituciones en 3 líneas                    5,1           Todo
```

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».

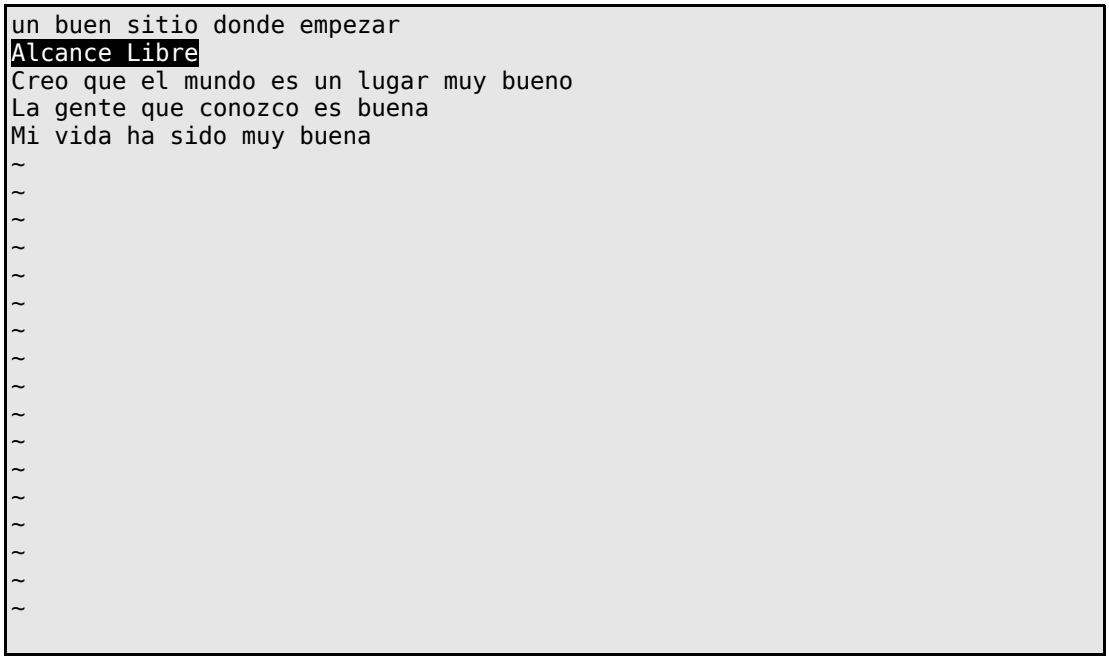
A continuación, posicione el cursor del teclado utilizando las flechas del teclado hasta el primer carácter de la primera línea:

```
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
```

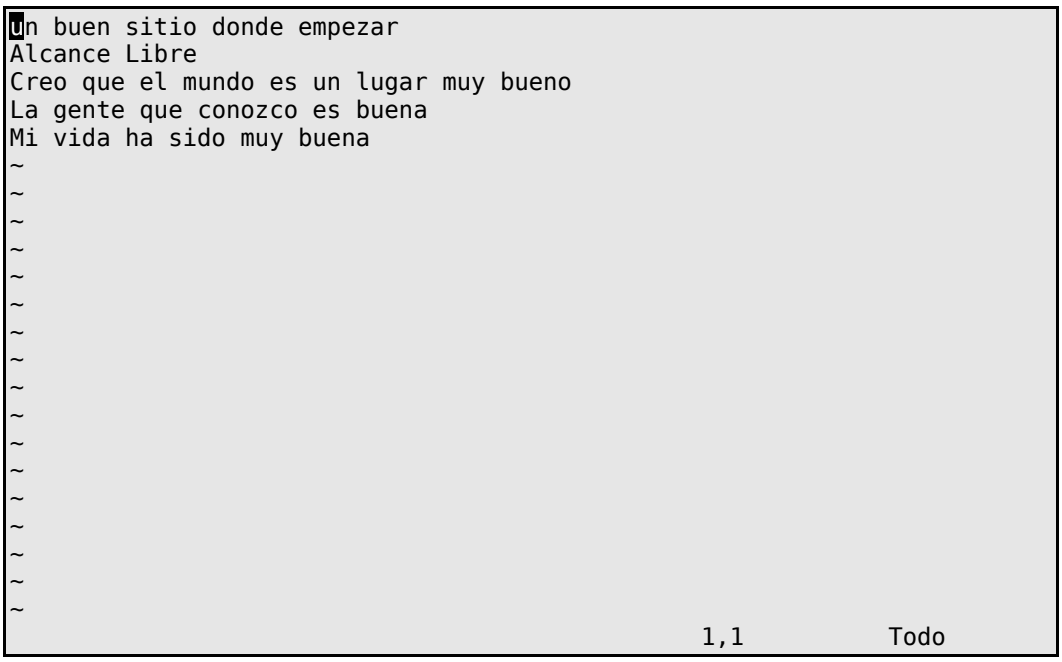
Ahora pulse dos veces consecutivas la tecla «d», es decir, pulsará «dd». Observe como desaparece la primera línea:



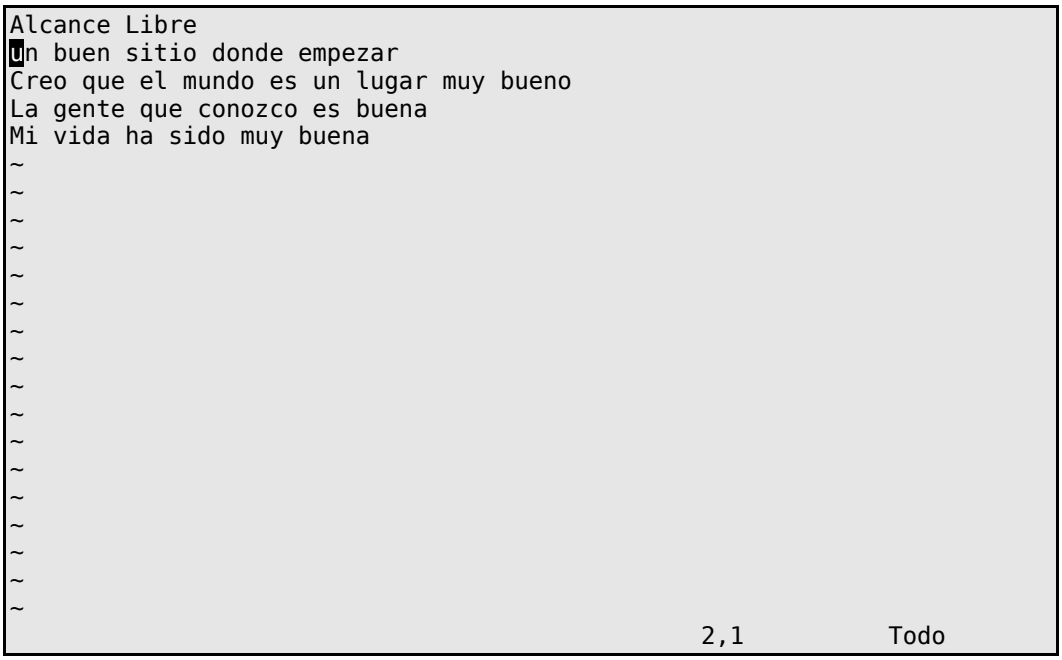
Pulse ahora la tecla «p» para volver a pegar la línea:



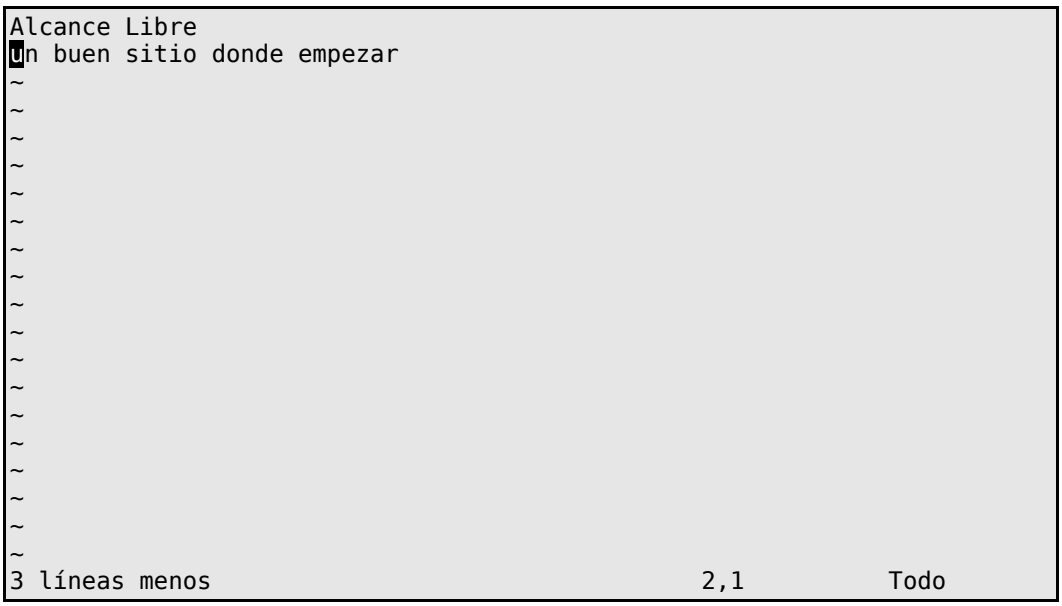
Observe que la línea «Alcance Libre» reapareció debajo de la línea «un buen sitio donde empezar». Utilizando las flechas del teclado, coloque el cursor del teclado nuevamente sobre el primer carácter de la primera linea del fichero, es decir, sobre la letra «u» de la línea «un buen sitio donde empezar»:



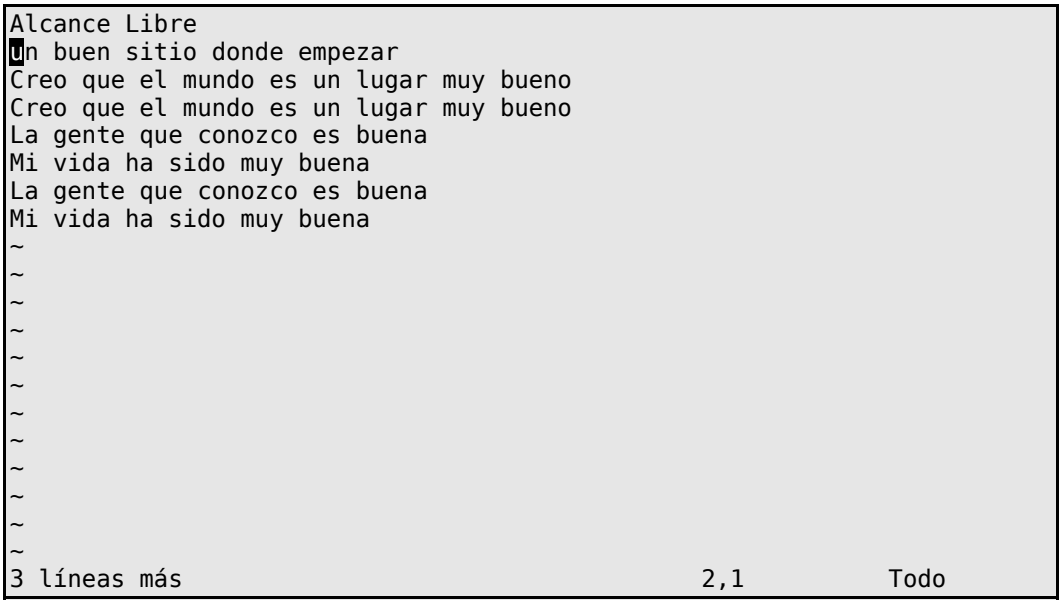
Vuelva a pulsar «dd» para cortar la línea «un buen sitio donde empezar» e inmediatamente pulse la tecla «p» para pegar la línea en el lugar correcto:



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:

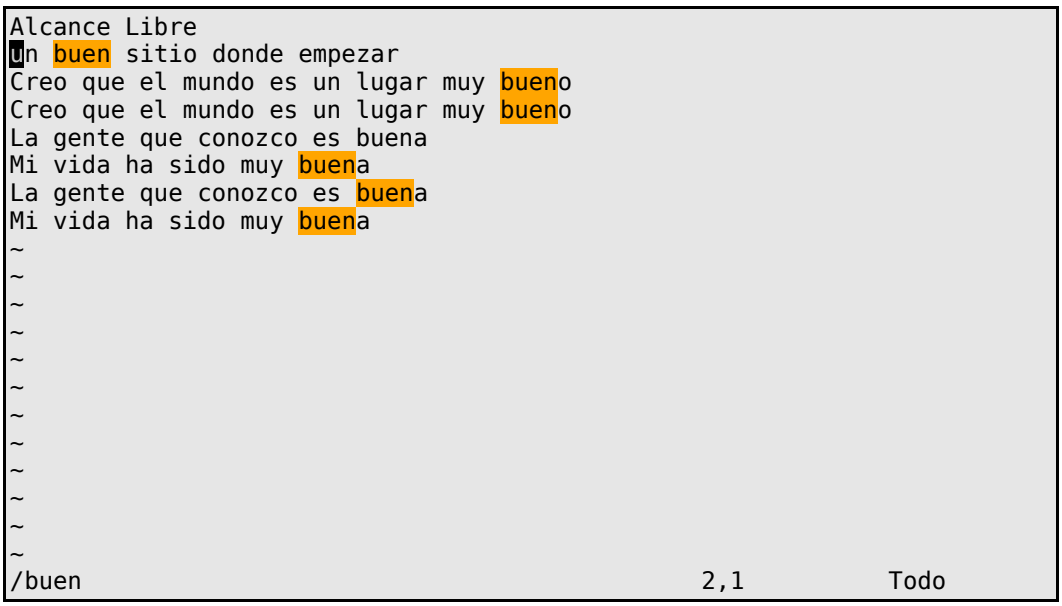


Pulse la tecla «p» una vez, observe el resultado. Vuelva a pulsar la tecla «p» y observe el resultado. Las dos acciones anteriores añadieron ahora 6 líneas restaurando las eliminadas anteriormente y agregando tres líneas más con el mismo contenido:

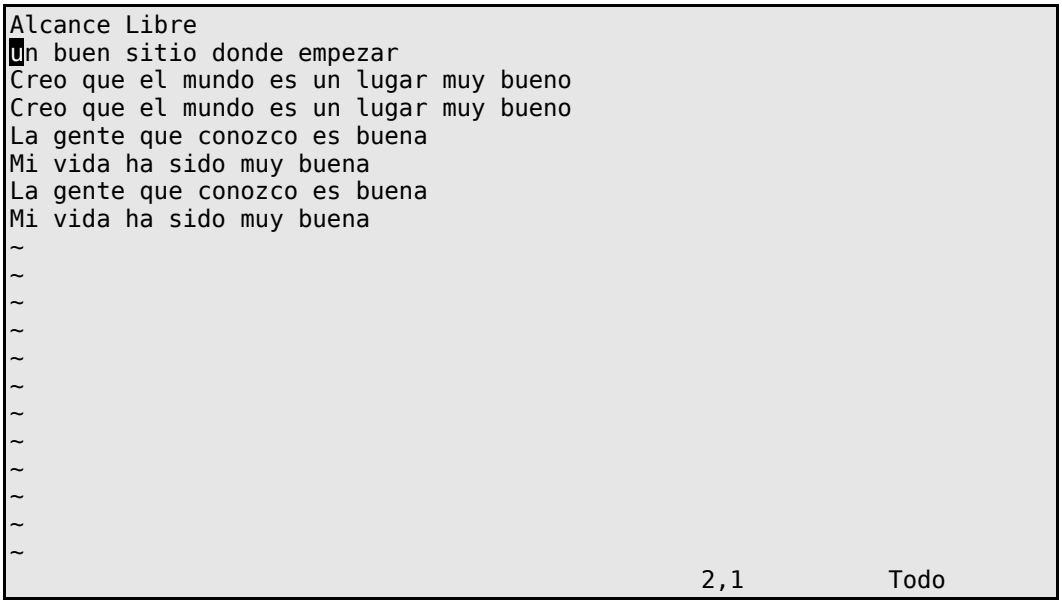


Pulse ahora la tecla **:** (dos puntos) seguido de la tecla «x» y la tecla <ENTER> a fin de salir guardando el fichero.

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:

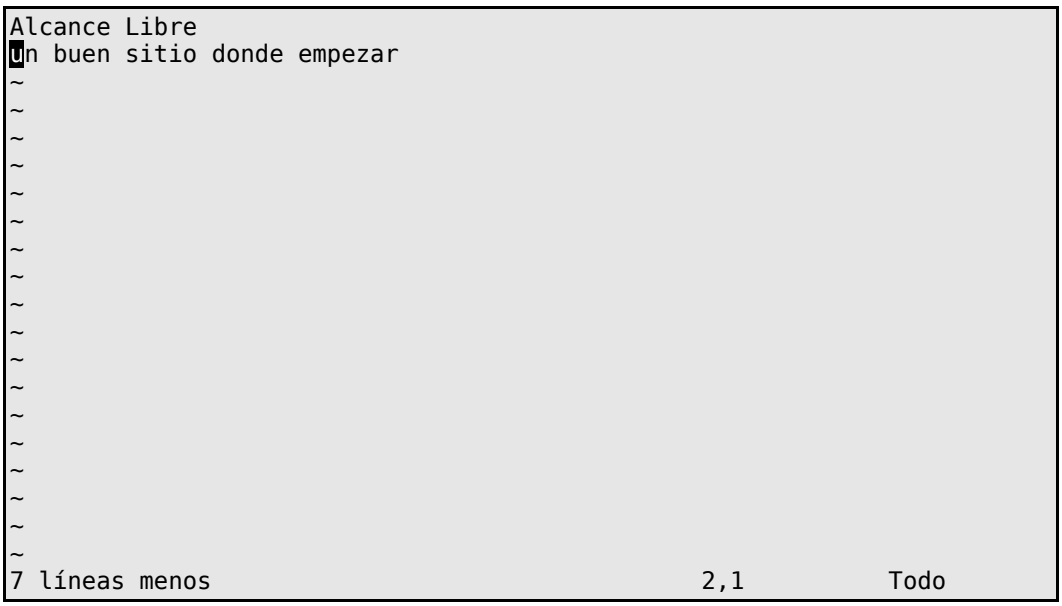
```
Alcance Libre
un buen sitio donde empezar
Creo que el mundo es un lugar muy bueno
Creo que el mundo es un lugar muy bueno
La gente que conozco es buena
Mi vida ha sido muy buena
La gente que conozco es buena
Mi vida ha sido muy buena
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERTAR --                        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

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

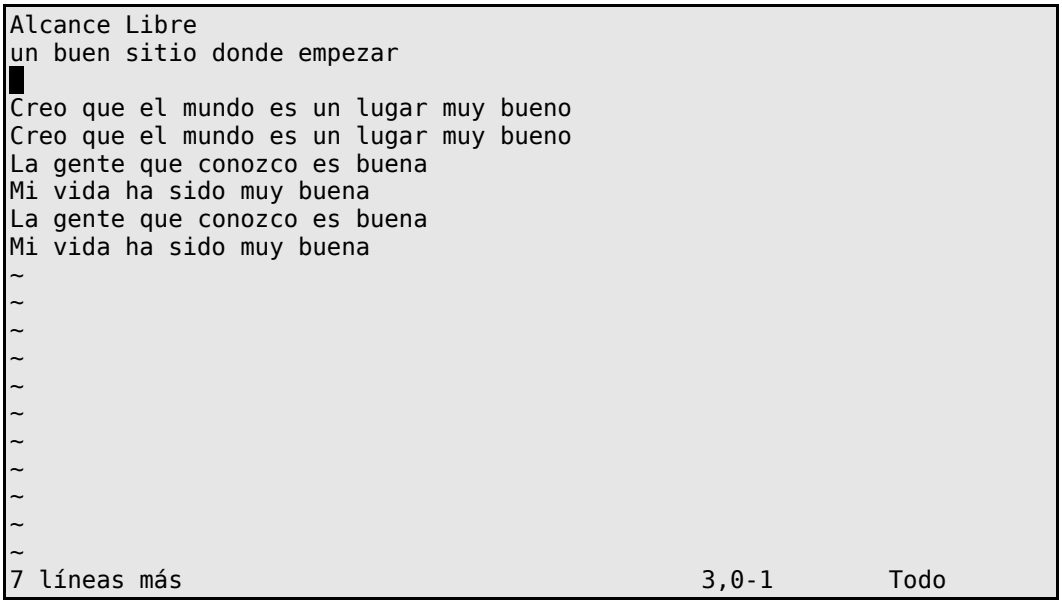
```
Alcance Libre
un buen sitio donde empezar

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:



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



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
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.

Combinación	Resultado
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/*

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. 12**9**456
```

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/*

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 en gmail punto com*
Sitio de Red: http://www.alcancelibre.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 en gmail punto com*
Sitio de Red: http://www.alcancelibre.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 en gmail punto com*
Sitio de Red: http://www.alcancelibre.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 en gmail punto com*
Sitio de Red: http://www.alcancelibre.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/*

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 en gmail punto com*
Sitio de Red: http://www.alcancelibre.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 en gmail punto com*
Sitio de Red: http://www.alcancelibre.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. Equipamiento lógico necesario.

23.2.1. Instalación a través de yum.

Si se utiliza de CentOS 5, Red Hat™ Enterprise Linux 5 o White Box Enterprise Linux 5, o versiones posteriores, se puede instalar lo necesario utilizando lo siguiente:

```
yum -y install quota
```

23.2.2. 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 quota
```

23.3. Procedimientos

I. Debe iniciarse el sistema en nivel de ejecución 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 ejecución 3 a fin de aplicar cuota de disco a algunos usuarios.

```
init 3
```

23.3.1. 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
```

23.3.1.1. 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**.

23.3.1.2. 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
```

23.3.1.3. 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`
```

23.4. 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 en gmail punto com*
Sitio de Red: http://www.alcancelibre.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 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.
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)

Nivel	Nombre	Descripción
		• **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
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 en gmail punto com*
Sitio de Red: http://www.alcancelibre.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 de origen)	RFC 1700
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	

Bloque de direcciones CIDR	Descripción	Referencia
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
/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 en gmail punto com*
Sitio de Red: http://www.alcancelibre.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 que 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 la 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). Debe verificarse que el módulo correspondiente a la tarjeta de red realmente este especificado de forma correcta. Ejemplo:

```
alias eth0 3c59x
```

Si se realizó alguna edición de este fichero, deberá de 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/2.6.9-42.0.2.EL/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 este 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 asociado a dicho nombre en el servidor del sistema de nombres de dominio (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. Este deberá ser un **FQDN** (acrónimo de **F**ully **Q**ualified **D**omain **N**ame o Nombre de Dominio Plenamente Calificado) resuelto por un servidor de nombres de domino (DNS) o bien. En el caso de sistemas sin conexión a red o sistemas caseros, sea resuelto localmente en el fichero **/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 previamente establecida. El administrador de la red deberá proporcionar una dirección IP disponible (IPADDR) y una máscara de la subred (NETMASK).

26.2.2.3. Servidores de nombres.

Debe modificarse con un editor de textos **/etc/resolv.conf**, donde se establecerán los servidores del sistema 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.

Los encaminamientos adicionales se pueden añadir utilizando el mandato **/sbin/route**, siguiendo la siguiente sintaxis:

```
/sbin/route add -net [IP-red-destino] netmask [máscara-subred] gw [IP-puerta-de-
enlace] dispositivo
```

En el siguiente ejemplo se definirá la ruta estática hacia la red **192.168.3.0** con máscara **255.255.255.0**, puerta de enlace a través de la dirección IP **192.168.1.36** y a través del dispositivo de red **eth1**:

```
/sbin/route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.1.36 eth1
```

Es un requisito que la puerta de enlace de destino sea alcanzable desde el dispositivo utilizado. Una ruta estática no puede ser establecida si no es posible alcanzar la puerta de enlace necesaria. Si se reinicia el servicio de red, los cambios se perderán.

Si se requiere establecer encaminamientos adicionales para obtener conectividad con otras redes y que los cambios sean permanentes, 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 hacer configurado todos los parámetros de red deseados, solo deberá de 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:

```
ifconfig
```

Los encaminamientos se pueden comprobar utilizando:

```
route -n
```

Para comprobar si hay resolución de nombres, se puede realizar una consulta hacia los servidores 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, 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 necesidad de configuración de servidores 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 utilizar el mandato **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         255.255.255.255 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, solo bastará añadir en el fichero **/etc/sysconfig/network** el parámetro **NOZEROCONF** con el valor **yes**:

```
NETWORKING=yes
HOSTNAME=nombre.dominio
NOZEROCONF=yes
```

Al terminar, solo hay que reiniciar el servicio de red para que surtan efecto los cambios y comprobar de nuevo con el mandato **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         255.255.255.255 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, estos son mDNSResponder y nifd. Desactivar estos dos servicios ahorrará tiempo en el arranque y se consumirán **algunos pocos menos recursos de sistema**.

```
chkconfig nifd off
chkconfig mDNSResponder off
service nifd stop
service mDNSResponder stop
```

Muchas aplicaciones y componentes para el modo gráfico dependen de Zeroconf para su correcto funcionamiento. Por tanto, no es conveniente desactivar este soporte si se va a hacer uso de el modo gráfico.

Para más detalles acerca de **Zeroconf**, puede consultarla información disponible en:

- http://www.zeroconf.org/
- http://en.wikipedia.org/wiki/Zeroconf

Desactivando el soporte para IPv6.

IPv6 o Protocolo de Internet versión 6 (Internet Protocol Version 6) es un estándar del **Nivel de Red** de TCP/IP orientado hacia datos utilizada por dispositivos electrónicos para transmitir datos a través de una *Interred* (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 limite de direcciones IP que se pueden asignar a través de IPv4, las cuales tendrán mucha demanda en un futuro no muy lejano cuando se incrementen el número de teléfonos móviles y otros dispositivos de comunicación que ofrezcan acceso hacia Internet.

IPv4 solo 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 a corregir errores y problemas en IPv6.

Mientras no se implemente de modo formal IPv6, el sistema cargará un controlador que hará que algunas aplicaciones manifiesten un acceso lento hacia Internet o problemas de conectividad. Si no se va a utilizar IPv6 lo mejor es desactivar éste del sistema. Edite el fichero **/etc/modprobe.conf** y añada lo siguiente:

```
alias ipv6 off
alias net-pf-10 off
```

Al terminar utilice:

```
depmod -a
```

Reinicie el sistema a fin de que surtan efecto los cambios.

```
reboot
```

26.3. Ejercicios.

26.3.1. Encaminamientos estáticos.

Este ejercicio considera lo siguiente:

1. Se tiene dos equipos de computo 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 10.3.2.1 con máscara de subred 255.255.255.240 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 10.3.2.1
```

El resultado esperado es que **ping** devuelva que hay 100% de pérdida de paquetes.

```
PING 10.3.2.1 (10.3.2.1) 56(84) bytes of data.

--- 10.3.2.1 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 10.3.2.1.

```
route add \
-net 10.3.2.0 \
netmask 255.255.255.240 \
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
10.3.2.0        192.168.0.1     255.255.255.240 UG    0      0        0 eth0
```

Intente ejecutar **ping** hacia la dirección recién añadida en **pc1.dominio**.

```
ping -c 3 10.3.2.1
```

El resultado esperado es que **ping** responda al ping, obteniéndose una salida similar a la siguiente:

```
PING 10.3.2.1 (10.3.2.1) 56(84) bytes of data.
64 bytes from 10.3.2.1: icmp_seq=0 ttl=64 time=0.453 ms
64 bytes from 10.3.2.1: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 10.3.2.1: icmp_seq=2 ttl=64 time=0.347 ms

--- 10.3.2.1 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 10.3.2.1 porque el registro en la tabla de encaminamiento fue eliminado al reiniciar el servicio de red.

```
service network restart
route -n
ping -c 3 10.3.2.1
```

Para hacer permanente el registro en la tabla de encaminamiento utilice un editor de texto el fichero **/etc/sysconfig/network-scripts/route-eth0** y ponga el siguiente contenido:

```
ADDRESS0=10.3.2.0
NETMASK0=255.255.255.240
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
10.3.2.0        192.168.0.1     255.255.255.240 UG    0      0        0 eth0
```

Intente ejecutar **ping** hacia la dirección recién añadida en **pc1.dominio**.

```
ping -c 3 10.3.2.1
```

Reinicie el servicio de red, visualice de nuevo los registros de la tabla de encaminamiento y compruebe de nuevo que hay respuesta al hacer ping hacia 10.3.2.1.

```
service network restart
route -n
ping -c3 10.3.2.1
```

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 solo 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 255.255.255.0
```

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 solo 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 configurar acoplamiento de tarjetas de red (bonding).

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

27.1. Introducción.

El controlador **bonding**, originalmente creado por **Donald Becker**, está incluido en prácticamente todas las distribuciones de GNU/Linux y permite sumar las capacidades de varias interfaces físicas de red con objeto de crear una interfaz lógica. Esto se lleva a cabo con el objeto de contar con redundancia o bien balanceo de carga.

27.2. Procedimientos.

27.2.1. Fichero de configuración /etc/modprobe.conf.

Se establece el controlador **bonding** para crear la interfaz **bond0** del siguiente modo:

```
alias bonding bond0
```

El controlador puede llevar parámetros que permiten modificar su funcionamiento, de entre los cuales los más importantes son **mode** y **miimon**. A fin de obtener un buen funcionamiento confiable, es importante configurar al menos éstos dos parámetros.

Para fines generales, se puede simplemente configurar del siguiente modo:

```
alias bond0 bonding
options bonding mode=0 miimon=0
```

Lo anterior establece en el parámetro **mode** la política de balanceo de carga y tolerancia a fallos y desactiva en el parámetro **miimon** la supervisión de **MII**, que corresponde la configuración más común.

Al terminar con el fichero **/etc/modprobe.conf**, es importante utilizar el mandato **depmod** para regenerar el fichero **modules.dep** y los ficheros mapa de los controladores.

```
depmod
```

Lo anterior solo debe devolver el símbolo de sistemas después de unos segundos.

27.2.1.1. Parámetro mode.

Se utiliza para establecer la política baja la cual se hará trabajar las tarjetas en conjunto. Los posibles valores son:

0 (cero): Establece una política de **Round-Robin**, que es un algoritmo que asigna una carga equitativa y ordenada a cada proceso, para proporcionar **tolerancia a fallos** y **balanceo de carga** entre los miembros del arreglo de dispositivos. Todas las transmisiones de datos son enviadas y recibidas de forma secuencial en cada interfaz esclava del arreglo empezando con la primera que esté disponible. **Es la política predeterminada** del controlador y la que funciona para la mayoría de los casos.

1 (uno): Establece una política de respaldo activo que proporciona **tolerancia a fallos**. Todo el tráfico se transmite a través de una tarjeta y solo se utilizará la otra en caso de que falle la primera.

2 (dos): Establece una política **XOR** (*exclusive-or*, exclusiva-o) para proporcionar **tolerancia a fallos** y **balanceo de carga**. Este algoritmo compara las solicitudes entrantes de las direcciones **MAC** hasta que coinciden para la dirección **MAC** (**M**edia **A**ccess **C**ontrol) de una de las tarjetas esclavas. Una vez que se establece el enlace, las transmisiones de datos de datos son enviadas en forma secuencial empezando con la primera interfaz disponible.

3 (tres): Establece una política de **Round-Robin**para proporcionar **tolerancia a fallos** y **balanceo de carga**. Todas las transmisiones de datos son enviadas de forma secuencial en cada interfaz esclava del arreglo empezando con la primera que esté disponible.

En el siguiente ejemplo se establece la política 0 (cero):

```
options bonding mode=0
```

27.2.1.2. Parámetro miimon.

Se utiliza para especificar cada cuantos milisegundos se debe supervisar el enlace **MII** (**M**edia **I**ndependent **I**nterface). Se utiliza cuando se necesita alta disponibilidad para verificar si la interfaz está activa y verificar si hay un cable de red conectado. En el siguiente ejemplo se establecen 100 milisegundos:

```
options bonding mode=0 miimon=100
```

Se requiere que **todos** los controladores del arreglo de tarjetas tengan soporte para **MII**. Para verificar si el controlador de la tarjeta tiene soporte para **MII**, se utiliza el mandato **ethtool**, donde la salida debe devolver el parámetro **Link Detected** con el valor **yes**. Ejemplo:

```
ethtool eth0
```

Lo anterior debe devolver algo similar a lo siguiente:

```
Settings for eth0:
        Supported ports: [ TP MII ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Supports auto-negotiation: Yes
```

```
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 100Mb/s
        Duplex: Half
        Port: MII
        PHYAD: 32
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: pumbg
        Wake-on: d
        Current message level: 0x00000007 (7)
        Link detected: yes
```

Para desactivar esta función, se utiliza el valor 0 (cero). Ejemplo:

```
options bonding mode=0 miimon=0
```

27.2.2. Fichero de configuración /etc/sysconfig/network-scripts/bond0.

Este se configura con los mismo parámetros que una tarjeta normal. Requiere los parámetros **ONBOOT**, **BOOTPROTO**, **DEVICE**, **IPADDR**, **NETMASK** y **GATEWAY**.

En el siguiente ejemplo se configura la interfaz **bond0** con la dirección IP estática 192.168.0.1, máscara de subred 255.255.255.0, puerta de enlace 192.168.0.254 y la interfaz inicia junto con el sistema creando el fichero **/etc/sysconfig/network-scripts/ifcfg-bond0** con el siguiente contenido:

```
DEVICE=bond0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192-168.0.1
NETMASK=255.255.255.0
GATEWAY=192.168.0.254
```

Las interfaces de red a utilizar como esclavas se configuran de la siguiente forma, considerando que se tiene eth0 y eth1, el contenido del fichero **/etc/sysconfig/network-scripts/ifcfg-eth0** sería:

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=no
SLAVE=yes
MASTER=bond0
```

Y el contenido del fichero **/etc/sysconfig/network-scripts/ifcfg-eth1** sería:

```
DEVICE=eth1
BOOTPROTO=none
ONBOOT=no
SLAVE=yes
MASTER=bond0
```

27.2.3. Iniciar, detener y reiniciar el servicio network.

Para ejecutar por primera vez el servicio **network** tras configurar el acoplamiento de tarjetas, utilice:

```
service network start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service network restart
```

Para detener el servicio **network** utilice:

```
service network stop
```

27.3. Comprobaciones.

Para verificar que la interfaz lógica quedó configurada, en el caso de haber utilizado las interfaces eth0 y eth1, utilice:

```
ifconfig
```

Lo anterior debe devolver algo similar a lo siguiente:

```
bond0     Link encap:Ethernet  HWaddr 00:01:80:41:9C:8A
          inet addr:192.168.1.64  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::201:80ff:fe41:9c8a/64 Scope:Link
          UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:5128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3817 errors:7 dropped:0 overruns:0 carrier:0
          collisions:3 txqueuelen:0
          RX bytes:3493139 (3.3 MiB)  TX bytes:495025 (483.4 KiB)

eth0      Link encap:Ethernet  HWaddr 00:01:80:41:9C:8A
          inet6 addr: fe80::201:80ff:fe41:9c8a/64 Scope:Link
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:5056 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3781 errors:0 dropped:0 overruns:0 carrier:0
          collisions:3 txqueuelen:1000
          RX bytes:3474685 (3.3 MiB)  TX bytes:488632 (477.1 KiB)
          Interrupt:11 Base address:0xc000

eth1      Link encap:Ethernet  HWaddr 00:01:80:41:9C:8A
          inet6 addr: fe80::201:80ff:fe41:9c8a/64 Scope:Link
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:7 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18454 (18.0 KiB)  TX bytes:6393 (6.2 KiB)
          Interrupt:10

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

```
          RX packets:6138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8364864 (7.9 MiB)  TX bytes:8364864 (7.9 MiB)
```

Para verificar que las interfaces de red están funcionando correctamente, y que hay un cable de red conectado a éstas, se utiliza el mandato **ethtool** del siguiente modo:

```
ethtool eth0 |grep "Link detected"
ethtool eth1 |grep "Link detected"
```

Si ambas tarjetas tiene soporte para **MII**, lo anterior debe devolver lo siguiente:

```
        Link detected: yes
        Link detected: yes
```

27.4. Bibliografía.

- Thomas Davis: http://www.linuxfoundation.org/en/Net:Bonding
- Thomas Davis: http://www.kernel.org/pub/linux/kernel/people/marcelo/linux-2.4/Documentation/networking/bonding.txt

28. Cómo conectarse a una red Wifi desde la terminal.

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

28.1. Introducción.

Configurar y conectarse a una red Wifi desde la interfaz gráfica es un procedimiento relativamente trivial, dejando que todos los procedimientos los realicen NetworkManager o Connman. Sin embargo ha circunstancias en las cuales puede ser necesario conectarse a una red Wifi desde una terminal. A continuación describiré los procedimientos para conectarse a los dos tipos de redes Wifi más utilizados, WEP y WPA, con configuraciones básicas utilizadas en dispositivos como seráin los puntos de acceso de los modem ADSL de Prodigy Infinitum.

28.1.1. Preparativos.

En sistemas operativos basados sobre Fedora, CentOS y Red Hat, el primer paso consiste en cambiarse al usuaro root:

```
su -l
```

En sistemas operativos basados sobre Ubuntu Linux, se puede utilizar el mandato **sudo** para todos los precedimientos, precediendo todos los mandatos utilizados con **sudo**.

```
sudo cualquier mandato utilizado
```

Ejemplos:

```
sudo ifup lo
sudo iwconfig wlan0
sudo iwlist wlan0 scan
```

Debido a que el servicio NetworkManager hará conflicto con los procedimientos, se debe detener este servicio:

```
service NetworkMananger stop
```

Muchos componentes del sistema requieren que esté activa la interfaz de retrono del sistema (*loopback*, por lo que es importante iniciar ésta:

```
ifup lo
```

Para poder comenzar a utilizar la interfaz Wifi, solo basta ejecutar el mandato iwconfig sobre dicha interfaz:

```
iwconfig wlan0
```

Es buena idea realizar un escaneado de las redes Wifi disponibles para asegurarse se puede acceder a la red Wifi deseada, y para determinarl el protocolo a utilizar:

```
iwlist wlan0 scan
```

28.1.2. Autenticando en el punto de acceso.

28.1.2.1. A través de redes WEP.

Para redes WEP, que se caracterizan por tener una seguridad muy pobre, es muy simple. Solo basta utilizar dos mandatos. El primero define el nombre del punto de acceso a utilizar:

```
iwconfig wlan0 essid nombre-punto-de-acceso
```

El segundo mandato se utiliza para definir la clave de acceso a utilizar, sea de 64 o 128 bit.

```
iwconfig wlan0 key clave-de-acceso
```

Si se utiliza una clave WEP tipo ASCII, se define de la siguiente manera:

```
iwconfig wlan0 key s:clave-de-acceso
```

28.1.2.2. A través de redes WPA.

Se procede a determinar el nombre de la red Wifi a utilizar y la clave de acceso. El mandato wpa_passphrase se utilizará para generar un fichero de configuración a utilizar posteriormente:

```
wpa_passphrase nombre-punto-de-acceso clave-de-acceso > /root/wpa.conf
```

Si se realiza el procedimiento desde Ubuntu Linux, el mandato anterior fallará si se utiliza **sudo** debido a limitaciones de seguridad de **sudo**, y deberá utilizarse entonces el siguiente:

```
sudo bash -c "wpa_passphrase nombre-punto-de-acceso clave-de-acceso > /root/wpa.conf"
```

Lo anterior generará el fichero wpa.conf dentro del directorio de inicio del usuario root.

Para iniciar la autenticación con la red Wifi, se utiliza el mandato wpa_supplicant con las opciones -B, para enviar el procesos a segundo plano, -D, para específicar el controlador a utilizar, y -c, para específicar el fichero de confifguración creado en el paso anterior.

```
wpa_supplicant -B -Dwext -iwlan0 -c/root/wpa.conf
```

28.1.3. Asigando parámetros de red a la interfaz.

28.1.3.1. Utilizando dhclient.

Lo más común es utilziar el mandato **dhclient** para dejar que el servidor DHCP del punto de acceso o la LAN se encargue de asignar los parámetros de red para la interfaz. Es buena idea indicar a **dhclient** que libere el préstamo que estuviera asignado en el servidor DHCP:

```
dhclient -r
```

Para obtener una nueva dirección IP, se utiliza el mandato **dhclient** de la siguiente manera:

```
dhclient wlan0
```

28.1.3.2. Asignando manualmente los parámetros de red.

Si se concocen los datos para la configuración de red, también es posible asignarlos manualmente. En el siguiente ejemplo, se asigna a la interfaz wlan0 la dirección IP 192.168.1.50, con máscara de subred 255.255.255.0 y puerta de enlace 192.168.1.254:

```
ifconfig wlan0 192.168.1.50 netmask 255.255.255.0
route add -net 0.0.0.0 netmask 0.0.0.0 gw 192.168.1.254 wlan0
```

Para definir el servidor DNS, como el usuario root, se edita el fichero /etc/resolv.conf y se define la dirección IP del servidor DNS a utilizar. En el siguiente ejemplo, se define 192.168.1.254 como servidor DNS:

```
echo "nameserver 192.168.1.254" > /etc/resolv.conf
```

Si se realiza el procedimiento desde Ubuntu Linux, el mandato anterior fallará si se utiliza **sudo** debido a limitaciones de seguridad de **sudo**, y deberá utilizarse entonces el siguiente:

```
sudo bash -c "echo 'nameserver 192.168.1.254' > /etc/resolv.conf"
```

29. Cómo utilizar lsof

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

29.1. Introducción.

29.1.1. 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**.

29.2. 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
```

30. Cómo utilizar Netcat (nc)

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

30.1. Introducción.

30.1.1. 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.

30.2. Equipamiento lógico necesario.

30.2.1. Instalación a través de yum.

Si se utiliza de CentOS 5, Red Hat™ Enterprise Linux 5 o White Box Enterprise Linux 5, o versiones posteriores, se puede instalar lo necesario utilizando lo siguiente:

```
yum -y install nc
```

30.2.2. 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 nc
```

30.3. Procedimientos.

30.3.1. 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
```

30.3.2. 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!
```

30.3.3. 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.

30.3.4. 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.

31. Como utilizar Netstat.

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

31.1. Introducción.

31.1.1. 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.

31.2. 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 **UDP**, 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
```

32. Cómo utilizar ARP.

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

32.1. Introducción

32.1.1. 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.

32.2. 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.

33. Introducción a IPTABLES

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

33.1. Introducción.

33.1.1. 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/

33.2. Equipamiento lógico necesario.

33.2.1. 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
```

33.2.2. 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
```

33.3. Procedimientos.

33.3.1. Cadenas.

Las cadenas pueden ser para tráfico entrante (INPUT), tráfico saliente (OUTPUT) o tráfico reenviado (**FORWARD**).

33.3.2. 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.

33.3.3. 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
```

33.3.4. 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
```

33.3.5. 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 201.161.1.226/32 --source-port 53 -d 0/0 -j ACCEPT
```

33.3.5.1. 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
```

33.3.6. 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
```

33.3.7. 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  --  201.161.1.226       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  --  201.161.1.226       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
```

33.3.8. 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
```

33.3.9. 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 ejecución (2, 3, 4, y 5), se utiliza lo siguiente:

```
chkconfig iptables on
```

33.4. Bibliografía.

- Wikipedia: http://en.wikipedia.org/wiki/Iptables
- Dennis G. Allard y Don Cohen http://oceanpark.com/notes/firewall_example.html

34. Cómo utilizar CBQ.

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

34.1. Introducción.

34.1.1. Acerca de cbq.

CBQ (**C**lass **B**ased **Q**ueueing o Encolamiento Basado sobre Clases), es un guión escrito en **BASH** utilizado para la gestión y control del uso de ancho de banda en GNU/Linux. Fue originalmente creado en 1999 por **Pavel Golubev** y posteriormente mantenido de 2001 a 2004 por **Lubomir Bulej**. Utiliza de una forma simplificada los mandatos **ip** y **tc** para su funcionamiento, y forma parte del paquete **iproute**, el cual se incluye en las instalaciones básica de la mayor parte de las distribuciones de GNU/Linux.

34.2. Comprendiendo la velocidad binaria (bit rate).

El término *bit rate* se traduce al español como **velocidad binaria**, **tasa de bits** o **flujo de bits**. Corresponde al numero de *bits* que se transmiten por segundo a través de un sistema de transmisión digital o entre dos dispositivos digitales. En otras palabras, es la velocidad de transferencia de datos.

De acuerdo al **Sistema Internacional de Unidades**, la unidad con la que se expresa la **velocidad binaria** (*bit rate*) es el **bit por segundo**, es decir **bit/s**, **b/s** o **bps**, donde la **b** siempre debe escribirse en minúscula para impedir confusión con la unidad **byte por segundo** (**B/s**). Los múltiplos para byte aplican de diferente modo que para bit. La unidad byte es igual a 8 bits, y a partir de esto se puede utilizar la siguiente tabla:

Tabla de equivalencias.

kbit/s o kbps (kb/s, kilobit/s)	1000 bits de por segundo
Mbit/s o Mbps(Mb/s, Megabit/s)	1 millón de bits por segundo
Gbit/s o Gbps (Gb/s, Gigabit/s)	Mil millones de bits por segundo
byte/s (B/s)	8 bits por segundo
kilobyte/s (kB/s, mil bytes)	8 mil bits por segundo
megabyte/s (MB/s, un millón de bytes)	8 millones de bit por segundo
gigabyte/s (GB/s, mil millones de bytes)	8 mil millones de bits

34.3. Equipamiento lógico necesario.

CBQ forma parte de la instalación del paquete **iproute**, mismo que a su vez se instala de modo predeterminado en casi todas las distribuciones de GNU/Linux.

34.3.1. 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 iproute
```

34.3.2. 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 iproute
```

34.4. Preparativos.

Antes de iniciar cualquier configuración, se deben determinarse los valores para los siguientes parámetros. Para construir una regla, se requiere al menos comprender y especificar los valores para los parámetros **DEVICE**, **WEIGHT**, **RATE** y **RULE**. Las reglas pueden ser tan complejas como la imaginación del administrador lo permita.

Los ficheros con las configuraciones se guardan dentro del directorio **/etc/sysconfig/cbq/** y deben llevar sl siguiente nomenclatura:

```
/etc/sysconfig/cbq/cbq-[número-ID-Clase].[nombre]
```

Donde **número-ID-Clase** corresponde a un número headecimal de 2 bits dentro del rango 0002-FFFF. Ejemplo: fichero que contiene una clase que controla el tráfico entrante de correo electrónico:

```
/etc/sysconfig/cbq/cbq-0002.smtp-in
```

34.4.1. Parámetro DEVICE.

Es un parámetro obligatorio. Se determina los valores con el nombre de la interfaz, ancho de banda y peso de esta interfaz. Este último valor, que es opcional en este parámetro, se calcula dividiendo el ancho de banda de la interfaz entre diez. Por ejemplo, sí se dispone de una interfaz denominada eth0 de 100 Mbit/s, el peso será 10 Mbit/s, de tal modo los valores del parámetro **DEVICE**, quedarían de la siguiente forma:

```
DEVICE=eth0,100Mbit,10Mbit
```

Si se dispone de una interfaz eth0 conectada a un modem ADSL de 2048 kbps de tráfico entrante o de bajada, el peso será de 204 kbps, de tal modo los valores del parámetro **DEVICE**, quedarían de la siguiente forma:

```
DEVICE=eth0,2048Kbit,204Kbit
```

Si se dispone de una interfaz eth0 conectada a un modem ADSL de 256 kbps de tráfico saliente o de subida, el peso será de 25 kbps, de tal modo los valores del parámetro **DEVICE**, quedarían de la siguiente forma:

```
DEVICE=eth0,256Kbit,25Kbit
```

34.4.1.1. Parámetro de clase RATE.

Es un parámetro obligatorio. Se refiere al ancho de banda a asignar a la clase. El tráfico que pase a través de esta clase será modificado para ajustarse a la proporción definida. Por ejemplo, sí se quiere limitar el ancho de banda utilizado a 10 Mbit/s, el valor de **RATE** sería 10Mbit, como se muestra a continuación.

```
RATE=10Mbit
```

Sí se quiere limitar el ancho de banda utilizado a 1024 kbit/s, el valor de **RATE** sería 1024Kbit, como se muestra a continuación.

```
RATE=1024Kbit
```

Sí se quiere limitar el ancho de banda utilizado a 512 kbit/s, el valor de RATE sería 512Kbit, como se muestra a continuación.

```
RATE=512Kbit
```

34.4.2. Parámetro de clase WEIGHT.

Es un parámetro obligatorio. Éste es proporcional al ancho de banda total de la interfaz. Como regla se se calcula dividiendo entre diez el ancho de banda total. Para una interfaz de 2048 kbps, correspondería un valor de 204Kbit:

```
WEIGHT=204Kbit
```

34.4.3. Parámetro de clase PRIO.

Es un parámetro opcional que se utiliza para especificar que prioridad tendrá sobre otras reglas de control de ancho de banda. Mientras más alto sea el valor, menos prioridad tendrá sobre otras reglas. Se recomienda utilizar el valor 5 que funcionará para la mayoría de los casos. Ejemplo:

```
PRIO=5
```

34.4.4. Parámetro de clase PARENT.

Cuando se utilizan reglas que se requiere estén jerarquizadas, se utiliza para establecer la identidad de clase padre a la que pertenecen. Puede llevar cualquier valor. Cuando se trata de una clase padre, se define junto con el parámetro **LEAF** con el valor **none**. En el siguiente ejemplo se establece la identidad 100 en una clase padre.

```
PARENT=100
LEAF=none
```

34.4.5. Parámetro de clase LEAF.

Es un parámetro opcional y se utiliza para determinar que política se utilizará para utilizar el ancho de banda de una clase padre.

Si se utiliza el valor **tbf**, que es el valor predeterminado, se utilizará el algoritmo **TBF** (**T**oken **B**ucket **F**ilter), el cual impide que la clase tome ancho de banda de la clase padre.

```
LEAF=tbf
```

Parámetros adicionales para algoritmo **TBF**.

BUFFER	Determina el tamaño máximo de ráfaga (*maximal burst size*) que la clase puede enviar, y puede llevar como parámetro opcional la longitud de los intervalos en bytes. El valor predeterminado es **10Kb/8**. es decir, ráfagas de 10Kb en intervalos de 8 bytes. `LEAF=tbf` **`BUFFER=10Kb/8`**
LIMIT	Determina el tamaño máximo de las reservas (*backlog*). Si la cola de datos por procesar contiene más de los especificados por **LIMIT**, los siguientes paquetes que lleguen serán descartados. La longitud de las reservas determina la latencia (tiempo de recuperación de datos) de la cola en caso de presentarse una congestión. El valor predeterminado es 15kb. `LEAF=tbf` **`LIMIT=15kb`**
PEAK	Determina el pico máximo para una ráfaga de tráfico de corto plazo que una clase puede enviar. Considerando que un ancho de banda de 256 kbps envía 256 Kbit por segundo, en un momento dado se puede dar el caso de el envío de 512 Kbit en 0.50 segundos, o 1 Mbit en 0.25 segundos. En el siguiente ejemplo se establece el el pico máximo para ráfagas de 1024 Kbit: `LEAF=tbf` **`PEAK=1024Kbit`**
MTU	Determina la máxima cantidad de datos que se pueden enviar al mismo tiempo en un medio físico. Es un parámetro obligatorio si se utiliza el parámetro **PEAK**. En el caso de una interfaz *Ethernet*, el valor predeterminado es igual al **MTU** de la propia interfaz (1500). `LEAF=tbf PEAK=1024Kbit` **`MTU=1500`**

El valor **sfq**, que corresponde al algoritmo **SFQ** (**S**tochastic **F**airness **Q**ueueing), hace que sea compartido el ancho de banda de la clase padre aproximadamente en la **misma** proporción de ancho de banda entre anfitriones dentro de la misma clase.

```
LEAF=sfq
```

El valor **none** permite utilizar libremente el ancho de banda disponible, siempre que el valor del parámetro **BOUDED** sea igual a **no**. En el siguiente ejemplo se especifica utilizar libremente el ancho de banda disponible:

```
LEAF=no
```

34.4.6. Parámetro de clase BOUNDED.

Es un parámetro opcional. Si el valor es **yes**, que es el valor predeterminado, la clase no tendrá

permitido utilizar ancho de banda de la clase padre. Si el valor es no, la clase podrá hacer uso del ancho de banda disponible en la clase padre. Si se establece con valor **no**, es necesario utilizar **none** o bien **sfq** en el parámetro **LEAF**.

```
PARENT=100
LEAF=sfq
BOUNDED=no
```

34.4.7. Parámetro de clase ISOLETED.

Es un parámetro opcional. Si se establece con el valor **yes**, la clase no prestará ancho de banda a las clases hijas. Si se utiliza el valor **no**, que es el valor predeterminado, se permitirá prestar el ancho de banda disponible a las clases hijas.

```
ISOLATED=no
```

34.4.8. Parámetros de filtración.

Son las reglas de filtración que se utilizan para seleccionar tráfico en cada una de las clases. La sintaxis completa es la siguiente:

```
RULE=[[saddr[/prefijo]][:puerto[/máscara]],][daddr[/prefijo]][:puerto[/máscara]]
```

En lo anterior, **saddr** se refiere a la dirección de origen. **daddr** se refiere a la dirección de destino.

La sintaxis simplificada es la siguiente, donde todos los valores son opcionales, pero se debe especificar al menos uno:

```
RULE=IP-origen:puerto-origen,IP-destino:puerto-destino
```

En general la interpretación sigue cuatro simples principios:

1. Cualquier dirección IP o red que se coloque **antes de la coma** se considera dirección IP o red de **origen**.

2. Cualquier dirección IP o red que se coloque **después de la coma** se considera dirección IP o red de **destino**.

3. Cualquier puerto **antes de la coma** se considera el puerto de **origen**.

4. Cualquier puerto especificado **después de la coma** se considera puerto de **destino**.

Ejemplos.

Selección de todo el tráfico **desde** cualquier puerto en cualquier red **hacia** los puertos 25 (SMTP), 465 (SMTPS) y 587 (SMTP Submission) en cualquier red (es decir, controla ancho de banda de correo saliente):

```
RULE=,:25
RULE=,:465
```

```
RULE=,:587
```

Selección de todo el tráfico **desde** los puertos 25 (SMTP), 465 (SMTPS) y 587 (SMTP Submission) en cualquier red **hacia** cualquier puerto en cualquier red (es decir, controla ancho de banda de correo entrante):

```
RULE=:25,
RULE=:465,
RULE=:587,
```

Selección de todo el tráfico **desde** la red 192.168.0.0/24 **hacia** cualquier puerto en cualquier red:

```
RULE=192.168.0.0/24,
```

Selección de todo el tráfico **desde** cualquier puerto en cualquier red **hacia** cualquier puerto en la red 192.168.0.0/24:

```
RULE=,192.168.0.0/24
```

Selección de todo el tráfico **desde** cualquier puerto en la red 192.168.0.0/24 **hacia** el puerto 25 (SMTP) en cualquier red:

```
RULE=192.168.0.0/24,:25
```

Selección de todo el tráfico **desde** el puerto 25 (SMTP) en la red 192.168.0.0/24 **hacia** cualquier puerto en cualquier red:

```
RULE=192.168.0.0/24:25,
```

Selección de todo el tráfico **desde** el puerto 25 (SMTP) en la red 192.168.0.0/24 **hacia** el puerto 25 (SMTP) en cualquier red:

```
RULE=192.168.0.0/24:25,:25
```

Selección de todo el tráfico **desde** el puerto 25 (SMTP) en cualquier red **hacia** cualquier puerto en la red 192.168.0.0/24:

```
RULE=:25,192.168.0.0/24
```

Selección de todo el tráfico **desde** el puerto 25 (SMTP) en cualquier red **hacia** el puerto 25 (SMTP) en la red 192.168.0.0/24:

```
RULE=:25,192.168.0.0/24:25
```

Selección de todo el tráfico **desde** el puerto 80 en cualquier red **hacia** cualquier puerto de cualquier red:

```
RULE=:80,
```

Selección de todo el tráfico **desde** cualquier puerto en el anfitrión 201.161.1.226 **hacia** cualquier puerto en cualquier red:

```
RULE=201.161.1.226,
```

Selección de todo el tráfico **desde** puerto 80 en el anfitrión 201.161.1.226 **hacia** cualquier puerto en cualquier red:

```
RULE=201.161.1.226:80,
```

Selección de todo el tráfico **desde** el puerto 80 (HTTP) en cualquier red **hacia** la red 192.168.0.0/24:

```
RULE=:80,192.168.0.0/24
```

Selección de todo el tráfico **desde** los puerto 20 (FTP-DATA), 21 (FTP) y 80 (HTTP) en cualquier red **hacia** la red 192.168.0.0/24:

```
RULE=:20,192.168.0.0/24
RULE=:21,192.168.0.0/24
RULE=:80,192.168.0.0/24
```

Selección de todo el tráfico **desde** de los puertos 20 (FTP-DATA), 21 (FTP) y 80 (HTTP) en el anfitrión 201.161.1.226 **hacia** la red 192.168.0.0/24:

```
RULE=201.161.1.226:20,192.168.0.0/24
RULE=201.161.1.226:21,192.168.0.0/24
RULE=201.161.1.226:80,192.168.0.0/24
```

34.5. Procedimientos.

Para poder configurar el uso de ancho de banda se requiere determinar primero lo siguiente:

- ¿Cual es el ancho de banda de tráfico entrante (de bajada) de la interfaz pública?
- ¿Cual es el ancho de banda de tráfico saliente (de subida) de la interfaz pública?
- ¿Qué servicios se van a controlar?
- ¿Cuanto ancho de banda para tráfico entrante y saliente se va a destinar a cada servicio?

Considerando el siguiente escenario:

- Servidor con un cortafuegos y un **NAT** compartiendo el acceso hacia Internet.
- Enlace ADSL de 2048 kbps de tráfico entrante y 256 kbps de tráfico saliente, a través de la interfaz **eth0**.
- Red local 192.168.0.0/24 accede desde la interfaz **eth1**.

- Se quiere gestionar el uso de ancho de banda para SMTP, POP3, IMAP, HTTP, HTTPS, FTP y SSH/SFTP.

- Al repartir el ancho de banda, se el 50% del ancho de banda de entrada a **HTTP** y **HTTPS**, y se dará el 50% del ancho de banda de subida a los servicios relacionados con el **correo electrónico**.

Como ejemplo, se asignarán los siguientes anchos de banda para cada servicio específicado.

Servicios	Puertos	Tráfico entrante	Tráfico saliente
Correo electrónico: SMTP, POP3 e IMAP	25, 465, 587, 110, 143, 993, 995	512Kbit	128Kbit
HTTP y HTTPS	80, 443	1024Kbit	64Kbit
FTP y SSH/SFTP	20, 21, 22	256Kbit	64Kbit

34.5.1. CBQ sin compartir ancho de banda entre clases.

En el ejemplo los anchos de banda se están asignando pensando en que se hará uso de todos los servicios de forma simultánea y que se quiere que cada servicio respete el ancho de banda de los otros, es decir, sin prestar ancho de banda de una clase a otra.

Con la finalidad de facilitar la organización, se recomienda crear ficheros independientes para cada política. Es decir, destinar un fichero para todo lo relacionado con correo, otro para lo relacionado con HTTP/HTTPS y otro relacionado con FTP.

Contenido de fichero /etc/sysconfig/cbq/cbq-0002.smtp-in:

```
DEVICE=eth0,2048Kbit
RATE=512Kbit
WEIGHT=204Kbit
PRIO=5
RULE=:25,192.168.0.0/24
RULE=:465,192.168.0.0/24
RULE=:587,192.168.0.0/24
RULE=:110,192.168.0.0/24
RULE=:143,192.168.0.0/24
RULE=:993,192.168.0.0/24
RULE=:995,192.168.0.0/24
```

Contenido de fichero /etc/sysconfig/cbq/cbq-0003.web-in:

```
DEVICE=eth0,2048Kbit
RATE=1024Kbit
WEIGHT=204Kbit
PRIO=5
RULE=:80,192.168.0.0/24
RULE=:443,192.168.0.0/24
```

Contenido de fichero /etc/sysconfig/cbq/cbq-0005.ftp-in:

```
DEVICE=eth0,2048Kbit
RATE=265Kbit
WEIGHT=204Kbit
PRIO=5
RULE=:20,192.168.0.0/24
RULE=:21,192.168.0.0/24
RULE=:22,192.168.0.0/24
```

Contenido de fichero /etc/sysconfig/cbq/cbq-0002.smtp-out:

```
DEVICE=eth0,2048Kbit
RATE=128Kbit
WEIGHT=204Kbit
PRIO=5
RULE=192.168.0.0/24,:25
RULE=192.168.0.0/24,:465
RULE=192.168.0.0/24,:587
RULE=192.168.0.0/24,:110
RULE=192.168.0.0/24,:143
RULE=192.168.0.0/24,:993
RULE=192.168.0.0/24,:995
```

Contenido de fichero /etc/sysconfig/cbq/cbq-0004.web-out:

```
DEVICE=eth0,2048Kbit
RATE=64Kbit
WEIGHT=204Kbit
PRIO=5
RULE=192.168.0.0/24,:80
RULE=192.168.0.0/24,:443
```

Contenido de fichero /etc/sysconfig/cbq/cbq-0006.ftp-out:

```
DEVICE=eth0,2048Kbit
RATE=64Kbit
WEIGHT=204Kbit
PRIO=5
RULE=192.168.0.0/24,:20
RULE=192.168.0.0/24,:21
RULE=192.168.0.0/24,:22
```

34.5.2. CBQ compartiendo ancho de banda entre clases.

En el ejemplo los anchos de banda se están asignando pensando en que se hará uso de todos los servicios de forma simultánea y que se quiere que cada servicio preste ancho de banda sin utilizar desde una clase hacia otra. Se utilizará a las clases con mayor ancho de banda disponible como las clases padre.

Con la finalidad de facilitar la organización, se recomienda crear ficheros independientes para cada política. Es decir, destinar un fichero para todo lo relacionado con correo, otro para lo relacionado con HTTP/HTTPS y otro relacionado con FTP.

Contenido de fichero /etc/sysconfig/cbq/cbq-0002.smtp-in:

```
DEVICE=eth0,2048Kbit
RATE=512Kbit
WEIGHT=204Kbit
PRIO=5
PARENT=100
LEAF=sfq
RULE=:25,192.168.0.0/24
RULE=:465,192.168.0.0/24
RULE=:587,192.168.0.0/24
RULE=:110,192.168.0.0/24
RULE=:143,192.168.0.0/24
RULE=:993,192.168.0.0/24
RULE=:995,192.168.0.0/24
```

Contenido de fichero /etc/sysconfig/cbq/cbq-0003.web-in:

```
DEVICE=eth0,2048Kbit
RATE=1024Kbit
WEIGHT=204Kbit
PRIO=5
PARENT=100
LEAF=no
BOUNDED=no
ISOLATED=no
RULE=:80,192.168.0.0/24
RULE=:443,192.168.0.0/24
```

Contenido de fichero /etc/sysconfig/cbq/cbq-0005.ftp-in:

```
DEVICE=eth0,2048Kbit
RATE=265Kbit
WEIGHT=204Kbit
PRIO=5
PARENT=100
LEAF=sfq
RULE=:20,192.168.0.0/24
RULE=:21,192.168.0.0/24
RULE=:22,192.168.0.0/24
```

Contenido de fichero /etc/sysconfig/cbq/cbq-0002.smtp-out:

```
DEVICE=eth0,2048Kbit
RATE=128Kbit
WEIGHT=204Kbit
PRIO=5
PARENT=200
LEAF=no
BOUNDED=no
ISOLATED=no
RULE=192.168.0.0/24,:25
RULE=192.168.0.0/24,:465
RULE=192.168.0.0/24,:587
RULE=192.168.0.0/24,:110
RULE=192.168.0.0/24,:143
RULE=192.168.0.0/24,:993
RULE=192.168.0.0/24,:995
```

Contenido de fichero /etc/sysconfig/cbq/cbq-0004.web-out:

```
DEVICE=eth0,2048Kbit
RATE=64Kbit
WEIGHT=204Kbit
PRIO=5
PARENT=200
LEAF=sfq
RULE=192.168.0.0/24,:80
RULE=192.168.0.0/24,:443
```

Contenido de fichero /etc/sysconfig/cbq/cbq-0006.ftp-out:

```
DEVICE=eth0,2048Kbit
RATE=64Kbit
WEIGHT=204Kbit
PRIO=5
PARENT=200
LEAF=sfq
RULE=192.168.0.0/24,:20
RULE=192.168.0.0/24,:21
RULE=192.168.0.0/24,:22
```

34.5.3. Iniciar, detener y reiniciar el servicio cbq.

El guión de inicio de cbq está instalado como **/sbin/cbq**. Es necesario copiar este fichero dentro de **/etc/init.d/** y tratarlo igual que cualquier otro servicio del sistema.

```
cp -a /sbin/cbq /etc/init.d
```

Para probar que las clases están correctas antes de utilizar éstas, puede recurrir a:

```
service cbq compile
```

Para ejecutar por primera vez el servicio **cbq**, utilice:

```
service cbq start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service cbq restart
```

Para detener el servicio **cbq** y eliminar de memoria todas las reglas utilice:

```
service cbq stop
```

Para supervisar las estadísticas de tráfico gestionado a través de **cbq** utilice:

```
service cbq stats
```

34.5.4. Agregar el servicio cbq al arranque del sistema.

Para hacer que el servicio de **cbq** esté activo con el siguiente inicio del sistema, en todos los niveles de ejecución (2, 3, 4, y 5), se utiliza lo siguiente:

```
chkconfig cbq on
```

35. Introducción a SELinux en CentOS 5 y Fedora.

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

35.1. Introducción.

Suele ocurrir que al intentar mejorar el rendimiento de un sistema se recurra a la práctica de desactivar SELinux. Ciertamente consume bastantes recursos, pero brinda un nivel de seguridad superior que en un futuro, que esperemos sea muy lejano, podría ser de gran utilidad para impedir ataques dirigidos específicamente hacia GNU/Linux. La gran popularidad que están teniendo las computadoras ultra-portátiles está incrementando el número de usuarios de GNU/Linux, lo cual eventualmente también significará que irá surgiendo equipamiento lógico malicioso (*malware*) específicamente diseñado para GNU/Linux. A continuación explico, **de forma breve**, como utilizar de manera básica **getsebool** y **setsebool** (y un poco de **chcon**) en CentOS 5 (aplicable a Red Hat Enterprise Linux 5) y Fedora, desde la terminal, ejemplificando políticas para algunos servicios.

35.2. ¿Qué es SELinux?

SELinux (del inglés **S**ecurity-**E**nhanced **Linux**, que se traduce como Seguridad Mejorada de Linux) es una implementación de seguridad para GNU/Linux que provee una variedad de políticas de seguridad, incluyendo el estilo de acceso a los controles del Departamento de Defensa de EE.UU., a través del uso de módulos de Seguridad en el núcleo de Linux.

En si es una colección de parches que fueron integrados hace algunos años al núcleo de Linux, fortaleciendo sus mecanismos de control de acceso y forzando la ejecución de los procesos dentro de un entorno con los mínimos privilegios necesarios. Utiliza un modelo de seguridad de control de acceso obligatorio.

Es una implementación compleja y robusta que suele ser muy oscura para la mayoría de los usuarios. Debido a ésto, falta de documentación amistosa y que muchos servicios simplemente son imposibles de operar sin una política correspondiente, muchas personas suelen desactivarlo editando **/etc/sysconfig/selinux**. El objetivo de este artículo es servir como una breve introducción a los conceptos básicos de administración de SELinux.

35.3. Mandato getsebool.

Este mandato permite listar políticas en SELinux, y determinar si están activos o inactivos. Básicamente se utiliza de la siguiente forma:

```
getsebool -a |grep cadena
```

Donde *cadena* es una cadena de texto que se puede utilizar para localizar las políticas relacionados con algún servicio en particular. Por ejemplo, si se desea conocer que políticas que incluyan la cadena ftp están activos, como **root** se puede utilizar lo siguiente:

```
getsebool -a |grep ftp
```

Lo anterior debe regresar algo similar como lo siguiente:

```
allow_ftpd_anon_write --> off
allow_ftpd_full_access --> off
allow_ftpd_use_cifs --> off
allow_ftpd_use_nfs --> off
ftp_home_dir --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
```

35.4. Mandato setsebool.

Setsebool permite cambiar los valores para diferentes políticas de SELinux, mismas que pueden verse a través de el mandato **getsebool**. La sintaxis básica es la siguiente:

```
setsebool nombre_politica valor
```

Cuando se ejecuta de la manera anteriormente descrita, las políticas son aplicadas de inmediato y estarán vigentes hasta el siguiente reinicio del sistema. Para hacer permanentes las políticas, se utiliza el mismo mandato con la opción **-P**:

```
setsebool -P nombre_politica valor
```

A continuación se muestran algunos ejemplos de gestión de políticas para varios servicios.

[page_break]

35.4.1. Servicios de FTP.

Para el servicio de FTP, como sería a través de VSFTPD, interesan las siguientes políticas:

- allow_ftpd_anon_write: Permite a los usuarios anónimos poder escribir en el servidor.
- allow_ftpd_full_access: Permite lectura y escritura sobre todos los ficheros disponibles desde el servidor.
- allow_ftpd_use_cifs: Permite transferencias de datos desde CIFS.
- allow_ftpd_use_nfs: Permite transferencias de datos desde NFS
- ftp_home_dir: Permite a los usuarios locales poder acceder a sus directorios de inicio.

Para activar estas, se utiliza el mandato **setsebool** con el nombre de la política y el valor 0 o bien 1 para desactivar o activar, respectivamente. En el siguiente ejemplo se activa poder acceder a los directorios de inicio de los usuarios:

```
setsebool ftp_home_dir 1
```

Lo anterior permitiría que los usuarios puedan acceder a sus propios directorios de inicios a través de VSFTPD, hasta que el sistema sea reiniciado. Para hacer permanente el cambio, se utiliza **setsebool** con la opción **-P**, de ls siguiente manera:

```
setsebool -P ftp_home_dir 1
```

35.4.2. OpenVPN.

Otro típico ejemplo es del OpenVPN, como cliente y servidor. Existen dos políticas:

- openvpn_enable_homedirs: Permite utilizar certificados almacenados en los directorios de los usuarios.
- openvpn_disable_trans: Por omisión, SELinux impide utilizar OpenVPN como servidor. Esta política permite desactiva toda gestión de SELinux sobre OpenVPN , pero permite a éste funcionar como servidor.

Para la política de **openvpn_enable_homedirs**, bajo algunas circunstancias se necesita permitir a los usuarios poder conectarse a redes VPN utilizando certificados que el mismo usuario almacena en su directorio de inicio, y esta es precisamente la política que lo permite. Con el nivel de seguridad por omisión, solo se podrían utilizar certificados definidos por el administrador en algún directorio del sistema.

35.4.3. Apache.

Cuando se trabaja con directorios que serán accedidos desde redes públicas, como un directorio virtual o un directorio para dominio virtual en Apache, se activa la política **httpd_enable_homedirs** y se utiliza el mandato **chcon** para permitir el acceso a los directorios ~/public_html, añadiendo el tipo httpd_sys_content_t.

```
setsebool -P httpd_enable_homedirs 1
chcon -R -t httpd_sys_content_t ~user/public_html
```

Para permitir la ejecución de programas CGI, se utiliza:

```
setsebool -P httpd_enable_cgi 1
```

Para permitir enviar correo desde apache, se utiliza:

```
setsebool -P httpd_can_sendmail 1
```

Para desactivar que SELinux controle a Apache, en su totalidad, se puede utilizar:

```
setsebool -P httpd_disable_trans 1
```

35.4.4. Samba.

En Samba es común la necesidad de permitir a este servicio operar como controlador de dominio. La política que lo habilita es **samba_domain_controller**:

```
setsebool -P samba_domain_controller
```

Si se desea permitir el acceso a los directorios de inicio de los usuarios, se utiliza la política **los directorios ~/public_html**:

```
setsebool -P samba_enable_home_dirs on
```

Para poder utilizar directorios que se compartirán a través de Samba, se utiliza chcon definiendo el tipo **samba_share_t** al contexto del directorio. En el siguiente ejemplo, se creará un directorio como /var/samba/publico:

```
mkdir -p /var/samba/publico
```

Para visualizar sus contextos en SELinux, se utiliza el mandato **ls** con la opción **-Z**:

```
ls -Z /var/samba/
```

Lo anterior debe devolver una salida como la siguiente:

```
drwxr-xr-x  root root unconfined_u:object_r:var_t:s0   publico
```

Para añadir el tipo **samba_share_t**, se utiliza el mandato chcon de la siguiente manera:

```
chcon -t samba_share_t /var/samba/publico
```

Al volver a visualizar el contexto del directorio con **ls -Z**, deberá devolver una salida como la siguiente:

```
ls -Z
drwxr-xr-x  root root unconfined_u:object_r:samba_share_t:s0 publico
```

Para compartir un directorios en Samba, hay dos políticas que se pueden utilizar:

- samba_export_all_ro: Permite el acceso a directorios compartidos en Samba en modo de solo lectura
- samba_export_all_rw: Permite el acceso a directorios compartidos en Samba en modo de lectura y escritura.

Ejemplo:

```
setsebool -P samba_export_all_rw 1
```

35.4.5. Otros servicios.

En general, todos las políticas de todos los servicios pueden ser gestionadas buscando cuales están relacionadas a través del mandato **getsebool**. Los detalles respecto de qué es lo que hace dada política pueden consultarse a través de las páginas de manual que están instaladas en el sistema. Por ejemplo, para consultar que políticas hay para el servicio NFS, el manual que contiene las descripciones correspondientes es **nfs_selinux**.

```
man httpd_selinux
```

Otros manuales que pueden consultarse en el sistema para diferentes servicios son:

- kerberos_selinux
- named_selinux
- ftpd_selinux
- nis_selinux
- rsync_selinux
- ypbind_selinux

- pam_selinux
- httpd_selinux
- nfs_selinux
- samba_selinux

36. Cómo configurar un servidor DHCP en una LAN

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

36.1. Introducción.

36.1.1. Acerca del protocolo 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

36.1.2. 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/

36.2. Equipamiento lógico necesario.

36.2.1. Instalación a través de yum.

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 dhcp
```

36.2.2. 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
```

36.3. Procedimientos.

36.3.1. SELinux y el servicio dhcpd.

A fin de que SELinux permita al servicio **dhcpd** funcionar normalmente y sin protección alguna, utilice el siguiente mandato.

```
setsebool -P dhcpd_disable_trans 1
```

A fin de que SELinux permita al sistema funcionar normalmente y sin protección alguna como **cliente DHCP**, utilice el siguiente mandato.

```
setsebool -P dhcpc_disable_trans 1
```

36.3.2. 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**): 200.23.51.205, 132.248.81.29 y 148.234.7.30.
- Rango de direcciones IP a asignar de modo dinámico: 192.168.0.11-192.168.0.199
- Dos direcciones IP se asignarán como fijas (192.168.1.252, 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) 00:24:2B:65:54:84, 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.

```
server-identifier proxy.redlocal.net;
ddns-update-style interim;
ignore client-updates;
authoritative;
option ip-forwarding off;
default-lease-time 21600;
max-lease-time 43200;

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 200.23.51.205, 132.248.81.29, 148.234.7.30;
        range 192.168.0.11 192.168.0.199;
        }
        host impresora-laser {
                option host-name "epl5900.redocal.net";
                hardware ethernet 00:24:2B:65:54:84;
                fixed-address 192.168.1.252;
                }
        host servidor {
                option host-name "servidor.redlocal.net";
                hardware ethernet 00:50:BF:27:1C:1C;
                fixed-address 192.168.0.253;
                }
        host proxy {
                option host-name "proxy.redlocal.net";
                hardware ethernet 00:01:03:DC:67:23;
                fixed-address 192.168.0.254;
                }
}
```

36.3.3. 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
```

36.3.4. 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
```

36.3.5. 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
```

36.4. 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 dirección **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
```

36.5. 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
```

37. Cómo configurar vsftpd (Very Secure FTP Daemon)

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

37.1. Introducción.

37.1.1. 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

37.1.2. Acerca del protocolo FTPS.

FTPS (también referido como **FTP/SSL**) es la forma de designar diferentes formas a través de las cuales se pueden realizar transferencias seguras de ficheros a través de **FTP** utilizando **SSL** o **TLS**. Son mecanismos muy diferentes a los del protocolo SFTP (**S**SH **F**ile **T**ransfer **P**rotocol).

Existen dos diferentes métodos para realizar una conexión **SSL/TLS** a través de **FTP**. La primera y más antigua es a través del **FTPS Implícito** (*Implicit FTPS*), que consiste en cifrar la sesión completa a través de los puertos 990 (FTPS) y 998 (FTPS Data), sin permitir negociación con el cliente, el cual deberá conectarse directamente al servidor FTPS con el inicio de sesión **SSL/TLS**. El segundo método, que es el recomendado por el RFC 4217 y el utilizado por **Vsftpd**, es **FTPS Explícito** (*Explicit FTPS* o **FTPES**), donde el cliente realiza la conexión normal a través del puerto 21 y permitiendo negociar opcionalmente una conexión **TLS**.

37.1.3. 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 ciframeinto 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

37.1.4. 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/

37.1.5. 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

37.1.6. 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/

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 vsftpd
```

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 vsftpd
```

37.3. 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.

37.4. Procedimientos.

37.4.1. SELinux y el servicio vsftpd.

SELinux controla varias funciones de el servicio **vsftpd** incrementando el nivel de seguridad de éste.

Para permitir que los usuarios anónimos puedan realizar procesos de escritura sobre el sistema de ficheros, utilice el siguiente mandato:

```
setsebool -P allow_ftpd_anon_write 1
```

Para hacer que SELinux permita al servicio **vsftpd** acceder a los usuarios locales a sus directorios de inicio, utilice el siguiente mandato:

```
setsebool -P allow_ftpd_full_access 1
```

Para permitir que el servicio **vsftpd** pueda hacer uso de sistemas de ficheros remotos a través de CIFS (Samba) o NFS, y que serán utilizados para compartir a través del servicio, utilice cualquiera de los siguientes mandatos:

```
setsebool -P allow_ftpd_use_cifs 1
setsebool -P allow_ftpd_use_nfs 1
```

Para que SELinux permita al servicio **vsftpd** funcionar normalmente, haciendo que todo lo anteriormente descrito en esta sección pierda sentido, utilice el siguiente mandato:

```
setsebool -P ftpd_disable_trans 1
```

37.4.2. Fichero /etc/vsftpd/vsftpd.conf.

Utilice un editor de texto y modifique el fichero **/etc/vsftpd/vsftpd.conf**. A continuación analizaremos los parámetros a modificar o añadir, según se requiera para necesidades particulares.

37.4.3. 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
```

37.4.4. 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
```

37.4.5. 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
```

37.4.6. 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
```

37.4.7. 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
```

37.4.8. 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.
```

37.4.9. 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
```

37.4.10. Control del ancho de banda.

37.4.10.1. 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
```

37.4.10.2. 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
```

37.4.10.3. 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
```

37.4.10.4. 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
```

37.4.11. Soporte SSL/TLS para VFSTPD.

VSFTPD puede ser configurado fácilmente para utilizar 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) a través de un certificado **RSA**.

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/mi-dominio.org
```

Acceder al directorio que se acaba de crear.

```
cd /etc/ssl/mi-dominio.org
```

El certificado se puede generar fácilmente utilizando el siguiente mandato, donde se generará un certificado con estructura **X.509**, algoritmo de ciframiento **RSA** de 1024 kb, sin **Triple DES**, la cual permita iniciar normalmente, sin interacción alguna, al servicio **>vsftpd**, con una validez por 730 días (dos años) en el fichero **/etc/ssl/mi-dominio.org/vsftpd.pem**.

```
openssl req -x509 -nodes -days 730 -newkey rsa:1024 \
-keyout /etc/ssl/mi-dominio.org/vsftpd.pem \
-out /etc/ssl/mi-dominio.org/vsftpd.pem
```

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:

```
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.mi-dominio.org
Email Address []:webmaster@mi-dominio.org
```

Finalmente se añaden las siguiente líneas al final del fichero **/etc/vsftpd/vsftpd.conf**:

```
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=NO
force_local_logins_ssl=NO
```

```
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
rsa_cert_file=/etc/ssl/mi-dominio.org/vsftpd.pem
```

37.4.12. 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 5, Red Hat™ Enterprise Linux 5 y White Box Enterprise Linux 5 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
```

37.4.13. 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
```

37.5. 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
```

37.6. 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.
```

38. Cómo configurar pure-ftpd.

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

38.1. Introducción.

38.1.1. 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

38.1.2. 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/

38.2. Equipamiento lógico necesario.

38.2.1. 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
```

38.3. Procedimientos.

38.3.1. 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.

38.3.1.1. 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
```

38.3.1.2. 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
```

38.3.1.3. 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
```

38.3.1.4. 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
```

38.3.1.5. 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**.

38.3.1.6. 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**.

38.3.1.7. 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.

38.3.1.8. 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
```

38.3.1.9. 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
```

38.3.1.10. 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
```

38.3.1.11. 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.

38.3.1.12. 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
```

38.3.1.13. 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
```

38.3.1.14. 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
```

38.3.1.15. 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
```

38.3.1.16. 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
```

38.3.2. 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 ejecución (2, 3, 4, y 5) se utiliza lo siguiente

```
chkconfig pure-ftpd on
```

38.3.3. 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
```

38.4. 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
```

39. Cómo configurar OpenSSH

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

39.1. Introducción.

39.1.1. 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.

39.1.2. 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.

39.1.3. 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**.

39.1.4. 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/.

39.2. 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
```

39.3. Ficheros de configuración.

/etc/ssh/sshd_config	Fichero central de configuración del servicio **SSH**.

39.4. Procedimientos.

Edite **/etc/ssh/sshd_config**. A continuación se analizarán los parámetros a modificar.

39.4.1. 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
```

39.4.2. 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
```

39.4.3. 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
```

39.4.4. 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
```

39.4.5. 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
```

39.5. 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 ejecución 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 ejecución con servicio de red. Para desactivar el servicio Sshd de los niveles de ejecución 2, 3, 4 y 5, ejecute:

```
chkconfig --level 2345 sshd off
```

39.6. Probando OpenSSH.

39.6.1. 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
```

39.6.2. 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:

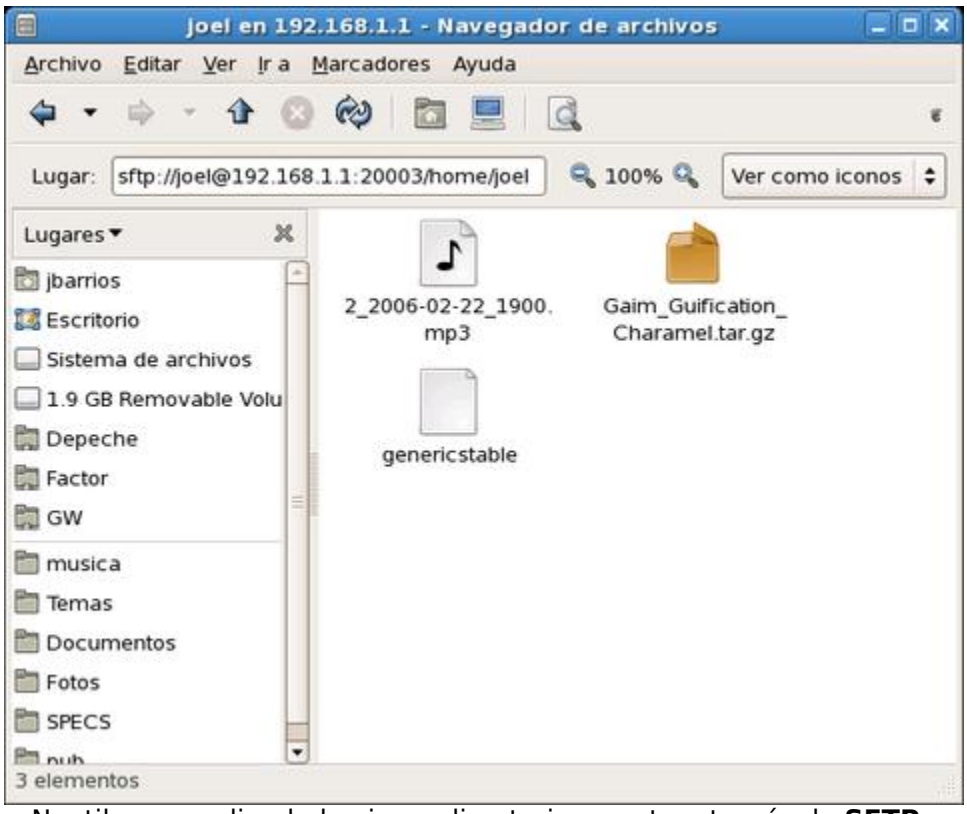
```
sftp usuario@servidor
```

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**.

39.6.3. 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 ./
```

39.7. 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
```

40. Cómo utilizar OpenSSH con autenticación a través de clave pública.

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

40.1. 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.

40.2. Procedimientos

40.2.1. 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
```

40.2.2. Modificaciones en el Cliente.

40.2.2.1. 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.

40.2.3. 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.

41. Cómo configurar OpenSSH con Chroot

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

41.1. 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**.

41.2. 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-*
```

41.3. 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**.

41.3.1. 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.

41.3.2. 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.

Ejemplo del contenido de /etc/passwd dentro de la jaula

```
usuario:x:503:503::/home/usuario:/bin/bash
```

Ejemplo del contenido de /etc/group dentro de la jaula

```
usuario:x:503:
```

41.3.3. 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
```

41.4. 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.

41.4.1. 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:
```

41.4.2. 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
```

41.4.2.1. 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.

42. Cómo configurar NTP.

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

42.1. Introducción.

42.1.1. 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

42.1.1.1. 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

42.1.2. 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

42.2. Equipamiento lógico necesario.

42.2.1. 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
```

42.2.2. 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
```

42.3. Procedimientos.

42.3.1. 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
```

42.3.2. 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
```

42.3.3. 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
```

42.3.4. 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 ejecución (2, 3, 4, y 5), se utiliza lo siguiente:

```
chkconfig ntpd on
```

42.4. 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
```

43. Cómo configurar Clamd.

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

43.1. Introducción.

Clamd es un servicio muy útil que es utilizado para añadir soporte antivirus a diversas implementaciones de servicios en **GNU/Linux**, como **clamdscan** y **samba-vscan**. Permite además utilizar con mejor desempeño la base de datos de firmas digitales de **ClamAV**. La configuración requiere un poco de trabajo, pero el resultado bien vale la pena.

43.2. Instalación de equipamiento lógico necesario.

Si se utiliza **CentOS 5**, se deben configurar los depósitos de **AL Server** para poder instalar **ClamaAV** en el fichero **/etc/yum.repos.d/AL_Server.repo** con el siguiente contenido.

```
[AL-Server]
name=AL Server para Enterprise Linux $releasever
mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server
gpgcheck=1
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

Si se va a utilizar **CentOS 5** con los depósitos de **AL Server**, es importante instalar antes la firma digital de **Alcance Libre**

```
rpm --import http://www.alcancelibre.org/al/AL-RPM-KEY
```

Fedora 10 incluye los paquetes necesarios y firmas digitales en sus depósitos yum, por lo que es innecesario modificar fichero alguno.

Se requiere instalar los paquetes clamav-server, clamav-server-sysv y clamav-update.

```
yum -y install clamav-server clamav-server-sysv clamav-update
```

43.3. Procedimientos.

43.3.1. SELinux y el servicio clamd.

Para que SELinux permita al servicio **clamd** funcionar normalmente, utilice el siguiente mandato:

```
setsebool -P clamd_disable_trans 1
```

43.3.2. Configuración de Clamd.

El fichero **/etc/freshclam.conf** en **Fedora 10** viene con una línea que requiere comentarse para que pueda funcionar el mandato **freshclam**. editar **/etc/freshclam.conf** y comentar la línea 8 del fichero para que quede de la siguiente forma:

```
##
## Example config file for freshclam
## Please read the freshclam.conf(5) manual before editing this file.
##
# Comment or remove the line below.
# Example
```

Este último procedimiento es innecesario para **CentOS 5**, si se utilizan los paquetes de ClamAV de **AL Server**.

Una vez hecho lo anterior, actualizar la base de datos de firmas digitales de virus con el mandato **freshclam**:

```
freshclam
```

Lo anterior puede devolver una salida similar a la siguiente, que por supuesto variará dependiendo de la cantidad de actualizaciones disponibles y la fecha en que se realice el procedimiento.

```
ClamAV update process started at Tue Mar  3 19:43:37 2009
main.cld is up to date (version: 50, sigs: 500667, f-level: 38, builder: sven)
Downloading daily-9052.cdiff [100%]
Downloading daily-9053.cdiff [100%]
Downloading daily-9054.cdiff [100%]
Downloading daily-9055.cdiff [100%]
Downloading daily-9056.cdiff [100%]
Downloading daily-9057.cdiff [100%]
Downloading daily-9058.cdiff [100%]
Downloading daily-9059.cdiff [100%]
Downloading daily-9060.cdiff [100%]
Downloading daily-9061.cdiff [100%]
Downloading daily-9062.cdiff [100%]
Downloading daily-9063.cdiff [100%]
Downloading daily-9064.cdiff [100%]
Downloading daily-9065.cdiff [100%]
daily.cld updated (version: 9065, sigs: 13972, f-level: 38, builder: arnaud)
Database updated (514639 signatures) from database.clamav.net (IP: 199.184.215.2)
```

Copiar el fichero de ejemplo de **clamd.conf** como **/etc/clamd.d/scan.conf**, el cual debe denominarse obligatoriamente como **scan.conf** en la ruta especificada.

```
cp /usr/share/doc/clamav-server-*/clamd.conf /etc/clamd.d/scan.conf
```

Editar **/etc/clamd.d/scan.conf** para configurar opciones.

```
vi /etc/clamd.d/scan.conf
```

De primera instancia, comentar la línea **Example**, que de otro modo impedirá iniciar el servicio.

```
# Comment or remove the line below.
# Example
```

Configurar el fichero de bitácoras, el cual debe denominarse obligatoriamente como **/var/log/clamd.scan**.

```
# Uncomment this option to enable logging.
# LogFile must be writable for the user running daemon.
# A full path is required.
# Default: disabled
LogFile /var/log/clamd.scan
```

Definir que se examinen los ficheros PDF.

```
# This option enables scanning within PDF files.
# Default: no
ScanPDF yes
```

Por motivos de seguridad, especificar que se utilice el usuario **clamav**.

```
# Run as another user (clamd must be started by root for this option to work)
# Default: don't drop privileges
User clamav
```

Definir el zócalo para el servicio:

```
# Path to a local socket file the daemon will listen on.
# Default: disabled (must be specified by a user)
LocalSocket /var/run/clamd.scan/clamd.sock
```

Crear fichero de bitácora, el cual debe pertenecer al usuario y grupo **clamav** y tenga permisos de lectura y escritura para propietario y sol escritura para grupo.

```
touch /var/log/clamd.scan
chown clamav:clamav /var/log/clamd.scan
chmod 0620 /var/log/clamd.scan
```

Copiar el fichero de ejemplo para rotación de bitácoras dentro de **/etc/logrotate.d/**.

```
cp /usr/share/doc/clamav-server-*/clamd.logrotate /etc/logrotate.d/clamd
```

El contenido del fichero **/etc/logrotate.d/clamd** debe ser similar al siguiente:

```
/var/log/clamd.scan {
        monthly
        notifempty
        missingok
        postrotate
                killall -HUP clamd.scan 2>/dev/null || :
        endscript
}
```

Copiar el fichero de ejemplo para sysconfig como **/etc/sysconfig/clamd.scan**. Debe denominarse obligatoriamente como **clamd.scan**

```
cp /usr/share/doc/clamav-server-*/clamd.sysconfig /etc/sysconfig/clamd.scan
```

Editar el fichero **/etc/sysconfig/clamd.scan** para definir variables de entorno a utilizar.

```
vi /etc/sysconfig/clamd.scan
```

El contenido del fichero **debe** ser el siguiente:

```
CLAMD_CONFIGFILE=/etc/clamd.d/scan.conf
CLAMD_SOCKET=/var/run/clamd.scan/clamd.sock
CLAMD_OPTIONS=
```

Copiar el guión de inicio de ejemplo como **/etc/init.d/clamd.scan**. Debe llevar el nombre **clamd.scan** obligatoriamente.

```
cp /usr/share/doc/clamav-server-*/clamd-init /etc/init.d/clamd.scan
```

Editar el fichero **/etc/init.d/clamd.scan**

```
vi /etc/init.d/clamd.scan
```

Debe configurarse el nombre del servicio, obligatoriamente, como **scan** y definirse la ruta del fichero de envoltorio:

```
#!/bin/bash
#
# chkconfig: - 75 25
# description: The clamd server running for locahost
CLAMD_SERVICE=scan
. /usr/share/clamav/clamd-wrapper
```

Añadir el servicio **clamad.scan** a los servicios de arranque del sistema.

```
chkconfig clamd.scan on
```

Crear un enlace simbólico de **/usr/sbin/clamd** hacia **/usr/sbin/clamd.scan**.

```
ln -s /usr/sbin/clamd /usr/sbin/clamd.scan
```

Crear el directorio que será utilizado para el fichero de número de proceso.

```
mkdir -p /var/run/clamd.scan
```

Configurar el directorio anterior como propiedad del usuario y grupo **clamav**:

```
chown clamav:clamav /var/run/clamd.scan
```

Iniciar el servico **clamad.scan**.

```
service clamd.scan start
```

Para añadir el servicio **clamd.scan** a los servicios de arrranque del sistema, solo basta ejecutar:

```
chkconfig clamd.scan on
```

A partir de este punto, se dispondrá de un servicio que trabajará en el trasfondo del sistema y que permitirá utilizar programas como **clamdscan** y **samba-vscan**. Este último es una implementación de antivirus para Samba.

44. Cómo configurar el sistema para sesiones gráficas remotas

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

44.1. 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.

44.2. 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.

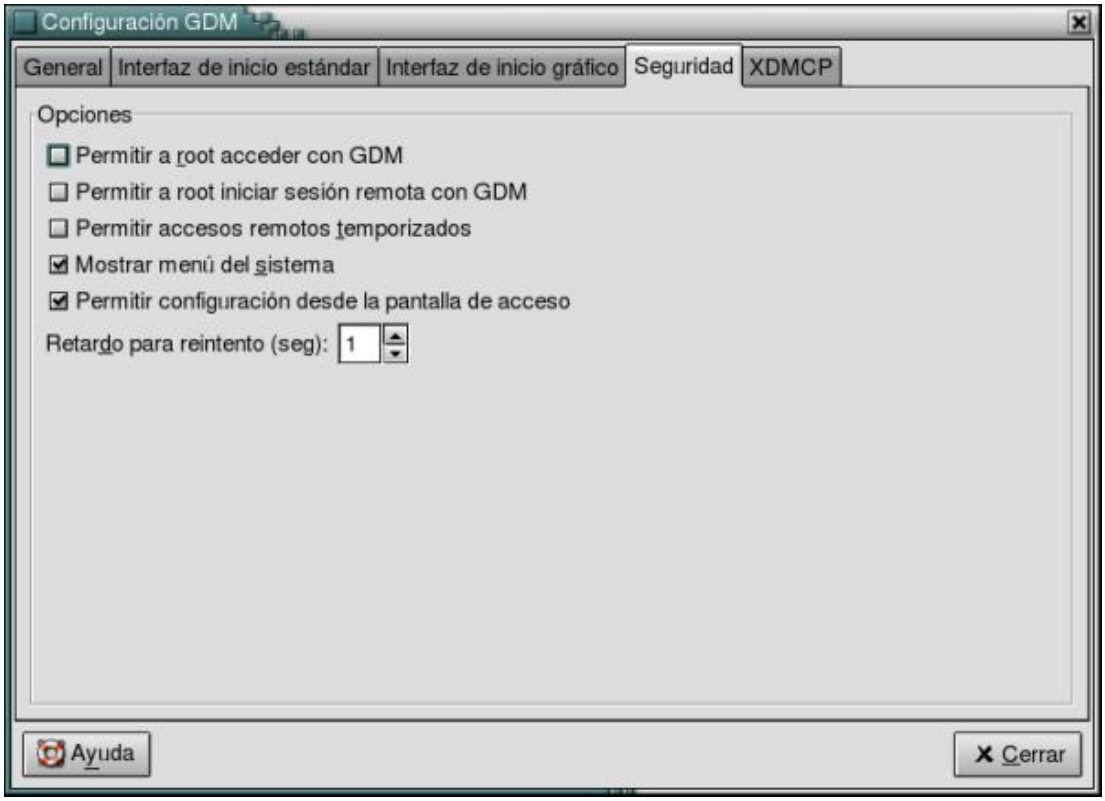
44.2.1. Procedimiento

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 ejecución 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
```

45. Cómo configurar un servidor NFS

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

45.1. 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.

45.2. 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.

45.2.1. Instalación del sustento lógico necesario

```
yum -y install nfs-utils portmap
```

45.3. 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
```

45.3.1. 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 ejecución 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.

45.3.2. 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:

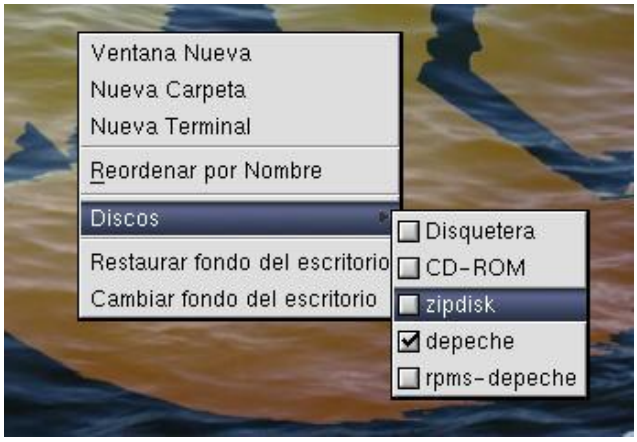
```
cd /mnt/servidornfs
```

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.



45.4. 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.

46. Cómo configurar Samba básico.

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

46.1. Introducción.

46.1.1. 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. *Por mera coincidencia* esto ocurrió por la misma época en que Sun Microsystems hizo 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 travaja 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**.

46.1.2. 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 implementan en sistemas basados sobre UNIX® el protocolo **SMB**. Sirve como reemplazo total para Windows® NT, Warp®, NFS® o servidores Netware®.

46.2. 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 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 o depósitos de equipamiento lógico de la distribución de GNU/Linux utilizada:

- samba: Servidor SMB.
- samba-client: Diversos clientes para el protoclo SMB.
- samba-common: Ficheros necesarios para cliente y servidor.

46.2.1. Instalación a través de yum.

Si utiliza **CentOS 4 y 5**, **Red Hat™ Enterprise Linux 5** o **White Box Enterprise Linux 4 y 5**, y versiones posteriores, solo se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
yum -y install samba samba-client samba-common
```

46.2.2. 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 samba samba-client samba-common
```

46.3. Procedimientos.

46.3.1. SELinux y el servicio smb.

A fin de que SELinux permita al servicio **smb** funcionar como Controlador Primario de Dominio (**PDC**, **P**rimary **D**omain **C**ontroler), utilice el siguiente mandato:

```
setsebool -P samba_domain_controller 1
```

A fin de que SELinux permita al servicio **smb** compartir los directorios de inicio de los usuarios locales del sistema, utilice el siguiente mandato:

```
setsebool -P samba_enable_home_dirs 1
```

Para definir que un directorio será compartido a través del servicio **smb**, como por ejemplo **/var/samba/publico**, y que se debe considerar como contenido tipo Samba, se utiliza el siguiente mandato:

```
chcon -t samba_share_t /var/samba/publico
```

Cada nuevo directorio que vaya a ser compartido a través de Samba, debe ser configurado como acaba de describirse antes de ser configurado en el fichero **/etc/samba/smb.conf**.

A fin de que SELinux permita al servicio **smb** compartir todos los recursos en modo de solo lectura, utilice el siguiente mandato:

```
setsebool -P samba_export_all_ro 1
```

A fin de que SELinux permita al servicio **smb** compartir todos los recursos en modo de lectura y escritura, utilice el siguiente mandato:

```
setsebool -P samba_export_all_rw 1
```

46.3.2. 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 interprete 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 interpete de mandatos para la cuenta de usuario involucrada.

```
useradd -s /sbin/nologin usuario-windows
smbpasswd -a usuario-windows
```

No hace falta se asigne una clave de acceso en el sistema con el mandato **passwd** puesto que la cuenta no tendrá acceso al interprete 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 interprete de mandatos, será necesario especificar **/bin/bash** como interprete de mandatos y además 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
```

46.3.3. El fichero lmhosts

Es necesario empezar resolviendo localmente los nombres **NetBIOS** asociándolos con direcciones IP correspondientes en el fichero **lmhosts** (**L**AN **M**anager **h**osts). Para fines prácticos el nombre *NetBIOS* debe tener un máximo de 11 caracteres. Normalmente se utiliza como referencia el nombre corto del servidor o el nombre corto que se asigno como alias a la interfaz de red. Si se edita el fichero **/etc/samba/lmhosts**, se encontrará un contenido similar al siguiente:

```
127.0.0.1       localhost
```

Se pueden añadir los nombres y direcciones IP de cada uno de los anfitriones de la red local. Como mínimo debe encontrarse el nombre del anfitrión **Samba** y su dirección IP correspondiente, y opcionalmente el resto de los anfitriones de la red local. La separación de espacios se hace con un tabulador. Ejemplo:

```
127.0.0.1       localhost
192.168.1.1     servidor
192.168.1.2     joel
192.168.1.3     blanca
192.168.1.4     jimena
192.168.1.5     regina
192.168.1.6     isaac
192.168.1.7     finanzas
192.168.1.8     direccion
```

46.3.4. Parámetros principales del fichero smb.conf.

Se modifica el fichero **/etc/samba/smb.conf** con cualquier editor de texto. Este información que

será de utilidad y que está comentada con un símbolo **#** y varios ejemplos comentados con **;** (punto y coma), siendo estos últimos los que se pueden tomar como referencia.

46.3.4.1. Parámetro workgroup.

Se establece el grupo de trabajo definiendo el valor del parámetro **workgroup** asignando un grupo de trabajo deseado:

```
workgroup = MIGRUPO
```

46.3.4.2. Parámetro netbios name.

Opcionalmente se puede establecer con el parámetro **netbios name** otro nombre distinto para el servidor si acaso fuese necesario, pero siempre tomando en cuenta que dicho nombre deberá corresponder con el establecido en el fichero **/etc/samba/lmhosts**:

```
netbios name = maquinalinux
```

46.3.4.3. Parámetro server string.

El parámetro **server string** es de carácter descriptivo. Puede utilizarse un comentario breve que de una descripción del servidor.

```
server string = Servidor Samba %v en %L
```

46.3.4.4. Parámetro hosts allow.

La seguridad es importante y esta se puede establecer primeramente estableciendo la lista de control de acceso que definirá que 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 solo se permitirá el acceso dichas máquinas. En el siguiente ejemplo se define la red 192.168.1.0/24 definiendo los tres primeros octetos de la dirección IP de red, así como cualquier dirección IP de la red 127.0.0.0/8 definiendo el primer octeto:

```
hosts allow = 192.168.1. 127.
```

46.3.4.5. Parámetro interfaces.

El parámetro **interfaces** permite establecer desde que 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 se establezcan conexiones desde fuera de la red local.

```
interfaces = lo eth0 192.168.1.254/24
```

46.3.5. Parámetro remote announce.

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 solo en el grupo de trabajo al que pertenece sino también otros grupos de trabajo. El grupo de trabajo de destino puede estar en donde sea mientras exista una ruta y sea posible la difusión exitosa de paquetes.

Los valores que pueden ser utilizados son direcciones IP de difusión (**broadcast**) de la red utilizada (es decir la última dirección IP del segmento de red) y/o nombres de grupos de trabajo. En el siguiente ejemplo se define que el servidor **Samba** se anuncie a través de las direcciones IP de difusión **192.168.1.255** (red **192.168.1.0/24**) y **192.168.2.255** (red **192.168.2.0/24**) y hacia los grupos de trabajo **DOMINIO1** y **DOMINIO2**.

```
remote announce = 192.168.1.255/DOMINIO1 192.168.2.255/DOMINIO2
```

46.3.6. Impresoras en Samba.

Las impresoras se comparten de modo predeterminado, así que solo hay que realizar algunos ajustes. Si se desea que se pueda 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
```

Se pude definir también a un usuario o bien un grupo (**@grupo_que_sea**) para la administración de las colas de las impresoras:

```
        comment = All Printers
        path = /var/spool/samba
        browseable = no
        guest ok = yes
        writable = no
        printable = yes
        public = yes
        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.

46.3.7. 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 ser 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 ser 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 que 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 que usuarios o grupos pueden acceder con permisos administrativos para el recurso. Es decir, podrán acceder hacia el recurso realizando todas las operaciones como super-usuarios. 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 que permiso en el sistema tendrán los subdirectorios creados dentro del recurso. Ejemplos: 1777
create mask	Define que 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 **datos**, el cual está localizado en el directorio **/var/samba/datos** del disco duro. Se permitirá el acceso a cualquiera pero será un recurso de solo lectura salvo para los usuarios administrador y fulano. Todo directorio nuevo que sea creado en su interior tendrá permiso **755** (**drwxr-xr-x**) y todo fichero que sea puesto en su interior tendrá permisos **644** (**-rw-r--r--**.

Primero se crea el nuevo directorio **/var/samba/datos**, utilizando el siguiente mandato:

```
mkdir -p /var/samba/datos
```

Luego se define en SELinux que dicho directorio debe ser considerado como contenido Samba.

```
chcon -t samba_share_t /var/samba/datos
```

Se edita el fichero **/etc/samba/smb.conf** y se añade hasta el final de éste el siguiente contenido:

```
[datos]
```

```
        comment = Directorio de de Datos
        path = /var/samba/datos
        guest ok = Yes
        read only = Yes
        write list = fulano, administrador
        directory mask = 0755
        create mask = 0644
```

46.3.7.1. Ocultando ficheros que inician con punto.

Es poco conveniente que los usuarios puedan acceder 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
```

Este parámetro es particularmente útil para complementar la configuración de los directorios personales de los usuarios.

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   hide dot files = Yes
```

46.4. Iniciar el servicio y añadirlo al arranque del sistema.

Para iniciar el servicio **smb** 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 solo utilice el siguiente mandato:

```
/sbin/chkconfig smb on
```

46.5. Comprobaciones.

46.5.1. Modo texto.

46.5.1.1. Herramienta smbclient.

Indudablemente el método más práctico y seguro es el mandato *smbclient*. Este permite acceder hacía cualquier servidor Samba o Windows®, similar al mandato **ftp** en modo texto.

Para acceder al cualquier recurso de alguna máquina Windows® o servidor SAMBA determine

primero que volúmenes o recursos compartidos posee está. 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
        datos           Disk      datos
        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
```

La 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/DATOS -U fulano
```

Después de ejecutar lo anterior, el sistema solicitará se proporcione la clave de acceso del usuario *fulano* en el equipo denominado *LINUX*.

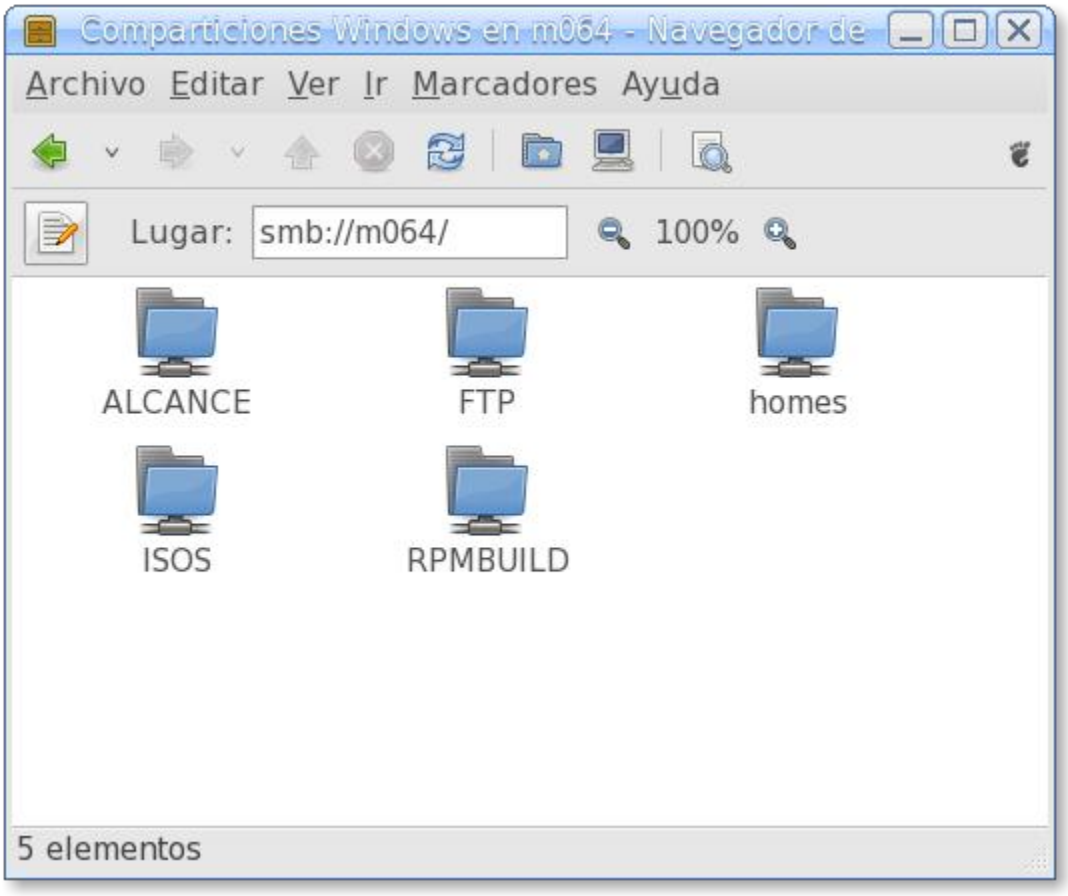
```
smbclient  //LINUX/DATOS -U jbarrios
added interface ip=192.168.1.254 bcast=192.168.1.255 nmask=255.255.255.0
Password:
Domain=[miusuario] OS=[Unix] Server=[Samba 2.2.1a]
smb: >
```

Pueden utilizarse casi los mismos mandatos que en el intérprete de *ftp*, como serían get, mget, put, del, etc.

46.5.2. Modo gráfico

46.5.2.1. Desde el escritorio 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. Solo hay que hacer clic en **Servidores de red** en el menú de GNOME.



46.5.2.2. Desde Windows.

Por su parte, desde Windows deberá ser posible acceder sin problemas hacia **Samba** como si fuese hacia cualquier otra máquina con Windows. Vaya, ni Windows ni el usuario notarán siquiera la diferencia.

47. Cómo configurar Samba denegando acceso a ciertos ficheros.

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

47.1. Introducción.

En algunos casos puede ser necesario denegar el acceso a ciertas extensiones de ficheros, como ficheros de sistema y ficheros de multimedios como MP3, MP4, MPEG y DivX.

Este documento considera que usted ya ha leído previamente, a detalle y en su totalidad el manual «Cómo configurar Samba básico». y que ha configurado exitosamente **Samba** como servidor de archivos.

47.2. Procedimientos.

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»*:

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   hide dot files = Yes
   veto files =  /*Security*/*.tmp/
```

En el siguiente ejemplo, se denegará el acceso hacia los ficheros que tengan las extensiones o terminen en *«.mp3»*, *«.mp4»*, *«.mpeg»* y *«.avi»* en todos los directorios personales de todos los usuarios del sistema:

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   hide dot files = Yes
   veto files =  /*.mp3/*.mp4/*.mpg/*.avi/*.tmp/
```

47.3. Aplicando los cambios.

Para hacer que los cambios hechos surtan efecto tras modificar la configuración, utilice:

```
service smb restart
```

47.4. Comprobaciones.

Con la finalizad de realizar pruebas, genere con el mandato **echo** del sistema un fichero denominado **prueba.mp3**:

```
echo "fichero MP3 de pruebas" > prueba.mp3
```

Si aún no existiera, genere al usuario **fulano**:

```
useradd fulano
```

Utilice el mandato **smbpasswd** y asigne **123qwe** como clave de acceso al usuario **fulano**:

```
smbpasswd -a fulano
```

Acceda con **smbclient** hacia el servidor **Samba** con el usuario **fulano**:

```
smbclient //127.0.0.1/fulano -Ufulano%123qwe
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Domain=[M064] OS=[Unix] Server=[Samba 3.2.0rc1-14.9.el5.al]
smb: >
```

Utilizando el mandato **put** del **intérprete SMB**, suba el fichero **prueba.txt** al directorio personal de fulano:

```
smb: > put prueba.mp3
```

Lo anterior debe devolver una salida similar a la siguiente indicando el mensaje **NT_STATUS_OBJECT_NAME_NOT_FOUND** como respuesta, lo cual indica que no fue permitido subir el fichero **prueba.mp3**:

```
smb: > put prueba.mp3
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file prueba.mp3
smb: >
```

Para salir del **intérprete SMB** utilice el mandato **exit**:

```
smb: > exit
```

48. Cómo configurar Samba con Papelera de Reciclaje.

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

48.1. Introducción.

En algunas circunstancias, es necesario añadir una **Papelera de Reciclaje** (**Recycle Bin**) para evitar la eliminación permanente del contenido de un directorio compartido a través de **Samba**. Es particularmente útil para los directorios personales de los usuario.

Este documento considera que usted ya ha leído previamente, a detalle y en su totalidad el manual «Cómo configurar Samba básico». y que ha configurado exitosamente **Samba** como servidor de archivos.

48.2. Procedimientos

La **Papelera de Reciclaje** se activa añadiendo al recurso a compartir los parámetros **vfs objects** y **recycle:repository** del modo ejemplificado a continuación:

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   vfs objects = recycle
   recycle:repository = Recycle Bin
```

Lo anterior creara el objeto **recycle**, que almacenará los contenidos eliminados desde el cliente en un subdirectorio denominado **Recycle Bin**, el cual es creado si éste no existiera. Si el contenido de **Recycle Bin** es eliminado, éste se hará de forma permanente.

En el caso de directorios compartidos que sean accedidos por distintos usuarios, el subdirectorio **Recycle Bin** se crea con permisos de acceso solo para el primer usuario que elimine contenido. Lo correcto es solo utilizarlo en directorios compartidos que solo sean utilizados por un solo usuario. De ser necesario, se puede cambiar el permiso de acceso del subdirectorio **Recycle Bin** con el mandato **chmod** de **0700** a **1777** para permitir a otros usuarios utilizar éste, tomando en cuenta que de esta forma el contenido conservará los privilegios de cada usuario y los contenidos solo podrán ser eliminados permanentemente por sus propietarios correspondientes.

Se pueden añadir más opciones para lograr un comportamiento más similar al de una **Papelera de Reciclaje** normal en **Windows**. El parámetro **recycle:versions** define que si hay dos o más ficheros con el mismo nombre, y estos son enviados a la **Papelera de Reciclaje**, se mantendrán todos donde los fichero más recientes tendrán un nombre con el esquema «**Copy #x of nombre-**

fichero» (es decir, **Copia #x del nombre-fichero**). El parámetro **recycle:keeptree** define que si se elimina un directorio con subdirectorios y contenido, se mantendrá la estructura de éstos.

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   vfs objects = recycle
   recycle:repository = Recycle Bin
   recycle:versions = Yes
   recycle:keeptree = Yes
```

Se puede definir además que se excluyan ficheros (**recycle:exclude**) y directorios (**recycle:exclude_dir**) de ser enviado a la **Papelera de Reciclaje** cierto tipo de contenido y sea eliminado de forma permanente de inmediato. Las listas para ficheros y directorios son separadas por tuberías (**|**), y aceptan comodines (***** y **?**). En el siguiente ejemplo se excluyen los ficheros con extensiones ***.tmp**, ***.temp**, ***.o**, ***.obj**, **~$***, ***.~??**, ***.log**, ***.trace** y ***.TMP**, y los directorios **/tmp**, **/temp** y **/cache**.

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   vfs objects = recycle
   recycle:repository = Recycle Bin
   recycle:versions = Yes
   recycle:keeptree = Yes
   recycle:exclude = *.tmp|*.temp|*.o|*.obj|~$*|*.~??|*.log|*.trace|*.TMP
   recycle:excludedir = /tmp|/temp|/cache
```

Si no se quiere que se guarden versiones distintas de ficheros con el mismo nombre, para algunas extensiones, es posible hacerlo definiendo el parámetro **recycle:noversions** y una lista de extensiones de ficheros separados por tuberías (**|**). En el siguiente ejemplo, se indica que no se guarden diferentes versiones de ficheros con el mismo nombre que tengan las extensiones ***.doc**, ***.ppt**, ***.dat** y ***.ini**.

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
   vfs objects = recycle
   recycle:repository = Recycle Bin
   recycle:versions = Yes
   recycle:keeptree = Yes
   recycle:exclude = *.tmp|*.temp|*.o|*.obj|~$*|*.~??|*.log|*.trace|*.TMP
   recycle:excludedir = /tmp|/temp|/cache
   recycle:noversions = *.doc|*.ppt|*.dat|*.ini
```

También es posible definir un mínimo y un máximo de tamaño en **bytes** a través de los parámetros **recycle:minsize**, que define un tamaño mínimo, y **recycle:maxsize**, que define un tamaño máximo. Cualquier fichero que esté fuera de estos límites establecidos, será eliminado permanentemente de forma inmediata. En el siguiente ejemplo se define que solo podrán ser enviados a la **Papelera de Reciclaje** los ficheros que tengan un tamaño mínimo de 10 bytes y un tamaño máximo de 5120 bytes (5 MB)

```
[homes]
```

```
comment = Home Directories
browseable = no
writable = yes
hide dot files = Yes
vfs objects = recycle
recycle:repository = Recycle Bin
recycle:versions = Yes
recycle:keeptree = Yes
recycle:exclude = *.tmp|*.temp|*.o|*.obj|~$*|*.~??|*.log|*.trace|*.TMP
recycle:excludedir = /tmp|/temp|/cache
recycle:noversions = *.doc|*.ppt|*.dat|*.ini
recycle:minsize = 10
recycle:maxsize = 5120
```

48.3. Aplicando los cambios.

Para hacer que los cambios hechos surtan efecto tras modificar la configuración, utilice:

```
service smb restart
```

48.4. Comprobaciones.

Con la finalizad de realizar pruebas, genere con el mandato **echo** del sistema un fichero denominado **prueba.txt**:

```
echo "fichero de pruebas" > prueba.txt
```

Si aún no existiera, genere al usuario **fulano**:

```
useradd fulano
```

Utilice el mandato **smbpasswd** y asigne **123qwe** como clave de acceso al usuario **fulano**:

```
smbpasswd -a fulano
```

Acceda con **smbclient** hacia el servidor **Samba** con el usuario **fulano**:

```
smbclient //127.0.0.1/fulano -Ufulano%123qwe
```

Lo anterior debe devolver una salida similar a la siguiente:

```
Domain=[M064] OS=[Unix] Server=[Samba 3.2.0rc1-14.9.el5.al]
smb: >
```

Utilizando el mandato **put** del **intérprete SMB**, suba el fichero **prueba.txt** al directorio personal de fulano:

```
smb: > put prueba.txt
```

Lo anterior debe devolver una salida similar a la siguiente:

```
smb: > put prueba.txt
putting file prueba.txt as prueba.txt (0,4 kb/s) (average 0,4 kb/s)
smb: >
```

Visualice el contenido del directorio actual desde el **intérprete SMB** utilizando el mandato **dir**para verificar que se ha subido el fichero **prueba.txt**:

```
smb: > dir
```

Lo anterior debe devolver una salida similar a la siguiente:

```
smb: > dir
  .                                   D        0  Wed Jun 18 20:44:39 2008
  ..                                  D        0  Wed Jun 18 20:04:14 2008
  .bashrc                             H      124  Wed Jun 18 20:04:14 2008
  .bash_profile                       H      176  Wed Jun 18 20:04:14 2008
  .bash_logout                        H       24  Wed Jun 18 20:04:14 2008
  prueba.txt                          A       19  Wed Jun 18 20:44:39 2008

                34173 blocks of size 524288. 12143 blocks available
smb: >
```

Elimine el fichero **prueba.txt** utilizando el mandato del desde el **intérprete SMB**:

```
smb: > del prueba.txt
smb: >
```

Visualice de nuevo el contenido del directorio con el mandato **dir**, lo cual debe devolver una salida similar a la siguiente donde ha desaparecido el fichero **prueba.txt** y ahora aparece el directorio **Recycle Bin**:

```
smb: > dir
  .                                   D        0  Wed Jun 18 20:52:49 2008
  ..                                  D        0  Wed Jun 18 20:04:14 2008
  .bashrc                             H      124  Wed Jun 18 20:04:14 2008
  .bash_profile                       H      176  Wed Jun 18 20:04:14 2008
  .bash_logout                        H       24  Wed Jun 18 20:04:14 2008
  .zshrc                              H      658  Wed Jun 18 20:04:14 2008
  .kde                               DH        0  Wed Jun 18 20:04:14 2008
  .emacs                              H      515  Wed Jun 18 20:04:14 2008
  Recycle Bin                         D        0  Wed Jun 18 20:52:49 2008

                34173 blocks of size 524288. 12143 blocks available
smb: >
```

Acceda al directorio **Recycle Bin** utilizando el mandato **cd**:

```
smb: > smb: > cd "Recycle Bin"
```

Visualice el contenido con el mandato **dir**, lo cual debe devolver una salida similar a la siguiente donde se muestra que el fichero **prueba.txt**, que fue eliminado con el mandato **del**, ahora está dentro del directorio **Recycle Bin**.

```
smb: Recycle Bin> dir
  .                                   D        0  Wed Jun 18 20:52:49 2008
  ..                                  D        0  Wed Jun 18 20:52:49 2008
  prueba.txt                          A       19  Wed Jun 18 20:44:39 2008

                34173 blocks of size 524288. 12141 blocks available
```

Para salir del **intérprete SMB** utilice el mandato **exit**:

```
smb: Recycle Bin> exit
```

49. Cómo instalar y configurar Samba-Vscan en CentOS 5.

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

49.1. Introducción.

49.2. Acerca de Samba-Vscan.

Samba-Vscan es un interesante módulo desarrollado por **OpenAntivirus**, como una **prueba de concepto** de módulo para el sistema de ficheros virtual de **Samba**. Su desarrollo aún está en fase experimental, pero es lo suficientemente estable para el uso diario, con un mínimo de fallas. Además de **ClamAV**, incluye soprote para otros antivirus como **H+BEDV AntiVir** (versión servidor), **F-Prot Daemon**, **Symantec AntiVirus**, **Kaspersky AntiVirus**, **Trend Micro FileScanner/InterScan VirusWall**, **NAI/McAfee uvscan** y **F-Secure AntiVirus**.

Este documento describe el procedimiento de instalación y configuración de **Samba-Vscan** utilizando **ClamAV** y requiere haber realizado primero los procedimientos descritos en el documento de **Alcance Libre** titulado **«Cómo configurar Clamd»**.

Es importante señalar que **samba-vscan 0.3.6cBeta5** es incompatible con **Samba 3.2.x** y versiones posteriores (**Nota usuarios equipamiento lógico de Alcance Libre:** samba-vscan 0.3.6cBeta5 es compatible con **AL Server**, pero es incompatible con **AL Desktop**).

49.3. Instalación de equipamiento lógico necesario.

Instalar primero los paquetes gcc, glibc-devel, clamav-devel, pcre-devel y **rpm-build**. Este último será utilizado para crear la estructura de directorios de **rpmbuild** y que solo serán necesarios para instalar y preparar los fuentes RPM.

```
yum -y install gcc glibc-devel rpm-build clamav-devel pcre-devel
```

49.4. Procedimientos.

Se debe descargar el paquete de fuentes de Samba de la siguiente forma:

```
wget http://mirrors.kernel.org/centos/5/updates/SRPMS/samba-3.0.28-1.el5_2.1.src.rpm
```

Instalar el código fuente:

```
rpm -ivh samba-3.0.28-1.el5_2.1.src.rpm
```

Cambiarse al directorio de ficheros de especificación:

```
cd /usr/src/redhat/SPECS/
```

Utilizar rpmbuild con las opciones **-bp** para descomprimir los fuentes de Samba.

```
rpmbuild -bp samba.spec
```

Cambiarse al subdirectorio **samba-3.0.28/source/** que se encuentra dentro del directorio de compilación:

```
cd /usr/src/redhat/BUILD/samba-3.0.28/source/
```

Ejecutar **./configure** dentro del directorio **/usr/src/redhat/BUILD/samba-3.0.28/source/**.

```
./configure
```

Lo anterior demorará algunos minutos en completarse.

Ejecutar el mandato **make proto** para compilar lo mínimo necesario para posteriormente compilar **Samba-Vscan**:

```
make proto
```

Cambiarse al directorio **../examples/VFS/**:

```
cd ../examples/VFS
```

Descargar la versión **0.3.6cBeta5** de **Samba-Vscan**.

```
wget http://www.openantivirus.org/download/samba-vscan-0.3.6c-beta5.tar.gz
```

Descomprimir **samba-vscan-0.3.6c-beta5.tar.gz**:

```
tar zxvf samba-vscan-0.3.6c-beta5.tar.gz
```

Cambiarse al directorio **samba-vscan-0.3.6c-beta5/**:

```
cd samba-vscan-0.3.6c-beta5/
```

Ejecutar dentro de este directorio **./configure**:

```
./configure
```

Ejecutar **make clamav**:

```
make clamav
```

Instalar **vscan-clamav.so** en **/usr/lib/samba/vfs/**:

```
install vscan-clamav.so /usr/lib/samba/vfs/
```

Instalar **clamav/vscan-clamav.conf** en **/etc/samba/**:

```
install -m 0644 clamav/vscan-clamav.conf /etc/samba/
```

Es importante mencionar que el procedimiento de compilación de **samba-vscan** debe **repetirse** cada vez que se actualice Samba, de otra manera este servicio dejará de funcionar.

Si se siguió al pie de la letra la configuración de Clamd en el documento de **Alcance Libre** titulado **«Cómo configurar Clamd»**, editar **/etc/samba/vscan-clamav.conf** y definir **/var/run/clamd.localhost/clamd.sock** como zócalo en el parámetro **clamd socket name**.

```
; socket name of clamd (default: /var/run/clamd). Setting will be ignored if
; libclamav is used
clamd socket name = /var/run/clamd
```

También es importante definir un directorio para cuarentena de ficheros infectados a través del parámetro **quarantine directory**. La recomendación es utilizar cualquier otro directorio distinto de **/tmp** y que haya sido creado específicamente para este fin.

```
; where to put infected files - you really want to change this!
quarantine directory  = /tmp
; prefix for files in quarantine
quarantine prefix = vir-
```

Para utilizar **samba-vscan** en la configuración de Samba, se añaden las siguientes dos líneas a cada recurso compartido, definido en el fichero **/etc/samba/smb.conf**, donde se desee utilizar protección con antivirus:

```
vfs object = vscan-clamav
vscan-clamav: config-file = /etc/samba/vscan-clamav.conf
```

Ejemplos:

```
[homes]
        comment = Home Directories
        browseable = yes
        writable = yes
        hide dot files = Yes
        vfs object = vscan-clamav
        vscan-clamav: config-file = /etc/samba/vscan-clamav.conf
[publico]
        comment = Directorio público
        path = /var/samba/publico
        writable = no
        printable = no
        browseable = yes
        public = yes
```

```
        vfs object = vscan-clamav
        vscan-clamav: config-file = /etc/samba/vscan-clamav.conf
```

Para probar, puede utilizarse el fichero de prueba Eicarcom2 a través de **smbclient** o bien interfaz gráfica desde Linux con Nautilus o bien desde Windows con Explorador de Windows, sobre cualquier recurso compartido que haya sido configurado con **Samba-Vscan**.

50. Cómo configurar Samba como cliente o servidor WINS.

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

50.1. Introducción.

WINS (**W**indows **I**nternet **N**ame **S**ervice) es un servidor de nombres de para NetBIOS, que se encarga de mantener una tabla con la correspondencia entre direcciones IP y nombres **NetBIOS** de los equipos que conforman la red local. Esta lista permite localizar rápidamente a otro equipo dentro de la red. Al utilizar un servidor **WINS** se evita el realizar búsquedas innecesarias a través de difusión (**broadcast**) reduciendo sustancialmente el tráfico de red. La resolución de nombres em **Samba**se lleva a cabo realizando consultas en el siguiente orden:

1. Servidor **WINS**
2. Información del fichero **/etc/samba/lmhosts**
3. Información del fichero **/etc/hosts**
4. Difusión (**broadcast**)

Este documento considera que usted ya ha leído previamente, a detalle y en su totalidad el manual «Cómo configurar Samba básico». y que ha configurado exitosamente **Samba** como servidor de archivos.

50.2. Procedimientos.

Todos los parámetros descritos a continuación, se definen en la sección **[global]** del fichero **/etc/samba/smb.conf**.

50.2.1. Parámetros wins server y wins support.

Se puede definir que el servidor **Samba** recién configurado se convierta en un servidor **WINS** o bien utilizar un servidor **WINS** ya existente. **No es posible ser cliente y servidor al mismo tiempo**. Los parámetros **wins server** y **wins support**, que se definen en la sección **[global]** del fichero **/etc/samba/smb.conf**, son mutuamente excluyentes.

Si el sistema va ser utilizado como servidor **WINS**, debe habilitarse el parámetro **wins support** con el valor **yes**:

```
wins support = Yes
```

Si el sistema va a utilizar un servidor **WINS existente**, debe habilitarse el parámetro **wins**

server y como valor se especifica la dirección IP que utilice el servidor **WINS**. En el siguiente ejemplo se define al sistema con dirección IP **192.168.1.1** como servidor **WINS**:

```
wins server = 192.168.1.1
```

50.2.2. Parámetro name resolve order

Define en **Samba** el orden de los métodos a través de los cuales se intentará resolver los nombres NetBIOS. Pueden definirse hasta hasta cuatro valores: wins, lmhosts, hosts y bcast, como se muestra en el siguiente ejemplo.

```
name resolve order = wins lmhosts hosts bcast
```

50.2.3. Parámetro wins proxy.

Cuando su valor es **yes**, permite a **Samba** como servidor intermediario (**proxy**) para otro servidor **WINS**.

```
wins proxy = yes
```

El valor predeterminado de este parámetro es **no**.

50.2.4. Parámetro dns proxy.

Cuando su valor es **yes**, permite a **Samba** realizar búsquedas en un servidor **DNS** si le es imposible determinar un nombre a través de un servidor **WINS**.

```
dns proxy = yes
```

El valor predeterminado de este parámetro es **no**.

50.2.5. Parámetro max ttl.

El parámetro **max ttl** define el máximo tiempo de vida en segundos para los nombres **NetBIOS** que han sido consultados como cliente **WINS** en un servidor **WINS**. su valor predeterminado es **259200**, que corresponde a tres días. **Por lo general no es necesario modificar este parámetro**. Si las direcciones IP de los equipos que integran la red local cambian demasiado frecuentemente, puede reducirse este tiempo. En el siguiente ejemplo, se definen 48 horas como tiempo máximo de vida para los nombres NetBIOS:

```
max ttl = 86400
```

50.2.6. Parámetros max wins ttl y min wins ttl.

Los parámetros **max wins ttl** y **min wins ttl** los tiempos máximo y mínimo en segundos que tendrán de vida los nombres **NetBIOS** que han sido asignados por el servidor **Samba**. El valor predeterminado de **max wins ttl** es **518400**, es decir, 6 días, y el valor predeterminado de **min wins ttl** es **21600**, es decir, 6 horas. **Por lo general no es necesario modificar estos parámetros**. Si las direcciones IP de los equipos que integran la red local cambian muy frecuentemente, pueden modificarse estos tiempos. En el siguiente ejemplo se redundan los

valores predeterminados:

```
max wins ttl = 518400
min wins ttl = 21600
```

50.3. Aplicando los cambios.

Para hacer que los cambios hechos surtan efecto tras modificar la configuración, utilice:

```
service smb restart
```

51. La ingeniería social y los [incorrectos] hábitos del usuario

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

51.1. 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.

52. Configuración básica de Sendmail

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

52.1. Introducción

52.1.1. 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/.

52.1.2. 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/.

52.1.3. 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.

52.1.4. Protocolos utilizados

52.1.4.1. 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.

52.1.4.2. 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.

52.1.4.3. 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.
```

52.2. Equipamiento lógico necesario

- sendmail
- sendmail-cf
- make
- cyrus-sasl

- dovecot (o bien imap)
- m4
- cyrus-sasl-md5
- cyrus-sasl-plain

52.2.1. 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
```

52.2.2. 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
```

52.3. Procedimientos

52.3.1. 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**.

52.3.2. 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
```

52.3.3. 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
```

52.3.4. 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
```

52.3.5. Configuración de funciones de Sendmail

Modificar el fichero **/etc/mail/sendmail.mc** y desactivar o habilitar funciones:

```
vi /etc/mail/sendmail.mc
```

52.3.5.1. 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**.

52.3.5.2. 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
```

52.3.5.3. 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
```

52.3.5.4. 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
```

52.3.5.5. 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
```

52.3.5.6. 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
```

52.3.5.7. 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
```

52.3.6. 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
```

52.3.7. 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
```

52.3.8. 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
```

52.3.9. 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
```

52.4. 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.

52.4.1. 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.

52.4.2. 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
```

52.5. 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.
```

52.6. Pruebas para el envío de correo

52.6.1. 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.
```

52.6.2. 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.
```

52.7. 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

53. Opciones avanzadas de seguridad para Sendmail.

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

53.1. 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. Añadir opciones avanzadas de seguridad se convierte en algo indispensable.

53.2. 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`.

53.2.1. 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
```

53.2.2. 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
```

53.2.3. 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 un spammer. También deshabilita las notificaciones de entrega, el cual es un mecanismo comunmente utilizado por quienes envían correo masivo no solicitado para verificar/confirmar la existencia de una cuenta activa, y hace que el sistema solicite obligatoriamente HELO o EHLO

antes de utilizar el mandato MAIL. Muchos programas de utilizados para enviar correo masivo no solicitado ni siquiera se molestan en utilizar HELO o EHLO. De modo predefinido los valores de confPRIVACY_FLAGS son `authwarnings,novrfy,noexpn,restrictqrun', cambie por lo siguiente:

```
define(`confPRIVACY_FLAGS',`goaway')dnl
```

53.2.4. 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 le 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 (requrerido para MailScanner):

```
define(`confMAX_HEADERS_LENGTH', `16384')dnl
```

El valor sugerido es 16 Kb (16384 bytes). Aumente o disminuya el valor a su discresión.

53.2.5. 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
```

53.2.6. confMAX_DAEMON_CHILDREN

Este parámetro sirve para especificar cuantos procesos hijos se permitirán simultáneamente en el servidor de correo. De modo predefinido sendmail no establece límites para este parámetro. Si se sobre pasa 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
```

53.2.7. confCONNECTION_RATE_THROTTLE

Este parámetro sirve para establecer el numero 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
```

54. Cómo configurar Sendmail y Dovecot con soporte SSL/TLS.

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

54.1. Introducción.

Este documento requiere la lectura y comprensión previa de los siguientes temas:

- Configuración básica de Sendmail.

54.1.1. 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

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.

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
```

54.2.1. Sendmail.

54.2.1.1. 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.*
```

54.2.1.2. 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
```

54.2.1.3. 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.

54.2.2. Dovecot.

54.2.2.1. 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.*
```

54.2.2.2. 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
```

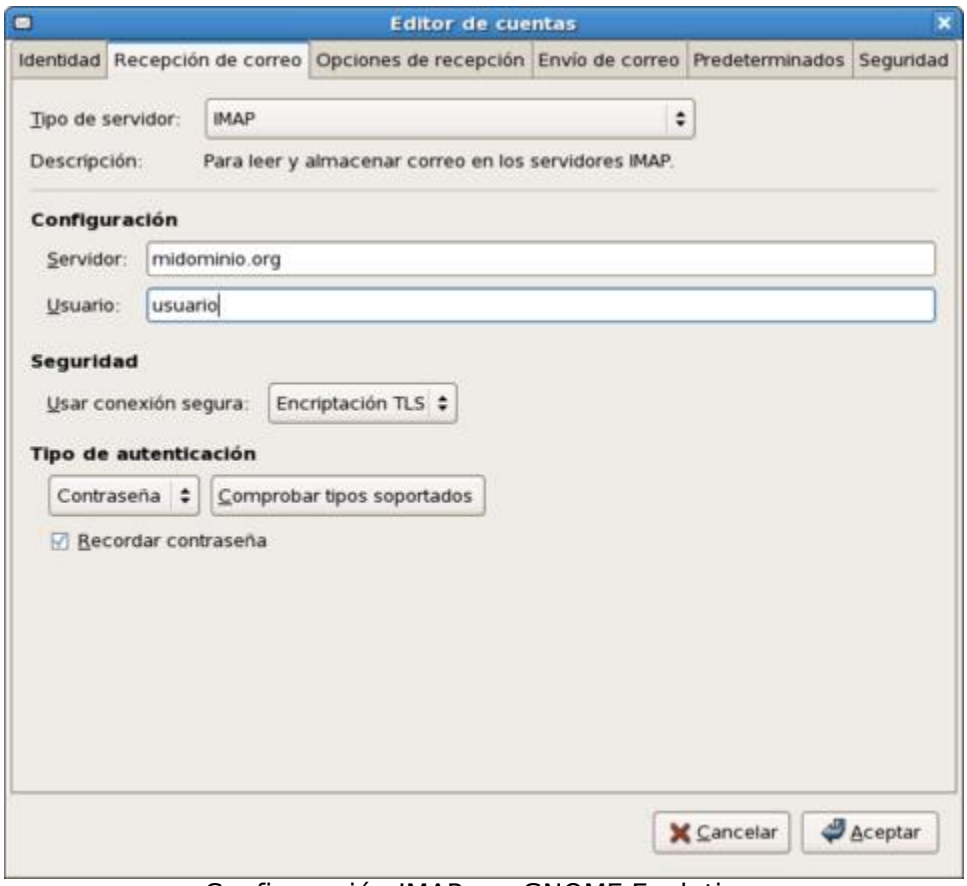
54.2.2.3. Comprobación.

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.

54.2.3. Configuración de GNOME Evolution.

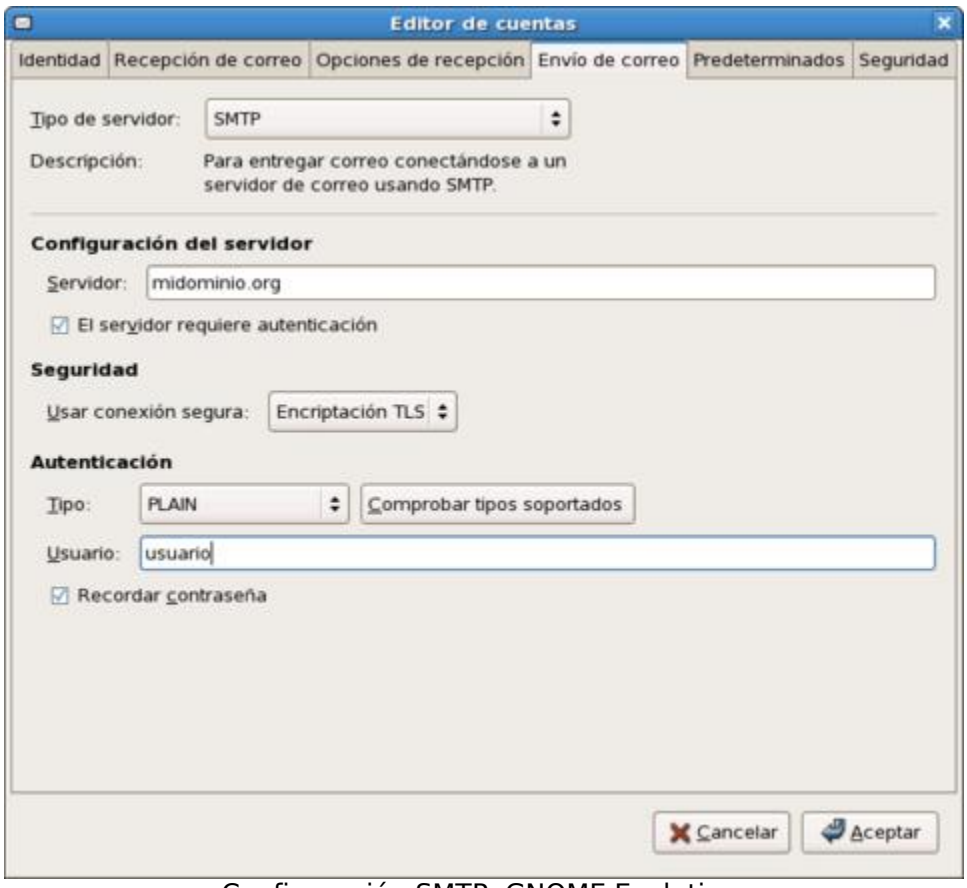
54.2.3.1. Configuración GNOME Evolution.

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.

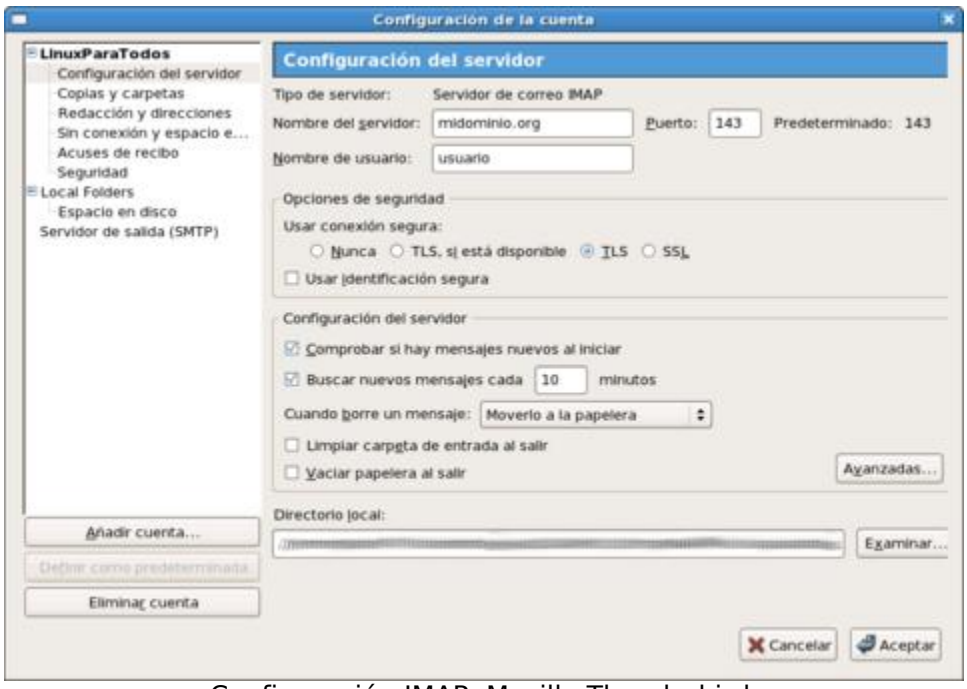
Se hace lo mismo para SMTP.



Configuración SMTP, GNOME Evolution.

54.2.3.2. 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.

54.2.4. 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
```

55. Cómo configurar Cyrus IMAP.

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

55.1. 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/

55.2. 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.

55.2.1. 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
```

55.2.2. 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
```

55.3. 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
```

55.3.1. 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**.

55.3.2. 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
```

55.3.3. 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 ejecución (2, 3, 4, y 5), se utiliza lo siguiente:

```
/sbin/chkconfig cyrus-imapd on
```

55.3.4. 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
```

55.4. 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.
```

56. Instalación y configuración de SquirrelMail (correo a través de interfaz HTTP)

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

56.1. 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.

56.2. Procedimientos

56.2.1. Instalación del sustento lógico necesario

```
yum -y install squirrelmail httpd
```

56.2.2. 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-dominio.org
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».

56.3. 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/
```

56.4. 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.

57. Cómo instalar GroupOffice en CentOS.

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

57.1. ¿Qué es Group Office?

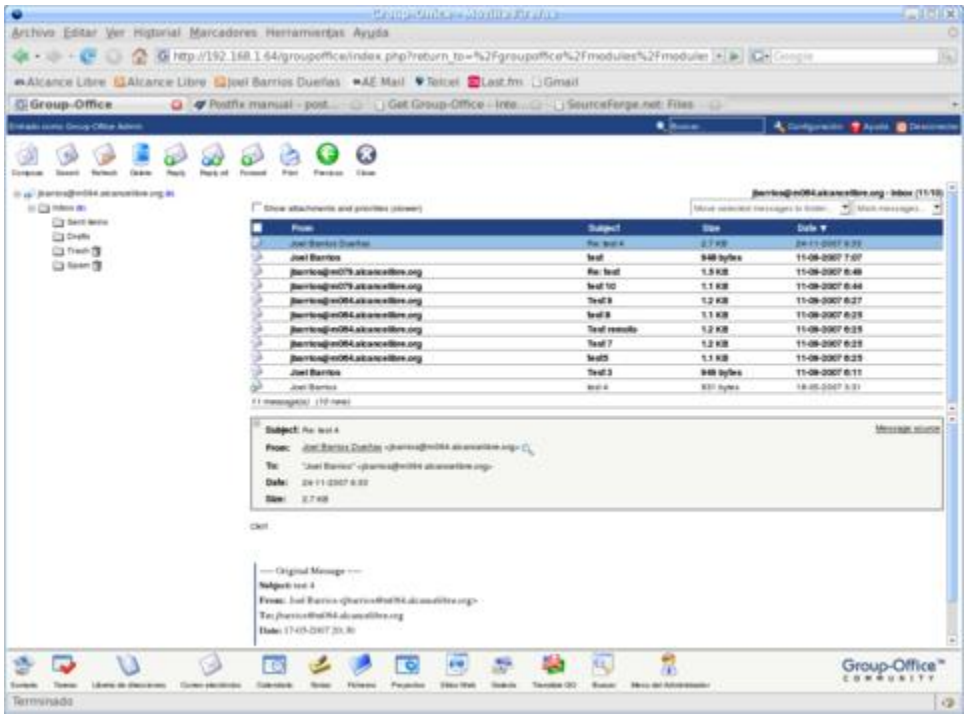
Es un conjunto *Groupware* que puede ajustarse a un amplio rango de audiencia. Ofrece muchas funciones que son importantes para cualquier empresa. Es amistoso con el usuario y se combina con funciones poderosas. Se desarrolló con los siguientes conceptos en mente:

- **Velocidad**: A diferencia de otras alternativas que son pesadas para el sistema y requieren servidores de gran capacidad, **Group Office** está diseñado para ser ligero y trabajar tan rápido como sea posible sin sacrificar funcionalidad (utiliza AJAX).
- **Simplicidad**: La interfaz de usuario está diseñada para ser intuitiva de modo que los usuarios pueden encontrar fácilmente las funciones que necesiten, sin sacrificar funcionalidad.
- **Modularidad**: Es fácil de actualizar gracias a su buen diseño de código. Actualizar no es un calvario.
- **Escalabilidad**: Está diseñado para ser utilizado por uno o por miles de usuarios.

Nota: CentOS 5 y Red Hat Enterprise Linux 5 solo pueden utilizar hasta la versión 2.18.STABLE21, debido a que estos sistemas operativos incluyen la versión 5.1.6 de PHP. Las versiones posteriores de GroupOffice (3.00, 3.01 y 3.02) requieren PHP 5.2, que oficialmente carece de soporte para CentOS 5 y Red Hat Enterprise Linux. La versión 2.18.STABLE21 es sumamente funcional y es ideal para pequeñas y medianas empresas. Se recomienda implementar en servidores con uno o dos microprocesadores con al menos 1 GB RAM para atender cómodamente hasta 25 usuarios, 2 GB RAM para hasta 50 usuarios y 4 GB RAM para hasta 100 usuarios.

Group Office es un muy completo sistema informático colaborativo (*Groupware*), en modalidad HTTP, que incluye un sistema base y diferentes módulos. Éstos últimos están diseñados de la forma en que los grupos de personas pueden colaborar en linea. Incluye como funciones a

calendarios, **libretas de direcciones**, **gestor de proyectos**, **gestor de ficheros** y **correo electrónico**. Los usuarios solo necesitan utilizar cualquier navegador gráfico para acceder a su *Groupware* desde cualquier parte del mundo. Combinado con un servidor GNU/Linux bien configurado, **es una solución completa** para las pequeñas y medianas empresas.



Siguiendo los procedimientos de este documento, es posible implementar fácilmente una aplicación colaborativa (**Groupware**) en menos de 5 minutos.

57.2. Equipamiento lógico necesario.

57.2.1. Configuración de depósitos YUM para CentOS 5 y Red Hat Enterprise Linux 5.

Se pueden utilizar el siguiente depósito YUM para la plataforma Enterprise Linux 5.

```
[AL-Server]
name=Enterprise Linux $releasever - $basearch - AL Server
mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

Instalar el paquete principal y el paquete de instalación utilizando el siguiente mandato:

```
yum -y install groupoffice groupoffice-install
```

57.3. Procedimientos.

1) Crear una base de datos en MySQL

```
mysqladmin -p create groupoffice
```

2) Otorgar privilegios a la nueva base de datos con un usuario y clave de acceso de la siguiente manera:

```
mysql -p
> GRANT all
> ON groupoffice.*
> TO groupoffice@localhost
> IDENTIFIED BY 'clave-de-acceso';
> exit;
```

Lo anterior también permitirá realizar conexiones remotas a MySQL desde cualquier ubicación.

3) Configurar **sudo** para que el usuario **apache** pueda ejecutar los mandatos **/usr/sbin/chpasswd**, **/usr/bin/quota** y **/usr/sbin/edquota**, así como también los ficheros **/usr/share/groupoffice/action.php** y **/usr/share/groupoffice/modules/email/account.php**. Ejecute el siguiente mandato:

```
visudo
```

Y al final de la configuración se añade:

```
apache  ALL=NOPASSWD: /usr/sbin/chpasswd
apache  ALL=NOPASSWD: /usr/bin/quota
apache  ALL=NOPASSWD: /usr/sbin/edquota
apache  ALL=NOPASSWD: /usr/share/groupoffice/action.php
apache  ALL=NOPASSWD: /usr/share/groupoffice/modules/email/account.php
apache  ALL=NOPASSWD: /usr/sbin/useradd
apache  ALL=NOPASSWD: /usr/sbin/userdel
```

Se debe conceder acceso al intérprete de mandatos al usuario apache, utilizado por Apache:

```
usermod -s /bin/bash apache
```

4) Configurar políticas y contextos de SELinux, cuando está habilitado. El directorio **/etc/groupoffice/** varios ficheros de configuración, los cuales se requiere se les asigne contexto para que se le considere como contenido HTTP a fin de que SELinux permita escribir sobre **/etc/groupoffice/config.php** al momento de crear la configuración y acceder hacia otras configuraciones. Ejecute el siguiente mandato:

```
chcon -R -t httpd_sys_content_t /etc/groupoffice/
```

También es necesario cambiar recursivamente el contexto los directorios **/usr/share/groupoffice** y **/var/lib/groupoffice/** a fin de que SELinux considere a este, y sus sub-directorios, como contenido HTTP a fin de permitir del ejecución de PHP en el primero y crear carpetas y almacenar contenidos en el caso segundo. Ejecute los siguientes mandatos:

```
chcon -R -t httpd_sys_content_t /var/lib/groupoffice
chcon -R -t httpd_sys_content_t /usr/share/groupoffice
```

Utilizando lo anterior se puede instalar y trabajar con **GroupOffice** sin necesidad alguna de

desactivar o cambiar a modo permisivo a SELinux, y sin activar las políticas **httpd_disable_trans** ni **mysqld_disable_trans**, las cuales desactivan la protección de SELinux para los servicios **httpd** y **mysqld** correspondientemente.

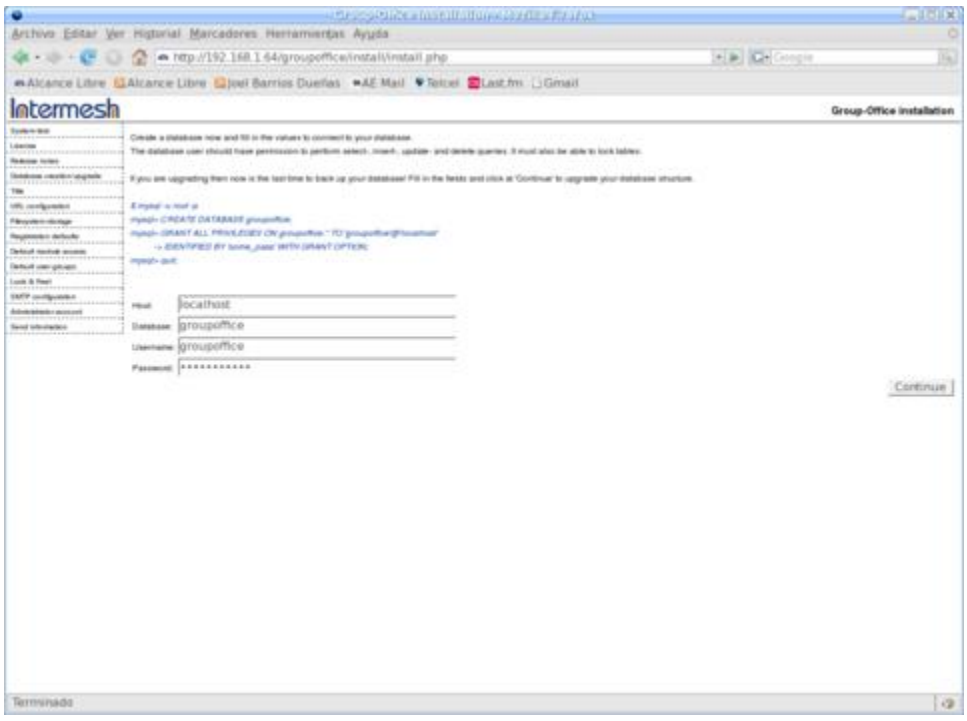
Si el servidor MySQL se encuentras en un servidor distinto, es necesario establecer las políticas **httpd_can_network_connect** y **httpd_can_network_connect_db** para que SELinux permita al servidor **httpd** establecer conexiones hacia servidores remotos. Ejecute los siguientes mandatos:

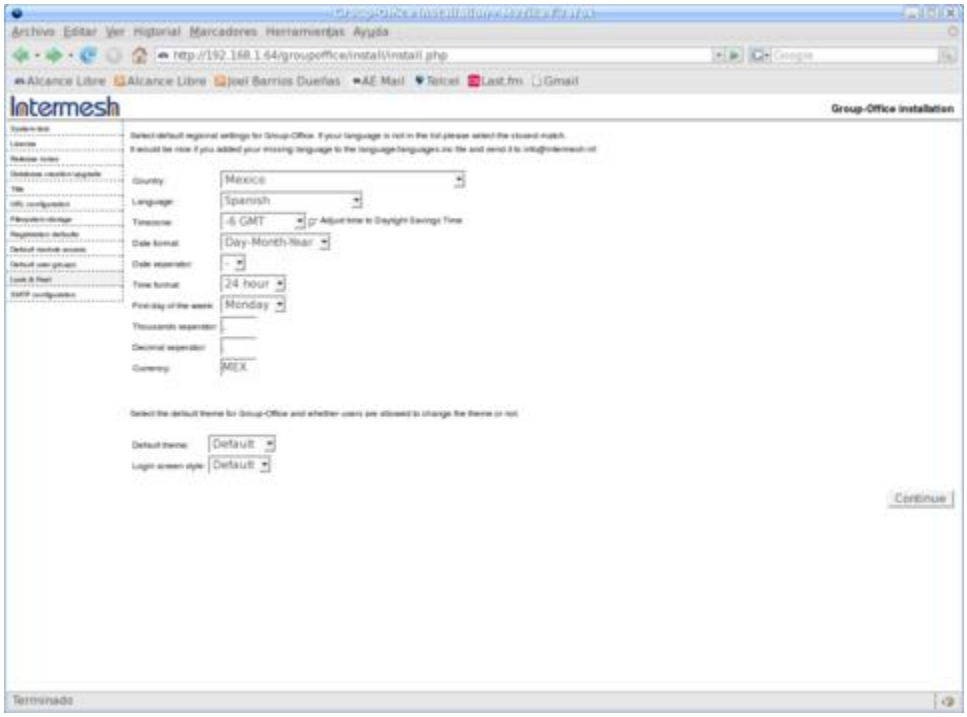
```
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_can_network_connect_db 1
```

5) Recargar el servicio httpd:

```
service httpd reload
```

6) Acceder hacia *http://www.dominio.algo/groupoffice/install/install.php* y configurar únicamente los datos de la base de datos y el usuario y la clave de acceso requeridos, así como los datos regionales como país, moneda y uso horario. En el resto de las pantallas se puede dar clic en los botones de *Continue* (continuar) sin necesidad de realizar cambio alguno, puesto que **todo lo necesario ya viene previamente configurado en el paquete RPM**, excepto los privilegios de acceso a las herramientas.





57.3.1. Ajustes posteriores a la instalación.

57.3.1.1. Corrección del módulo Ficheros.

De ser necesario, hay que corregir instalación del módulo de **Ficheros**. Este se instala incorrectamente en algunos casos, por lo que es necesario crear manualmente las tablas en la base de datos.

```
cd /usr/share/groupoffice/modules/filesystem/sql/
mysql -p groupoffice < filesystem.install.sql
```

57.3.1.2. Modificaciones a la configuración en el fichero /etc/groupoffice/config.php.

Si se edita el parámetro **register_modules_write** del fichero **/etc/groupoffice/config.php**, y se colocan los valores email, calendar, addressbook, todos, projects, cms, filesystem, summary y notes del siguiente modo, los usuarios que se registren a partir de ese momento, tendrán activadas las funciones de correo electrónico, calendario, libreta de direcciones, tareas, CMS, ficheros, proyectos, resumen y notas.

```
$config['register_modules_write']='email,calendar,addressbook,summary,notes';
```

Si se activa la función **allow_registration** del siguiente modo, los usuarios podrán registrarse desde la pantalla de autenticación (requiere que el administrador active las cuentas):

```
$config['allow_registration']=true;
```

Lo anterior también se puede configurar volviendo a acceder a la interfaz de instalación en

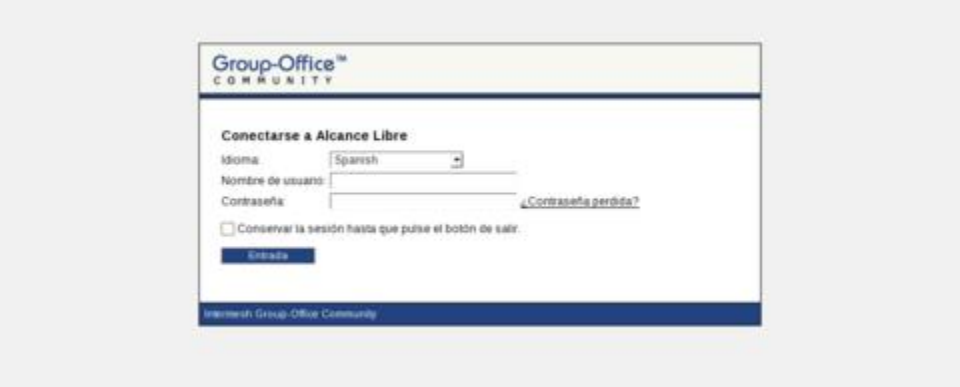
http://www.dominio.algo/groupoffice/install/install.php, misma que permitirá en todo momento realizar cambios.

Si se ha concluido con los ajustes de la configuración, por seguridad, es importante desinstalar el paquete groupoffice-install, mismo que será innecesario en lo sucesivo, salvo que, como se menciona arriba, se requiera modificar desde interfaz HTTP la configuración del acceso hacia la base de datos o cambiar cualquiera de los datos suministrados durante el procedimiento de instalación.

```
rpm -e groupoffice-install
```

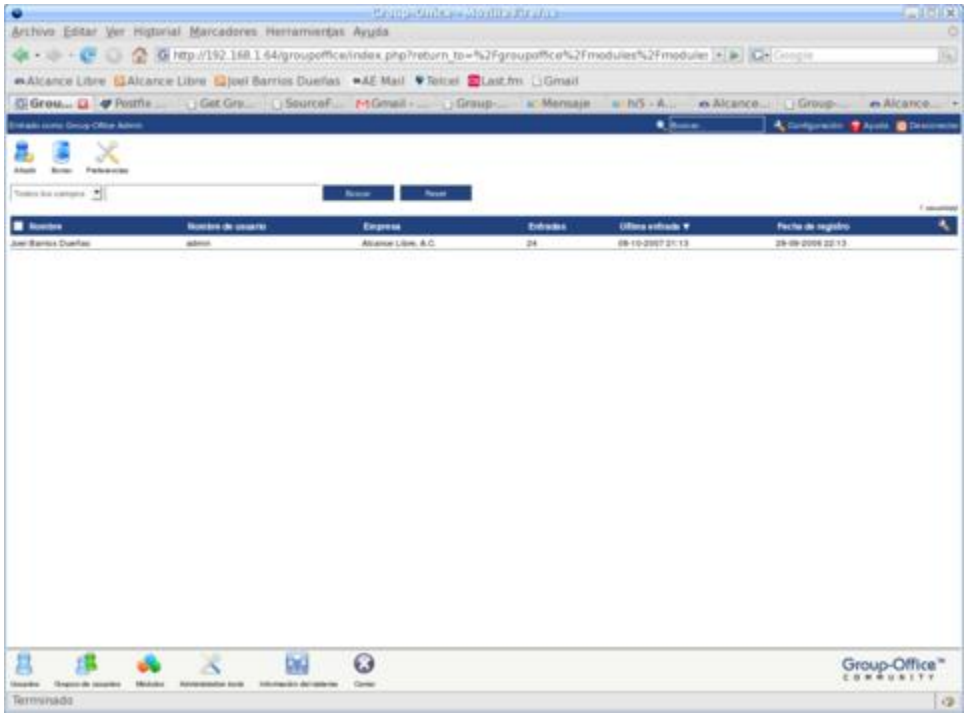
57.3.1.3. Ingresando como administrador.

Se puede ingresar a GroupOffice como administrador desde la pantalla de ingreso en *http://www.dominio.algo/groupoffice/* como el usuario *admin* y la clave de acceso *admin*, todo en minúsculas.

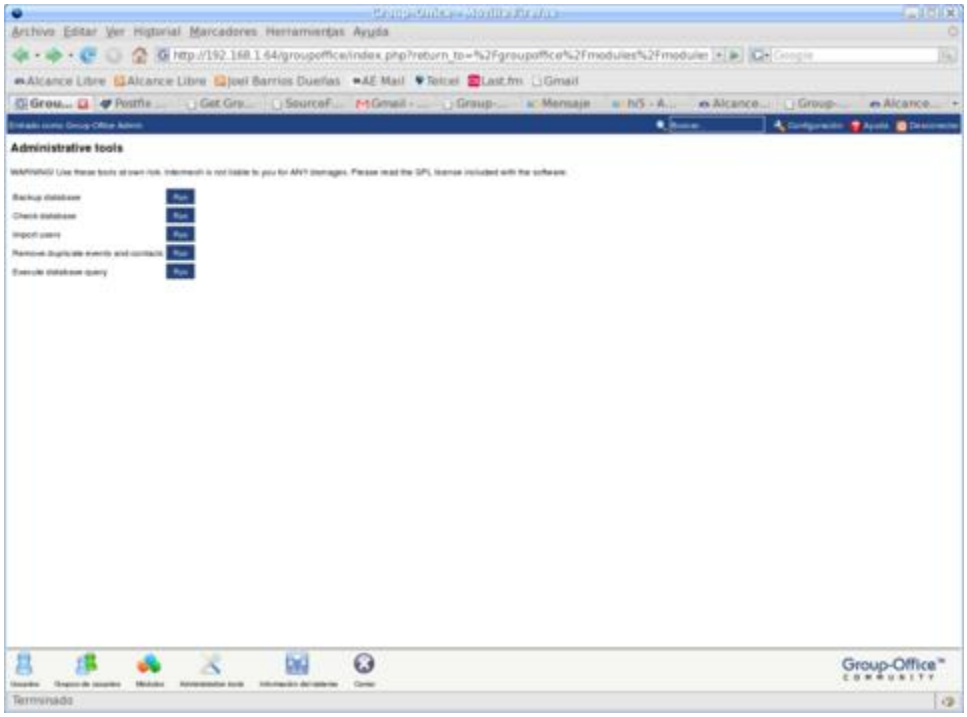


Pantalla de ingreso de GroupOffice.

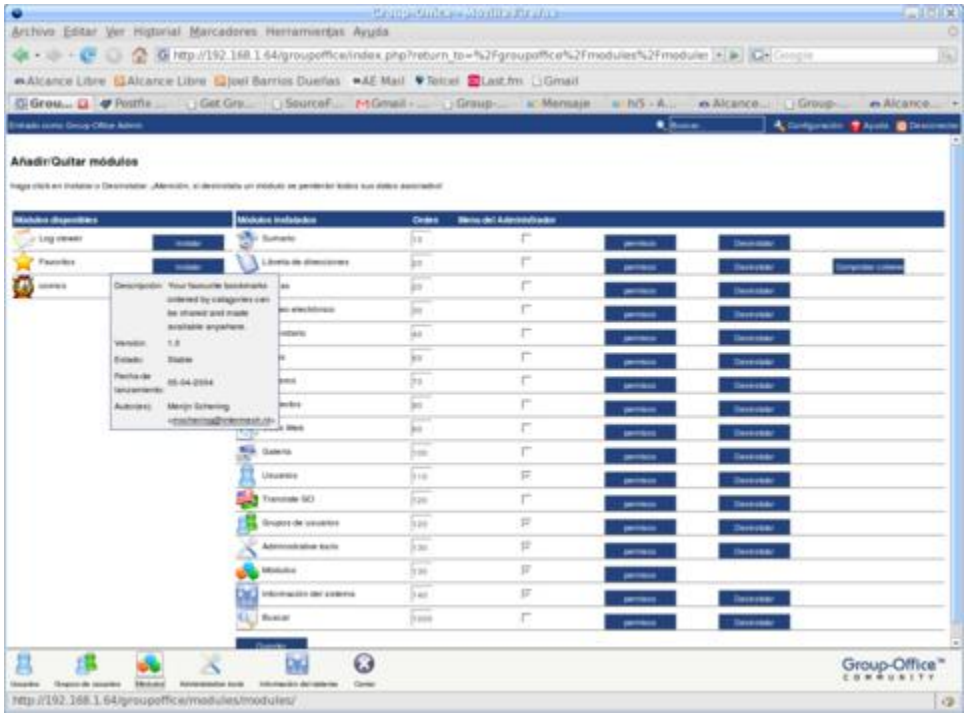
Hecho lo anterior, se podrá personalizar y dar de alta en el *Groupware* a los usuarios, los cuales deben existir previamente en el servidor como cuentas regulares de usuario de correo electrónico. Para dar de alta los usuarios se hace clic en el icono de menú de administración y luego en el icono **Usuarios**.



Lista de usuarios. Desde esta interfaz se dan de alta los usuarios.



Las herramientas administrativas permiten hacer respaldos dela base de datos y verificar integridad de los datos.



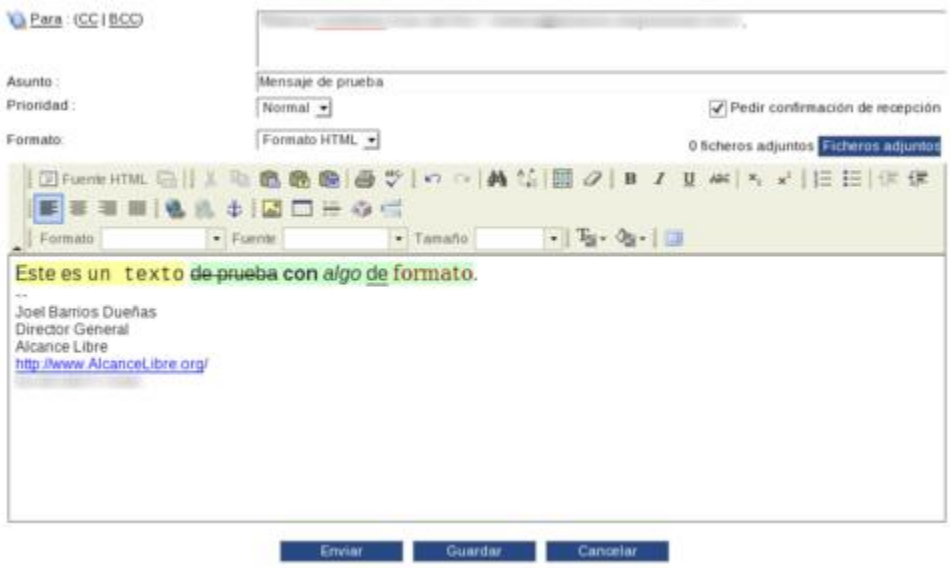
También permite instalar otros complementos y desactivar los complementos que se considere innecesarios.

57.3.1.4. Ingresando como usuario regular.

Cuando se ingrese como usuario regular y se de de alta la cuenta de correo electrónico de éste, es importante rellenar la casilla **No validar el certificado**, salvo que se cuente con un certificado validado por **Verisign** y si éste está configurado en el servidor IMAP. Puede darse de alta más de una cuenta IMAP.

Ventana de configuración de cuenta de correo electrónico del usuario.

La ventana para crear un nuevo mensaje tiene suficientes funciones para cubrir las necesidades de la mayoría de los usuarios. Permite enviar corre electrónico en formato de texto simple y en formato HTML, guardar mensajes como borrador, establecer prioridad y solicitar confirmación de lectura al destinatario.



Ventana de configuración de cuenta de correo electrónico del usuario.

Para compartir la libreta de direcciones o el calendario con otros usuarios, hacer clic en los iconos de cualquiera de éstos, luego hacer clic en el icono **Administrar**, seleccionar y hacer doble clic sobre la entrada de la libreta de direcciones o calendario del usuario, según sea el caso.

Definiendo permisos de lectura en la libreta de direcciones.

Luego se hace clic en la pestaña de **Leer permisos** o **Escribir permisos**. Desde esta interfaz se pueden añadir usuarios a quienes se les comparte la libreta de direcciones o calendario con permisos de solo lectura o permisos de lectura y escritura.

Añadiendo usuarios con permiso de lectura en el módulo **Libreta de Direcciones**.

Para compartir la carpeta del módulo **Ficheros** con otros usuarios, se debe hacer clic en el icono **Ficheros**, luego hacer clic en el icono **Administrar**, y en esta interfaz habilitar la casilla de **Activar compartición**en el módulo **Ficheros**.

Activando compartición en carpeta del módulo **Ficheros**.

Para definir los usuarios a quienes se comparte la carpeta, se hace clic en las pestañas de **Permisos leer** o **Permisos escribir** de la misma forma en que se hace para los módulos de **Calendario** o **Libreta de direcciones**.

Añadiendo usuarios con permiso de lectura y escritura en el módulo **Ficheros**.

58. Apéndice: Enviar correo a todos los usuarios del sistema

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

58.1. 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.

58.2. 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*.

59. Cómo instalar y configurar el programa vacation para responder avisos automáticos en vacaciones.

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

59.1. Intrucción.

Vacation es un pequeño pero útil programa que permite configurar cuentas de correo electrónico para que respondan automáticamente con un mensaje que indica que el usuario se encuentra de vacaciones.

59.2. Equipamiento lógico necesario.

59.2.1. Instalación a través de yum.

Proceda a configurar el depósito YUM de Alcance Libre que incluye el paquete modificado de squid con soporte para direcciones MAC:

```
cd /etc/yum.repos.d/
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo
cd -
```

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 vacation
```

59.2.2. Instalación a través de up2date.

Edite el fichero **/etc/sysconfig/rhn/sources**.

```
vim /etc/sysconfig/rhn/sources
```

Añada el siguiente contenido.

```
yum AL-Server http://www.alcancelibre.org/al/server/4/
```

Si se utiliza **Red Hat™ Enterprise Linux 4**, solo bastará realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

```
up2date -i vacation
```

59.3. Procedimientos.

Es indispensable que el usuario tenga acceso al intérprete de mandatos a fin de poder utilizar el programa **vacation**. Asigne como intérprete de mandatos **/bin/bash** o bien **/bin/sh** al usuario:

```
usermod -s /bin/bash usuario
```

Cambie a la sesión del usuario:

```
su -l usuario
```

Utilice vim para crear el fichero **~/.vacation.msg**:

```
vim ~/.vacation.msg
```

Pulse la tecla **Insert**.

Coloque dentro del fichero un contenido similar al siguiente, evitando utilizar acentos y la letra ñ:

```
Subject: Estoy de vacaciones.
From: como se llame <usuaario@mi-dominio.com.mx>
Reply-To: como se llame <usuaario@mi-dominio.com.mx>
Buen dia, por el momento no me encuentro en la oficina, estoy de regreso el
proximo DD de MMMM de AAAA.

Reciba un cordial saludo.

Atentamente
Lic. como se llame

NOTA: Mensaje *intencionalmente* enviado sin acentos.
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

Utilice vim para crear el fichero **~/.forward**:

```
vim ~/.forward
```

Pulse la tecla **Insert**.

Añada el siguiente contenido, tomando en cuenta que la omisión de la barra invertida (\) al inicio hará que el programa **vacation** falle irremediablemente:

```
\usuario, "|/usr/bin/vacation usuario"
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

Cambie los permisos del fichero para que solo permitan la lectura y escritura al usuario propietario de éste.

```
chmod 600 ~/.forward
```

Como usuario ejecute el siguiente mandato, a fin de iniciar el programa.

```
vacation -I
```

Salga de la sesión del usuario.

```
exit
```

A partir de este momento, todo el correo electrónico que se envié a la cuenta del usuario, será respondido automáticamente con un aviso que incluirá el texto definido en el fichero **/home/usuario/.vacation.msg**.

Para desactivar el programa, solo es necesario ingresar nuevamente al sistema como **root** y eliminar o renombrar el fichero **/home/usuario/.forward**.

```
mv /home/usuario/.forward /home/usuario/.forward.old
```

Y definir de nuevo **/dev/null**, **/bin/false** o **/sbin/nologin** como intérprete de mandatos para el usuario.

```
usermod -s /sbin/nologin usuario
```

60. Cómo configurar clamav-milter.

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

60.1. Introducción.

60.1.1. 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/

60.1.2. 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/

60.2. Equipamiento lógico necesario.

- sendmail (previamente configurado)
- sendmail-cf

- make
- clamav
- m4
- clamav-milter

60.2.1. Instalación a través de yum.

Si dispone de un servidor con **CentOS 4** y **5**, **Red Hat™ Enterprise Linux 5** o **White Box Enterprise Linux 4** y **5**, puede utilizar el el depósito yum de **Alcance Libre** para servidores en producción:

```
[AL-Server]
name=AL Server para Enterprise Linux $releasever
mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server
gpgcheck=1
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
```

60.3. Procedimientos.

60.3.1. SELinux y el servicio clamav-milter.

Para que SELinux permita al servicio **clamav-milter** funcionar normalmente y que permita realizar la revisión de correo electrónico, utilice el siguiente mandato:

```
setsebool -P clamscan_disable_trans 1
```

Para que SELinux permita al mandato **freshclam** funcionar normalmente y que permita actualizar la base de datos de firmas digitales, utilice el siguiente mandato:

```
setsebool -P freshclam_disable_trans 1
```

60.3.2. 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).»*.

60.3.3. 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
```

60.3.4. 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
```

60.3.5. 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
```

61. Cómo configurar spamass-milter.

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

61.1. Introducción.

61.1.1. 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/

61.1.2. 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/

61.2. Equipamiento lógico necesario.

- sendmail (previamente configurado)
- make
- spamassassin
- sendmail-cf
- m4
- spamass-milter

61.2.1. 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
```

61.3. Procedimientos.

61.3.1. SELinux y el servicio spamass-milter.

Para que SELinux permita al servicio **spamass-milter** funcionar normalmente y que permita realizar la revisión de correo electrónico, utilice el siguiente mandato:

```
setsebool -P spamd_disable_trans 1
```

61.3.2. 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).»*.

61.3.3. 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, _, {daemon_name}, {if_name},
{if_addr}')dnl
define(`confMILTER_MACROS_HELO',`s, {tls_version}, {cipher}, {cipher_bits},
{cert_subject}, {cert_issuer}')dnl
```

Si se combina con **ClamAV 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
```

61.3.4. 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: {¿Spam?}
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 201.161.1.226
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.

61.3.5. Fichero /etc/sysconfig/spamass-milter.

El fichero **/etc/sysconfig/spamass-milter** 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 incrementando 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 {Spam?}** y

en el fichero **/etc/sysconfig/spamass-milter** se establece **EXTRA_FLAGS="-m -r 6"**, ocurrirá lo siguiente:

1. Todos los mensajes marcados 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 {Spam?} 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"
```

61.3.6. Fichero /etc/procmailrc.

Si se desea que el correo marcado con una mínima puntuación para ser considerado **Spam** (igual o superior al valor definido para el parámetro **required_hits** del fichero /etc/mail/spamassassin/local.cf) se entregue en una carpeta diferente al buzón de entrada, para ser consultado a través de un webmail (Squirrelmail o GroupOffice) o bien un cliente con soporte IMAP (Microsoft Outlook, GNOME Evolution o Mozilla Thunderbird), se puede crear el fichero **/etc/procmailrc** con el siguiente contenido:

```
# Hacer pasar el correo por spamassassin
:0fw
| /usr/bin/spamc

# Mover mensajes positivos sa Spam hacia la capeta mail/Spam del usuario
:0:
* ^X-Spam-Status: Yes
$HOME/mail/Spam
```

Lo anterior define una regla condicionada a que la cabecera del mensaje incluya **X-Spam-Status: Yes**, el cual es agregado por **SpamAssassin** cuando hay casos que superan el mínimo de puntos para ser considerado **Spam**, de modo que todo correo que incluya esta cabecera será almacenado en la carpeta **mail/Spam** propiedad del usuario a quien sea destinado el mensaje. Al estar en **/etc/procmailrc**, esta regla se aplica a todas la cuentas de usuario en el servidor. Combinado con todo lo anterior, 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 {Spam?} al inicio y se almacenarán en la capeta **mail/Spam** del usuario.

3. Todos los mensajes que estén marcados con 6.0 puntos o más serán rechazados automáticamente.

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"
```

61.3.7. 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
```

62. Cómo configurar un servidor NIS

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

62.1. 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.

62.2. 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.

62.2.1.1. 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
```

62.2.1.2. 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
```

62.2.2. Configuración del servidor NIS.

62.2.2.1. 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
```

62.2.2.2. 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
```

62.2.2.3. 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
```

62.2.2.4. 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
```

62.2.2.5. 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
```

62.2.2.6. 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
```

62.2.2.7. 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
```

62.2.3. Instalación del equipamiento lógico necesario en el cliente NIS.

62.2.3.1. 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
```

62.2.3.2. 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
```

62.2.4. Configuración del cliente NIS.

62.2.4.1. 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
```

62.2.4.2. 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
```

62.2.4.3. 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
```

62.2.4.4. Iniciar servicio ypbind.

Inicie y añada al arranque del sistema el servicio ypbind:

```
service ypbind start
chkconfig ypbind on
```

62.2.4.5. 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
```

63. Cómo configurar OpenLDAP como servidor de autenticación

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

63.1. 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

63.2. Equipamiento lógico necesario.

- openldap-2.2.13
- openldap-clients-2.2.13
- openldap-servers-2.2.
- authconfig-4.6.10
- authconfig-gtk-4.6.10 (opcional)

63.2.1. Instalación a través de yum.

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 openldap openldap-clients openldap-servers authconfig authconfig-gtk
```

63.2.2. 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 openldap openldap-clients openldap-servers authconfig authconfig-gtk
```

63.3. Procedimientos.

63.3.1. SELinux y el servicio ldap.

Para que SELinux permita al servicio **ldap** funcionar normalmente, haciendo que se pierda toda la protección que brinda esta implementación, utilice el siguiente mandato:

```
setsebool -P slapd_disable_trans 1
```

63.3.2. Creación de directorios.

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
```

Se requiere además copiar el fichero **/etc/openldap/DB_CONFIG.example** dentro de **/var/lib/ldap/addressbook/** como el fichero **DB_CONFIG**:

```
cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/autenticar/DB_CONFIG
```

63.3.3. Generación de claves de acceso para LDAP.

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:

```
{SSHA}XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Copie y respalde este criptograma. El texto de la salida será utilizado más adelante en el fichero **/etc/openldap/slapd.conf** y se definirá como clave de acceso para el usuario *Administrador*, quien tendrá todos los privilegios sobre el directorio.

63.3.4. Fichero de configuración /etc/openldap/slapd.conf.

Se edita el fichero **/etc/openldap/slapd.conf** y se verifica que los ficheros de esquema mínimos requeridos estén presentes. De tal modo, al inicio del fichero debe haber algo similar a lo siguiente:

```
#
# 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
# Allow LDAPv2 client connections.  This is NOT the default.
allow bind_v2
```

Se añade al 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-dominio,dc=com"
rootdn          "cn=Administrador,dc=su-dominio,dc=com"
rootpw          {SSHA}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
```

63.3.5. Inicio del servicio ldap.

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
```

63.3.6. Migración de cuentas existentes en el sistema.

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-dominio.com";

# Default base
$DEFAULT_BASE = "dc=su-dominio,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-dominio, 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-dominio, dc=com' -h 127.0.0.1 -f group.ldif
ldapadd -x -W -D 'cn=Administrador, dc=su-dominio, dc=com' -h 127.0.0.1 -f
passwd.ldif
```

63.4. 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-dominio,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-dominio**,dc=com).

```
ldapsearch -x -b 'dc=su-dominio,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-dominio,dc=com'
```

Lo anterior debe regresar algo como lo siguiente:

```
# extended LDIF
#
# LDAPv3
# base su-dominio,dc=com with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# fulano, People, su-dominio.com
dn: uid=fulano,ou=People,dc=su-dominio,dc=com
uid: fulano
cn: fulano
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: xxxxxxxxxxx
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
```

63.5. Configuración de clientes.

Defina los valores para los parámetros **host** y **base** a fin de establecer hacia que servidor y a que directorio conectarse en el fichero **/etc/ldap.conf**. Para fines prácticos, el valor del parámetro **host** corresponde a la dirección IP del servidor LDAP y el valor del parámetro **base** debe ser el mismo que se especificó en el fichero **/etc/openldap/slapd.conf** para el parámetro **suffix**. Considerando que el servidor LDAP tiene la dirección IP 192.168.0.1, se puede definir lo siguiente en el fichero **/etc/openldap/slapd.conf**:

```
# 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-dominio,dc=com
```

Lo que sigue es utilizar ya sea **authconfig**, **authconfig-tui** o **authconfig-gtk** para configurar el sistema a fin de que se utilice el servidor LDAP para autenticar.

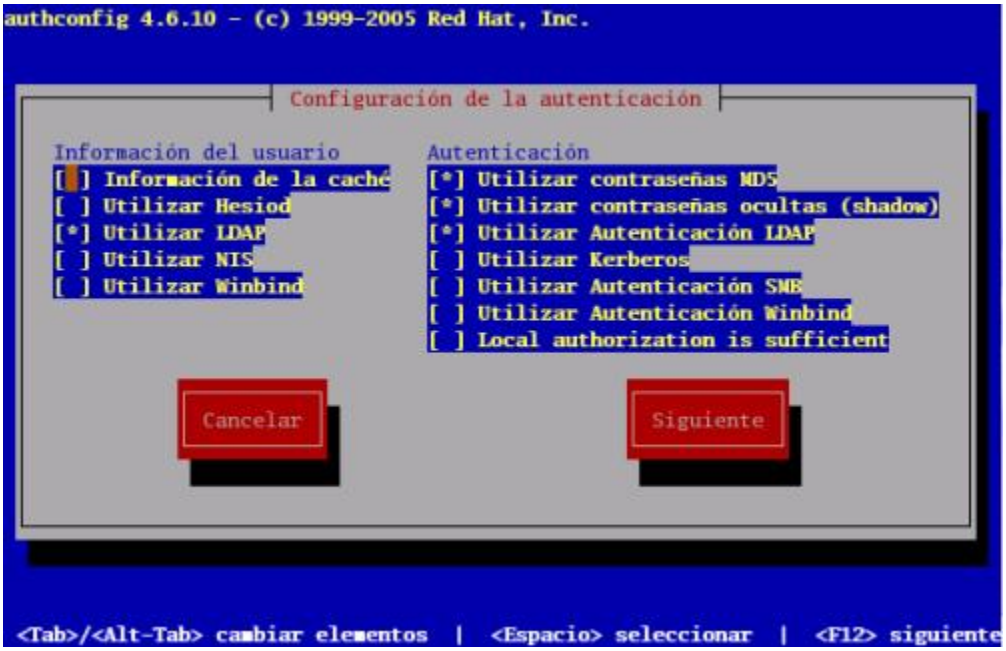
63.5.1. authconfig (modo-texto)

Suponiendo que el servidor LDAP tiene la dirección IP 192.168.0.1, utilice el siguiente mandato para configurar al cliente remoto a fin de que autentique en el directorio LDAP.

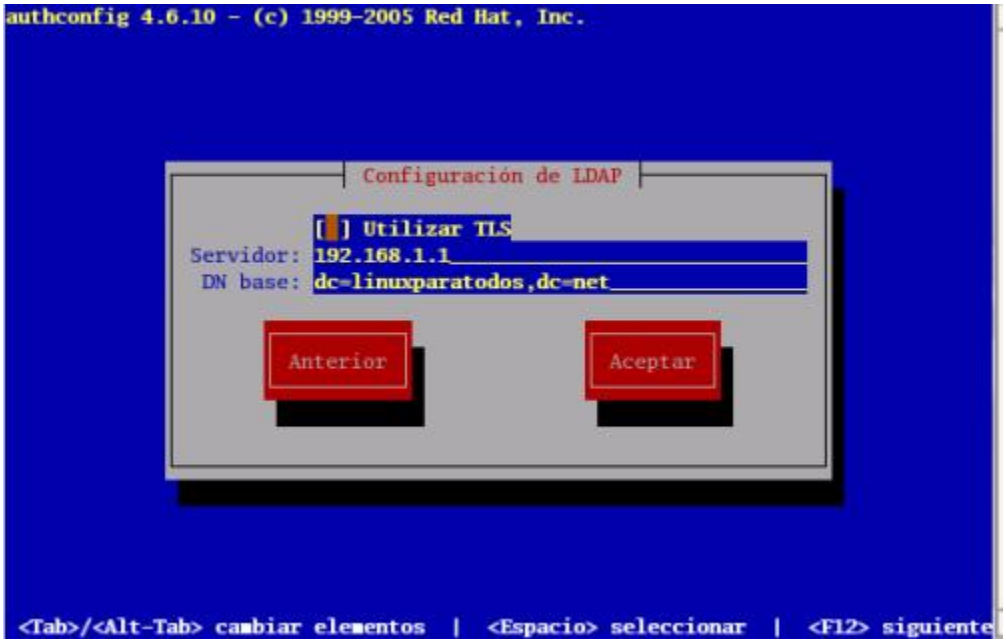
```
authconfig --useshadow  --enablemd5  --nostart \
--enableldap --enableldapauth --ldapserver=ldap://192.168.0.1/ \
--ldapbasedn=dc=su-dominio,dc=com --update
```

63.5.2. authconfig-tui (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.



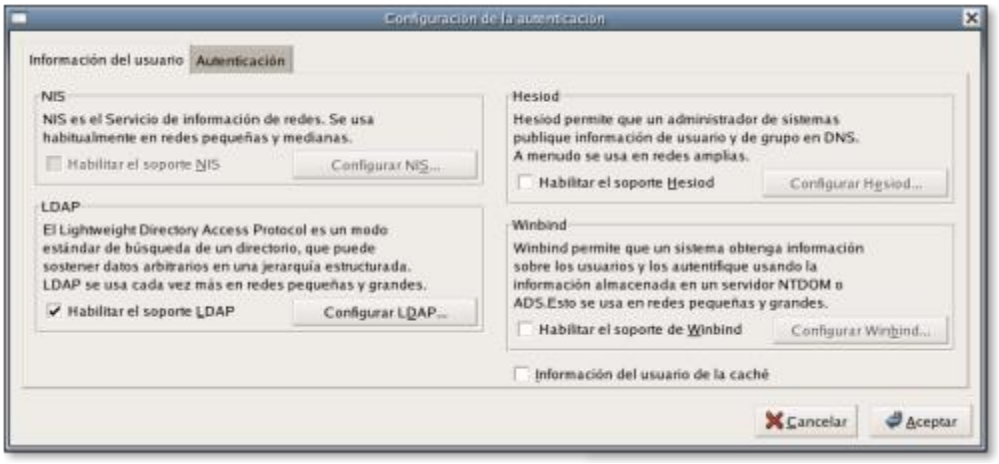
authconfig-tui, pantalla principal.



authconfig-tui, pantalla configuración ldap.

63.5.3. 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.

63.6. 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 PHP LDAP Admin.

63.7. 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
```

63.8. 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 *.ldif 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
```

63.9. 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
```

64. Cómo configurar OpenLDAP como libreta de direcciones.

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

64.1. 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

64.2. Equipamiento lógico necesario.

- 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)

64.2.1. Instalación a través de yum.

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 openldap openldap-clients openldap-servers evolution-data-server
```

64.2.2. 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 openldap openldap-clients openldap-servers evolution-data-server
```

64.3. Procedimientos.

64.3.1. SELinux y el servicio ldap.

Para que SELinux permita al servicio **ldap** funcionar normalmente, haciendo que se pierda toda la

protección que brinda esta implementación, utilice el siguiente mandato:

```
setsebool -P slapd_disable_trans 1
```

64.3.2. Creación de directorios.

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
```

Se requiere además copiar el fichero **/etc/openldap/DB_CONFIG.example** dentro de **/var/lib/ldap/addressbook/** como el fichero **DB_CONFIG**:

```
cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/addressbook/DB_CONFIG
```

64.3.3. Generación de claves de acceso para LDAP.

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:

```
{SSHA}XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Copie y respalde este criptograma. El texto de la salida será utilizado más adelante en el fichero **/etc/openldap/slapd.conf** y se definirá como clave de acceso para el usuario *Administrador*, quien tendrá todos los privilegios sobre el directorio.

64.3.4. Fichero de esquemas.

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/
```

64.3.5. Fichero de configuración /etc/openldap/slapd.conf.

Edite el fichero **/etc/openldap/slapd.conf** y agregue entre las primeras líneas del fichero el esquema de datos instalado con el paquete **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
# Allow LDAPv2 client connections.  This is NOT the default.
allow bind_v2
```

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, donde dc=**su-dominio**,dc=net corresponde al nombre único y exclusivo para el nuevo directorio. Jamás utilice el mismo nombre de otro directorio existente.

```
database        bdb
suffix          "dc=su-dominio,dc=net"
rootdn          "cn=Administrador,dc=su-dominio,dc=net"
rootpw          {SSHA}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
```

64.3.6. Inicio del servicio ldap.

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
```

64.3.7. Añadir datos al directorio.

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, del cual solo reemplace la cadena de texto **su-dominio** por el dominio deseado:

```
dn: dc=su-dominio, dc=net
objectclass: top
objectclass: dcObject
objectclass: organization
o: Nombre completo de su compañia
dc: su-dominio

dn: ou=Addressbook, dc=su-dominio, dc=net
ou: Addressbook
objectClass: top
objectClass: organizationalUnit
```

Es importante señalar que si se omite el **renglón vacío** entre **dc: su-dominio** y **dn: ou=Addressbook, dc=su-dominio, dc=net**, ocurrirá un irremediable error de sintaxis cuando se intente cargar los datos en el directorio. Respete los espacios, signos de puntuación, las mayúscula y las minúsculas.

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=net' -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 sean de poca utilidad, porque de otra manera LDAP impedirá 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=net
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 compañía.
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.alcancelibre.org/
# 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:

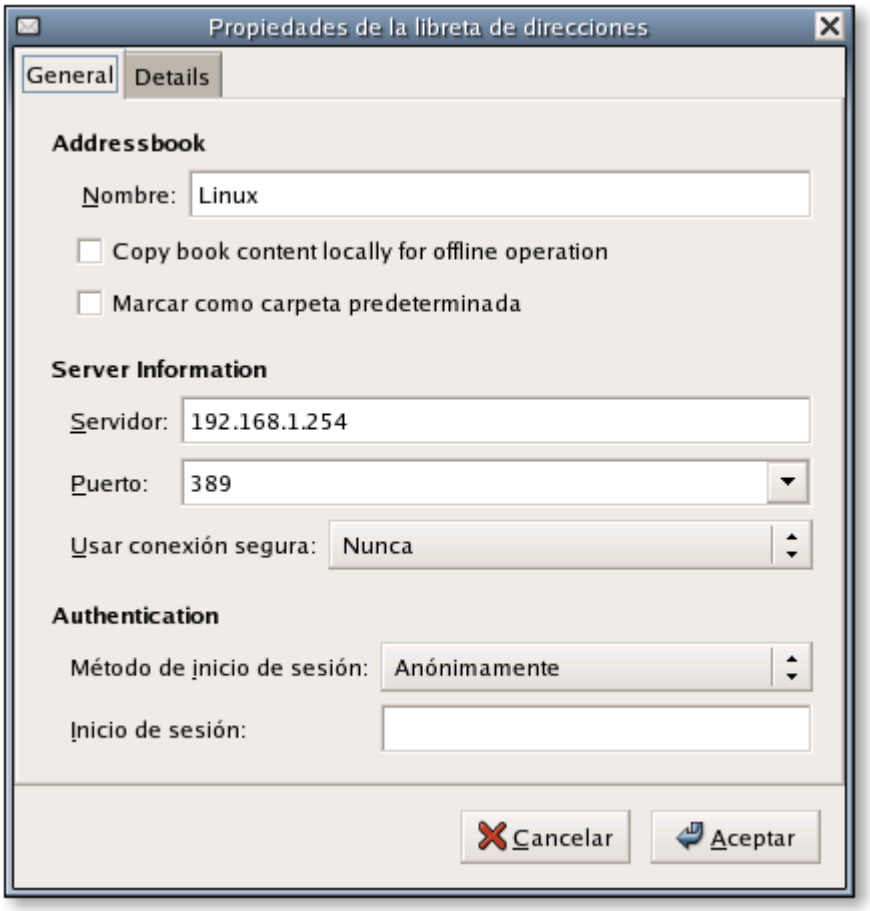
```
ldapadd -x -W -D 'cn=Administrador, dc=su-dominio, dc=net' -h 127.0.0.1 -f su-
usuario.ldif
```

64.4. Configuración de clientes.

Acceda hacia el directorio con cualquier cliente que tenga soporte para acceder hacia directorios LDAP.

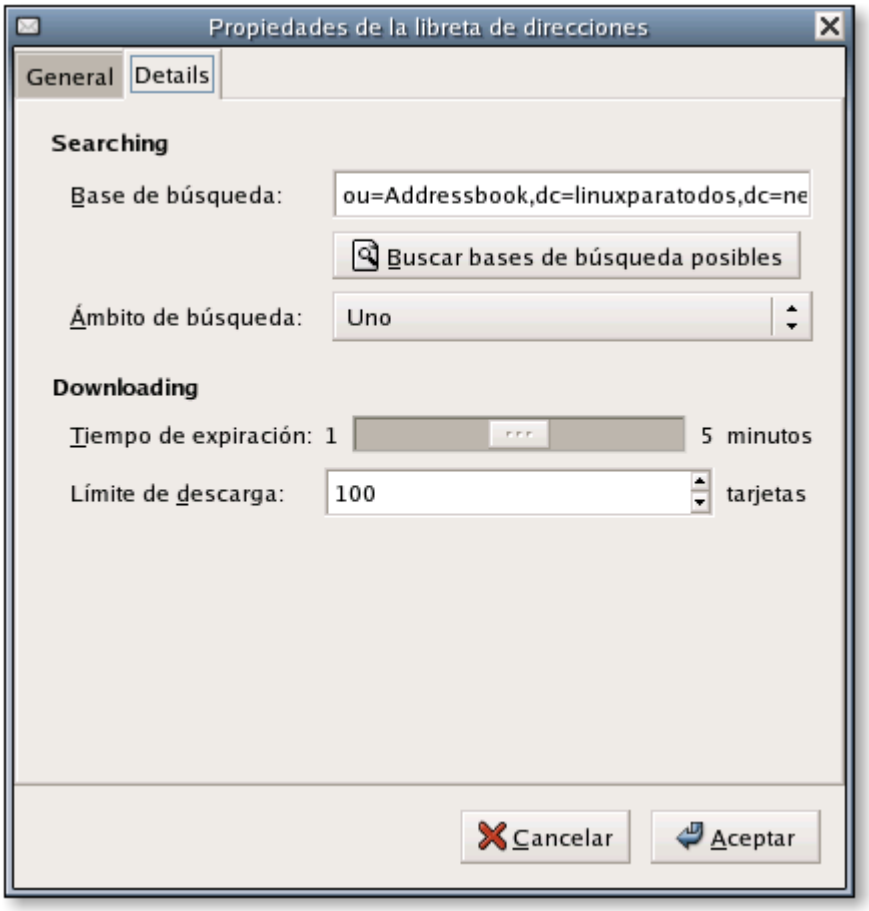
64.4.1. Novell Evolution.

Hacer clic en Archivo → Nuevo → Libreta de direcciones.



Propiedades de la libreta de direcciones, pestaña General.

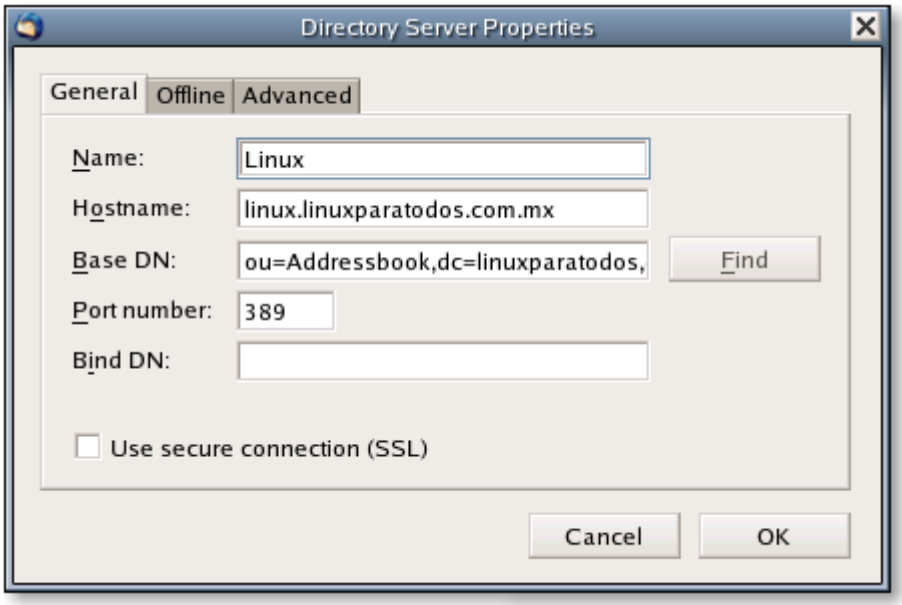
Si en lugar de autenticar de manera anónima (modo de solo lectura) lo hace con **cn=Administrador, dc=su-dominio, dc=net** (modo de lectura y escritura), podrá realizar modificaciones y añadir fácilmente nuevos registros en la libreta de direcciones.



Propiedades de la libreta de direcciones, pestaña Detalles.

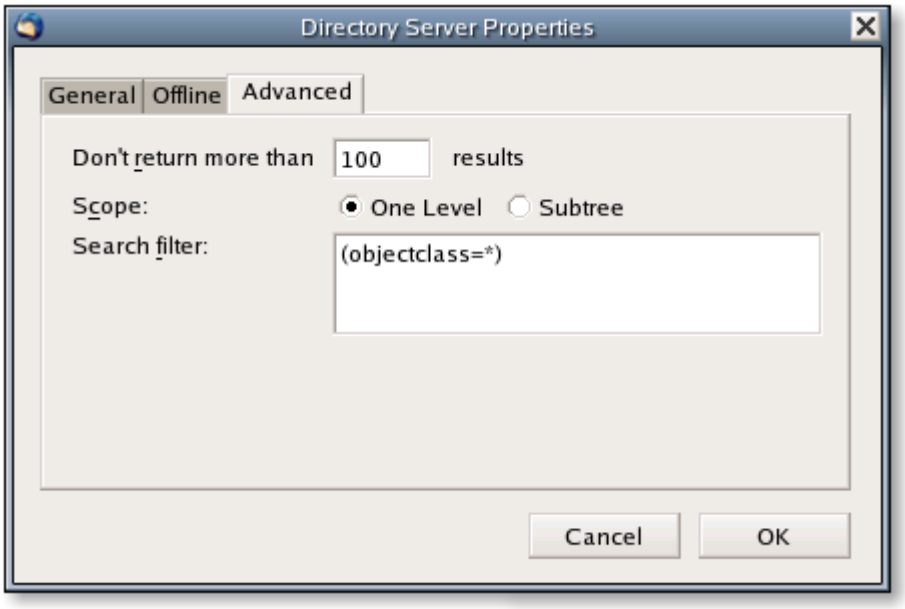
64.4.2. Mozilla Thunderbird.

Hacer clic en Archivo → Nuevo → Directorio LDAP



Propiedades de servidor de directorio, pestaña General.

Al igual que con Novell Evolution, si en lugar de autenticar de manera anónima (modo de solo lectura) lo hace con **cn=Administrador, dc=su-dominio, dc=net** (modo de lectura y escritura), podrá realizar modificaciones y añadir fácilmente nuevos registros en la libreta de direcciones.



Propiedades de servidor de directorio, pestaña Avanzado.

64.4.3. 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=net',
    'name' >= 'Addressbook'
);
```

64.5. 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 como diradmin y el módulo de LDAP de Webmin. La mejor herramienta de administración de directorios LDAP que podemos recomendar es PHP LDAP Admin.

64.6. 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
```

64.7. 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
```

64.8. 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 REMOV
```

65. Cómo configurar OpenLDAP con soporte SSL/TLS.

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

65.1. 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.

65.1.1. 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

65.1.2. 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

65.1.3. 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

65.1.4. 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/

65.2. Procedimientos.

65.2.1. 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.*
```

65.2.2. Parámetros de /etc/openldap/slapd.conf.

Se deben descomentar los parámetros **TLSCACertificateFile**, **TLSCertificateFile** y **TLSCertificateKeyFile** estableciendo 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**.

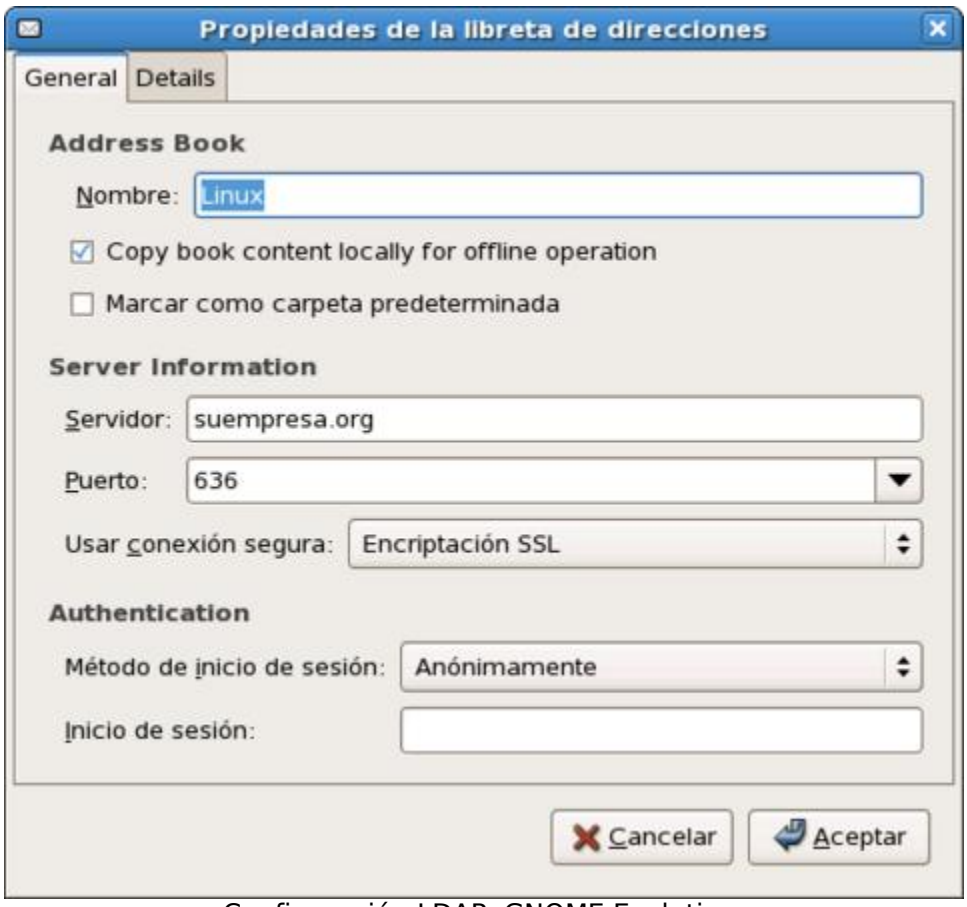
```
service ldap restart
```

65.2.3. 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.

65.2.4. 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.

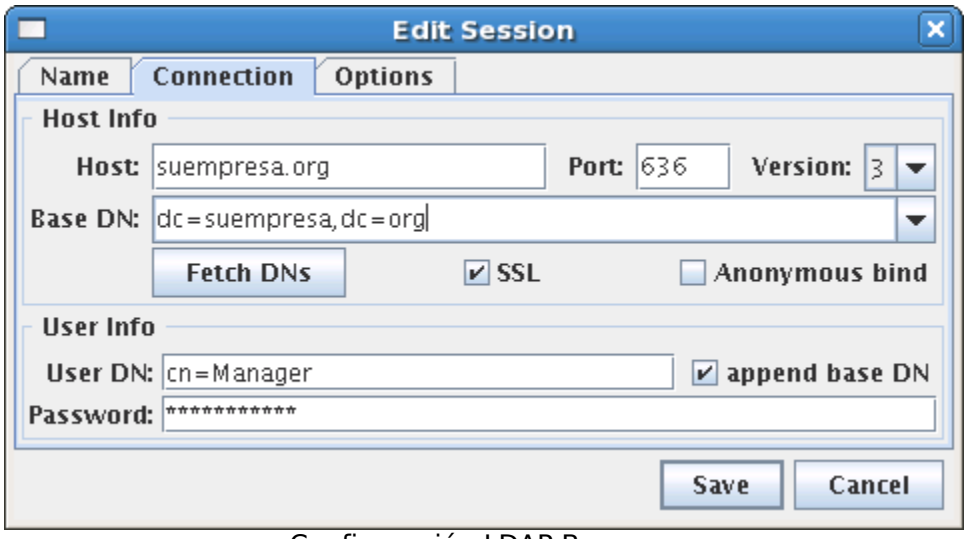
65.2.5. Configuración de Mozilla Thunderbird.

Se debe establecer el mismo nombre del servidor utilizado para crear el certificado, y conexión por SSL.

Configuración LDAP, Mozilla Thunderbird.

65.2.6. Configuración LDAP Browser.

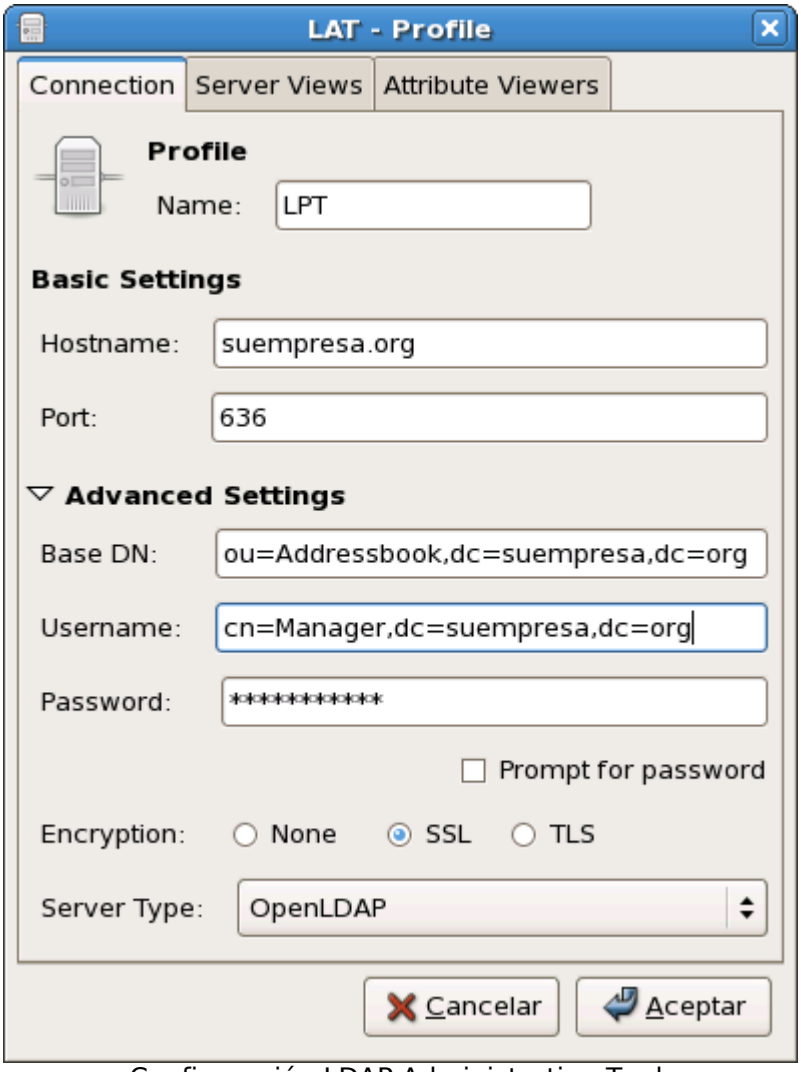
Se debe establecer el mismo nombre del servidor utilizado para crear el certificado, y conexión por SSL.



Configuración LDAP Browser.

65.2.7. 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.

65.3. 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
```

66. Cómo instalar y configurar MySQL™.

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

66.1. Introducción.

66.1.1. Acerca de MySQL™.

MySQL™ es un **DBMS** (**D**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.

URL: http://www.mysql.com/

66.2. Equipamiento lógico necesario.

66.2.1. 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
```

66.2.2. 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
```

66.3. Procedimientos.

66.3.1. SELinux y el servicio mysqld.

Si utiliza **CentOS 4**, **Red Hat™ Enterprise Linux 4** o **White Box Enterprise Linux 4** o versiones posteriores de estos sistemas operativos, active la política **mysqld_disable_trans** con el mandato **setsebool** para permitir funcionar al servicio **mysqld**. De otro modo, el servicio **mysqld** jamás podrá iniciar.

```
setsebool -P mysqld_disable_trans 1
```

Para que SELinux permita utilizar el cliente **mysql** para establecer conexiones hacia servidores MySQL, utilice el siguiente mandato:

```
setsebool -P allow_user_mysql_connect 1
```

66.3.2. 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
```

66.3.3. 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
```

66.3.4. 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.

66.3.4.1. 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.

66.3.4.2. 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™

66.4. 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
```

66.5. 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';
```

66.6. 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
```

67. Configuración básica de Apache.

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

67.1. Introducción.

67.1.1. 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

67.1.2. 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/

67.2. Equipamiento lógico necesario.

67.2.1. Instalación a través de yum.

Si se utiliza de **CentOS 4**, **Red Hat Enterpirse Linux 5** o **White Box Enterprise Linux 4** o versiones posteriores de éstos, solo se necesita 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
```

67.2.2. Instalación a través de Up2date

Si se utiliza de Red Hat™ Enterprise Linux 4, solo se necesita 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
```

67.3. 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 se necesita ejecuta:

```
chkconfig httpd on
```

Para iniciar el servicio por primera vez, solo se necesita utilizar:

```
service httpd start
```

Para reiniciar el servicio, considerando que se interrumpirán todas las conexiones establecidas en ese momento, solo se necesita 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 se necesita utilizar:

```
service httpd stop
```

67.4. Procedimientos.

67.4.1. 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.

Para permitir a Apache poder enviar correo electrónico desde alguna aplicación, utilice el siguiente mandato:

```
setsebool -P httpd_can_sendmail 1
```

Para permitr a Apache poder ejecutar guiones CGI, utilice el siguiente mandato:

```
setsebool -P httpd_enable_cgi 1
```

Para permitir las inclusiones del lado del servidor (**SSI**, **S**erver **S**ide **I**ncludes), utilice el siguiente mandato:

```
setsebool -P httpd_ssi_exec 1
```

Para permitir que Apache se pueda conectar a través de red hacia un servidor de bases de datos, utilice el siguiente mandato:

```
setsebool -P httpd_can_network_connect_db 1
```

Para permitir a Apache realizar conexiones de red hacia otro servidor, utilice el siguiente mandato:

```
setsebool -P httpd_can_network_connect 1
```

Para permitir que los usuarios locales tengan puedan utilizar un directorio público (**public_html**), utilice el siguiente mandato:

```
setsebool -P httpd_enable_homedirs 1
```

Para **desactivar** la ejecución de PHP y otros lenguajes de programación para HTTP a través de Apache, utlice el siguiente mandato:

```
setsebool -P httpd_builtin_scripting 0
```

Para consultar que otras políticas disponibles existen para Apache, utilice el siguiente mandato:

```
getsebool -a |grep httpd
```

Para definir que un directorio o fichero fuera de **/var/www/html**, como por ejemplo

/var/www/dominio/html se debe considerar como contenido HTTP, se utiliza el siguiente mandato:

```
chcon -t httpd_sys_content_t /var/www/dominio/html
```

Para definir que se permite ejecutar un guión CGI en particular, como por ejemplo **/var/www/dominio/cgi-bin/formulario.pl**, se utililiza el siguiente mandato:

```
chcon -t httpd_sys_script_exec_t /var/www/dominio/cgi-bin/formulario.pl
```

Para definir que un programa, que por ejemplo puede estar ecrito en PHP como **/var/www/dominio/html/leer.php**, solo pueda realizar procedimientos de lectura de datos y nunca de escritura, utilice el siguiente mandato:

```
chcon -t httpd_sys_script_ro_t /var/www/dominio/html/leer.php
```

Para definir que un programa, que por ejemplo puede estar ecrito en PHP como **/var/www/dominio/html/escribir.php**, pueda realizar procedimientos de lectura y escritura de datos, utilice el siguiente mandato:

```
chcon -t httpd_sys_script_rw_t /var/www/dominio/html/leer.php
```

Para definir que se desactive la protección de SELinux para Apache, haciendo que todo lo anteriormente descrito en esta sección pierda sentido, utilice el siguiente mandato:

```
setsebool -P httpd_disable_trans 1
```

67.4.2. 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
```

67.4.3. 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/.**

67.4.4. Directorios virtuales.

Si, por ejemplo, se quisiera añadir el alias para un directorio localizado en **/var/contenidos/varios/** y el cual queremos visualizar como el directorio **/varios/** en Apache, lo primero será crear el directorio:

```
mkdir -p /var/contenidos/varios
```

A continuación se configura el contexto en SELinux de dicho directorio a fin de que sea tratado como un objeto (**object_r**) creado por usuario de sistema (**system_u**) y que es contenido de Apache (**https_sys_content_t**):

```
chcon -u system_u /var/contenidos/varios
chcon -r object_r /var/contenidos/varios
chcon -t https_sys_content_t /var/contenidos/varios
```

Y se crea un fichero que se denominará arbitrariamente como **/etc/httpd/conf.d/aliases.conf** con el siguiente contenido:

```
Alias  /varios  /var/contenidos/varios
```

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 /varios /var/contenidos/varios
        <Directory "/var/contenidos/varios">
                Options Indexes
        </Directory>
```

El parámetro **Indexes** indica que se deberá mostrar el índice de contenido del directorio. Si se

requiere que este directorio tenga mayor funcionalidad, se pueden añadir más opciones, como por ejemplo:

```
Alias /varios /var/contenidos/varios
        <Directory "/var/contenidos/varios">
                Options Indexes Includes FollowSymLinks
                AllowOverride all
        </Directory>
```

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 **AllowOverride all** posibilita utilizar ficheros **.htaccess**.

Reinicie o recargue Apache y acceda hacia *http://127.0.0.1/varios/* con cualquier navegador de red y visualice el resultado.

67.4.5. 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*.

67.4.6. 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
```

67.4.7. 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
```

67.4.7.1. 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/htmlnn";
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
```

67.4.7.2. 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.

67.4.7.3. 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.

67.4.7.4. 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.

67.4.8. 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 adicional 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 cualquier fichero *.conf dentro del directorio **/etc/httpd/conf.d/**.

67.5. 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
```

67.6. 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/mi-dominio/
        ServerName www.dominio.net
        ErrorLog /var/www/mi-dominio/logs/www.dominio.net-error_log
        CustomLog /var/www/mi-dominio/logs/www.dominio.net-access_log combined
</VirtualHost>
```

68. 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/

68.1. 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
```

68.2. Procedimientos.

68.2.1. 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
```

68.2.1.1. 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/
```

68.2.2. 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
```

68.2.2.1. 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

69. Cómo configurar Apache con soporte SSL/TLS.

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

69.1. Introducción.

69.1.1. 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

69.1.2. 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 ciframiento 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

69.1.3. 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 ciframiento, 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

69.1.4. 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

69.1.5. 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/

69.1.6. 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

69.2. 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.

69.3. Equipamiento lógico necesario.

69.3.1. Instalación a través de yum.

Si se utiliza de CentOS 4 y 5 o White Box Enterprise Linux 4 y 5, ejecute lo siguiente:

```
yum -y install mod_ssl
```

69.3.2. Instalación a través de Up2date

Si se utiliza de Red Hat™ Enterprise Linux 4 y 5, ejecute lo siguiente:

```
up2date -i mod_ssl
```

69.4. 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
```

69.4.1. 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.*
```

69.4.2. Configuración de Apache.

Crear la estructura de directorios para el sitio de red virtual.

```
mkdir -p /var/www/midominio.org/{cgi-bin,html,logs,etc,var}
```

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/
                <Directory "/var/www/midominio.org/cgi-bin">
                        SSLOptions +StdEnvVars
                </Directory>
                SSLEngine on
                SSLProtocol all -SSLv2
                SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
                SSLCertificateFile /etc/ssl/midominio.org/server.crt
                SSLCertificateKeyFile /etc/ssl/midominio.org/server.pem
                SetEnvIf User-Agent ".*MSIE.*" \
                        nokeepalive ssl-unclean-shutdown \
                        downgrade-1.0 force-response-1.0
                CustomLog /var/www/midominio.org/logs/ssl_request_log \
                        "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
                Errorlog /var/www/midominio.org/logs/ssl_error_log
                TransferLog /var/www/midominio.org/logs/ssl_access_log
                LogLevel warn
        </VirtualHost>
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **httpd**.

```
service httpd restart
```

69.4.3. 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.

69.4.4. 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
```

70. 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/

70.1. Introducción.

70.1.1. 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.

70.1.2. 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**.

70.1.3. 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.

70.1.4. 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 llamado «dominio.com», el **FQDN** sería «**maquina1.dominio.com.**», así es que se define de forma única 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 un dominio de otro 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.

70.1.5. Componentes de un DNS.

Los DNS operan a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

70.1.5.1. 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.

70.1.5.2. Servidores DNS.

Son servicios que contestan las consultas realizadas por los **Clientes DNS**. Hay dos tipos de servidores de nombres:

- **Servidor Maestro**: También denominado **Primario**. Obtiene los datos del dominio a partir de un fichero alojado en el mismo servidor.
- **Servidor Esclavo**: También denominado **Secundario**. Al iniciar obtiene los datos del dominio a través de un Servidor Maestro (o primario), 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 para 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 facilita la **propagación** de la zona y mejoran la eficiencia del sistema en general al 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 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 obtener la respuesta solicitada.

70.1.5.3. 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.
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

Tipo de Registro.	Descripción.
	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**.

70.1.6. Herramientas de búsqueda y consulta.

70.1.6.1. 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 de manera opcional el **Servidor DNS** a consultar.

```
host www.alcancelibre.org
```

Lo anterior realiza una búsqueda en los **Servidores DNS** definidos en el fichero **/etc/resolv.conf** del sistema, devolviendo como resultado una dirección IP.

```
host www.alcancelibre.org 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.

70.1.6.2. 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 de manera opcional 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 alcancelibre.org 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 *alcancelibre.org*.

```
dig alcancelibre.org 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 *alcancelibre.org*.

```
dig @200.33.146.217 alcancelibre.org 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 *alcancelibre.org*.

70.1.6.3. Mandato jwhois (whois).

El mandato **jwhois** es una herramienta de consulta a través de servidores **WHOIS**. La sintaxis básica es:

```
jwhois dominio
```

Ejemplo:

```
jwhois alcancelibre.org
```

Loa anterior regresa la información correspondiente al dominio *alcancelibre.org*.

70.2. 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.

70.2.1. Instalación a través de yum.

Si se utiliza de CentOS 5, Red Hat™ Enterprise Linux 5 o White Box Enterprise Linux 5, o versiones posteriores, se puede instalar utilizando lo siguiente:

```
yum -y install bind bind-chroot bind-utils caching-nameserver
```

70.2.2. 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
```

70.3. Procedimientos.

70.3.1. SELinux y el servicio named.

A mediados de 2008, Common Vulnerabilities and Exposures List y US-CERT reportaron que el investigador **Dan Kaminsky** descubrió que varias implementaciones de **DNS** (BIND 8 y 9 antes de 9.5.0-P1, 9.4.2-P1, y 9.3.5-P1; Microsoft DNS en todas las versiones de Windows 2000 SP4, XP SP2 y SP3, y Server 2003 SP1 y SP2). La vulnerabilidad permite a atacantes remotos falsificar tráfico DNS a través de ciertas técnicas de envenamiento de cache contra servidores de resolución recursiva (es decir cuando se usa la opción *allow-recursion* abierta a todo el mundo, como ocurre en los servidores DNS públicos), y se relaciona a insuficiente aleatoriedad de las ID de transacción y puertos de origen. Es decir, vulnerabilidad de entropía de insuficiencia de zócalos (*sockets*) de DNS (**DNS Insufficient Socket Entropy Vulnerability**). En otras palabras, un atacante puede contaminar el cache de un servidor DNS y hacer que los clientes se conecten hacia direcciones falsas. Es importante aclarar que esta es realmente una vulnerabilidad del

protocolo DNS.

SELinux protege casi por completo al servicio **named** contra la vulnerabilidad anteriormente descrita. Es por tal motivo que es importante utilizar SELinux.

A fin de que SELinux permita al servicio **named** trabajar con permisos de escritura para zonas maestras, es decir un esquema de servidor maestro con servidores esclavos o bien un servidor DNS dinámico, utilice el siguiente mandato:

```
setsebool -P named_write_master_zones 1
```

Para definir que se desactive la protección de SELinux para el servicio **named**, haciendo que todo lo anteriormente descrito en esta sección pierda sentido y el servidor sea parcialmente **susceptible a la vulnerabilidad de Kaminski**, utilice el siguiente mandato:

```
setsebool -P named_disable_trans 1
```

Sí realiza el procedimiento anterior, es importante configurar la función de consultas recursivas exclusivamente para redes en la que se confíe plenamente.

Sí se va a configurar un DNS dinámico, SELinux impedirá crear los ficheros ***.jnl** (*journal*, ficheros de diario) correspondientes. Las zonas de DNS dinámicas deben ser almacenadas en directorios específicos que solo contengan zonas dinámicas. Sugiero crear el directorio **/var/named/chroot/var/named/dynamics** para tal fin y configurar éste para qué pertenezca al usuario y grupo **named**, tenga permisos de lectura, escritura y ejecución para el usuario y grupo **named** (770) y tenga los contextos de SELinux de usuario de sistema (**system_u**), rol de objeto (**object_r**) y tipo cache del servicio **named** (**named_cache_t**) a fin de permitir escritura en este directorio.

```
cd /var/named/chroot/var/named/
mkdir dynamics/
chmod 770 dynamics/
chown named:named dynamics/
chcon -u system_u -r object_r -t named_cache_t dynamics/
```

Cualquier fichero de zona que se vaya a utilizar a través del servicio **named**, debe contar con los contextos de SELinux de usuario de sistema (**system_u**), rol de objeto (**object_r**) y tipo zona del servicio **named** (**named_zone_t**). En el siguiente ejemplo se utiliza el mandato **chcon** para cambiar los contextos del fichero **mi-dominio.zone** y definir los contextos de SELinux mencionados:

```
cd /var/named/chroot/var/named/
chcon -u system_u -r object_r -t named_zone_t mi-dominio.zone
```

70.3.2. 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).

Lista de todos los servidores de nombres (NS) que se utilizarán para efectos de redundancia.

3. **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 modificar éstos en el caso de tratarse de zonas esclavas.

70.3.3. 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. Cabe señalar que en las zonas de reenvío siempre se especifica al menos un registro **MX** (Mail Exchanger o intercambiador de correo), para definir donde está el servidor de correo para el dominio, 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.

70.3.3.1. Configuración mínima para /var/named/chroot/etc/named.conf.

La configuración mínima del fichero **/var/named/chroot/etc/named.conf**, y que permitirá utilizar el servicio para todo tipo de uso, es la siguiente:

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-recursion {
                127.0.0.1;
                192.168.1.0/24;
        };
        forwarders {
                200.33.146.209;
```

```
                200.33.146.217;
        };
        forward first;
};

include "/etc/named.rfc1912.zones";
include "/etc/rndc.key";

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckey"; };
};
```

Lo anterior define como opciones que el directorio predeterminado será **/var/named** (ruta relativa a **/var/named/chroot**), de define un fichero conde se almacena la información del caché en **/var/named/data/cache_dump.db**; un fichero de estadísticas en **/var/named/data/named_stats.txt**, un fichero de estadísticas específicas en lo concerniente al uso de la memoria en **/var/named/data/named_mem_stats.txt**; consultas recursivas permitidas solo a 127.0.0.1 y 192.168.1.0/24, se definen como **ejemplos** de servidores DNS para reenviar consultas a 200.33.146.209 y 200.33.146.217 (solo éstos utilizar desde redes de Prodigy Internet de Telmex, **definir en lugar de éstos los servidores DNS del proveedor de acceso a Internet**); se define que la primera opción al realizar una consulta será reenviar a los DNS que se acaban de definir; se incluyen los ficheros de configuración **/etc/named.rfc1912.zones**, que corresponde a las zonas del **RFC 1912**, y la firma digital única que se generó automáticamente tras instalar el paquete bind; Se define también que los controles se realizan solo desde 127.0.0.1 hacia 127.0.0.1 utilizando la firma digital única.

El fichero conviene asegurarse que el fichero **/var/named/chroot/etc/named.conf** tenga los contextos correspondientes para SELinux a fin de evitar potenciales problemas de seguridad.

```
chcon -u system_u -r object_r -t named_conf_t /var/named/chroot/etc/named.conf
```

70.3.3.2. Zona de reenvío red local /var/named/chroot/var/named/red-local.zone.

```
$TTL 86400
@               IN      SOA     dns.red-local.  alguien.gmail.com. (
                2009091001; 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
```

70.3.3.3. 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.  alguien.gmail.com. (
                2009091001 ; 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.
```

70.3.3.4. 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 Reenvío** con un contenido similar al siguiente:

```
$TTL 86400
@               IN      SOA     fqdn.dominio-resuelto.  alguien.gmail.com. (
                2009091001; 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
```

70.3.3.5. 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** (regularmente lo es el proveedor de servicio de acceso hacia Internet), se puede crear una **Zona de Resolución Inversa** con un contenido similar al siguiente:

```
$TTL 86400
@               IN      SOA     fqdn.dominio-resuelto.  alguien.gmail.com. (
                2009091001 ; 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 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.

Las zonas de resolución inversa que involucran direcciones IP públicas son responsabilidad de los ISP (proveedores de servicio de acceso hacia Internet). Crear una zona de resolución inversa sin ser la autoridad de dicha zona tiene efecto solo para quien use el servidor DNS recién configurado como único DNS.

70.3.3.6. 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";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-recursion {
                127.0.0.1;
                192.168.1.0/24;
        };
        forwarders {
                200.33.146.209;
                200.33.146.217;
        };
        forward first;
};
include "/etc/named.rfc1912.zones";
include "/etc/rndc.key";
controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckey"; };
};

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; };
};
```

70.3.4. Seguridad adicional en DNS para uso público.

Quienes hayan utilizado en recientes fechas los servicios de DNS Report, habrán notado que el diagnóstico en línea devuelve ahora un error que, en resumen, indica que el servidor puede ser susceptible de sufrir/participar en un ataque **DDoS** (**D**istributed **D**enail **o**f **S**ervice o denegación de servicio distribuido).

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.

La falla reportada por la herramienta en línea de DNS Report, para un servidor DNS que permite consultas recursivas, indicará algo como lo siguiente:

> *«ERROR: One or more of your nameservers reports that it is an open DNS server. This usually means that anyone in the world can query it for domains it is not authoritative for (it is possible that the DNS server advertises that it does recursive lookups when it does not, but that shouldn't happen). This can cause an excessive load on your DNS server. Alos, it is strongly discouraged to have a DNS server be both authoritative for your domain and be recursive (even if it is not open), due to the potential for cache poisoning (with no recursion, there is no cache, and it is impossible to poison it). Alos, the bad guys could use your DNS server as part of an attack, by forging their IP address»*

Significa que el servidor DNS puede permitir a cualquiera realizar consultas recursivas. Si se trata de un DNS que se desea pueda ser consultado por cualquiera, como puede ser el caso del DNS de un ISP, esto es normal y esperado. Si se trata de un servidor que solo debe consultar la red local, o bien que se utiliza para propagar dominios alojados de manera local, si es conveniente tomar medidas al respecto.

Solución al problema es modificar el fichero **named.conf**, donde se añade en la sección de opciones (**options**) una línea que defina la red, las redes o bien los **ACL** (**A**ccess **C**ontrol **L**ist o listas de control de acceso) que tendrán permitido realizar todo tipo de consultas.

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders { 192.168.0.1; };
        forward first;
        allow-recursion { 127.0.0.1; 192.168.0.0/24; };
};
controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckey"; };
};
```

Lo anterior hace que solo se puedan realizar consultas recursivas en el DNS desde 192.168.0.0/24, ya sea para un nombre de dominio alojado de manera local y otros dominios resueltos en otros servidores (ejemplo: www.yahoo.com, www.google.com, www.alcancelibre.org, etc). El resto del mundo solo podrá realizar consultas sobre los dominios alojados de manera local y que estén configurado para permitirlo.

En la siguiente configuración de ejemplo, se pretende lograr lo siguiente:

- Red Local: cualquier tipo de consulta hacia dominios externos y locales (es decir, www.yahoo.com, www.google.com, alcancelibre.org, además de ***midominio.com***).
- Resto del mundo: solo puede hacer consultas para la zona de ***midominio.com***

De este modo se impide que haya consultas recursivas y con esto impedir la posibilidad de sufrir/participar de un ataque DDoS.

```
options {
        directory "/var/named";
```

```
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders { 192.168.0.1; };
        forward first;
        allow-recursion { 127.0.0.1; 192.168.0.0/24; };
};

controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckey"; };
};

include "/etc/named.rfc1912.zones";
include "/etc/rndc.key";

zone "miredlocal" {
        type master;
        file "miredlocal.zone";
        allow-update { none; };
        allow-query { 192.168.0.0/24; };
        allow-transfer { 192.168.0.2; };
};

zone "midominio.com" {
        type master;
        file "midominio.com.zone";
        allow-update { none; };
        allow-transfer { 200.76.185.252; 200.76.185.251; };
};
```

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.

La falla reportada por la herramienta en línea de DNS Report, para un servidor DNS que permite consultas recursivas, indicará algo como lo siguiente:

> *«ERROR: One or more of your nameservers reports that it is an open DNS server. This usually means that anyone in the world can query it for domains it is not authoritative for (it is possible that the DNS server advertises that it does recursive lookups when it does not, but that shouldn't happen). This can cause an excessive load on your DNS server. Alos, it is strongly discouraged to have a DNS server be both authoritative for your domain and be recursive (even if it is not open), due to the potential for cache poisoning (with no recursion, there is no cache, and it is impossible to poison it). Alos, the bad guys could use your DNS server as part of an attack, by forging their IP address»*

Significa que el servidor DNS puede permitir a cualquiera realizar consultas recursivas. Si se trata de un DNS que se desea pueda ser consultado por cualquiera, como puede ser el caso del DNS de un ISP, esto es normal y esperado. Si se trata de un servidor que solo debe consultar la red local, o bien que se utiliza para propagar dominios alojados de manera local, si es conveniente tomar medidas al respecto.

Solución al problema es modificar el fichero **named.conf**, donde se añade en la sección de opciones (options) una línea que defina la red, las redes o bien los **ACL** (**A**ccess **C**ontrol **L**ist o listas de control de acceso) que tendrán permitido realizar todo tipo de consultas.

```
options {
```

```
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders { 192.168.0.1; };
        forward first;
        allow-recursion { 127.0.0.1; 192.168.0.0/24; };
};
controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckey"; };
};
include "/etc/named.rfc1912.zones";
include "/etc/rndc.key";
```

Lo anterior hace que solo se puedan realizar todo tipo de consultas en el DNS desde 192.168.0.0/24, ya sea para un nombre de dominio alojado de manera local y otros dominios resueltos en otros servidores (ejemplo: www.yahoo.com, www.google.com, www.alcancelibre.org, etc). El resto del mundo solo podrá realizar consultas sobre los dominios alojados de maneja local y que estén configurado para permitirlo.

En la siguiente configuración de ejemplo, se pretende lograr lo siguiente:

- Red Local: cualquier tipo de consulta hacia dominios externos y locales (es decir, www.yahoo.com, www.google.com, alcancelibre.org, además de ***midominio.com***).

- Resto del mundo: solo puede hacer consultas para la zona de ***midominio.com***

De este modo se impide que haya consultas recursivas y con esto impedir la posibilidad de sufrir/participar de un ataque DDoS.

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        forwarders { 192.168.0.1; };
        forward first;
        allow-recursion { 127.0.0.1; 192.168.0.0/24; };
};
controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckey"; };
};
include "/etc/named.rfc1912.zones";
include "/etc/rndc.key";

zone "miredlocal" {
        type master;
        file "miredlocal.zone";
        allow-update { none; };
        allow-query { 192.168.0.0/24; };
        allow-transfer { 192.168.0.2; };
};

zone "midominio.com" {
        type master;
        file "midominio.com.zone";
        allow-update { none; };
        allow-transfer { 200.76.185.252; 200.76.185.251; };
```

```
};
```

70.3.5. 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**.

70.3.5.1. 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";
        memstatistics-file "/var/named/data/named_mem_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;
        };
};
controls {
        inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckey"; };
};
include "/etc/named.rfc1912.zones";
include "/etc/rndc.key";

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; };
};
```

70.3.6. 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 **named.conf**, donde las zonas se definen como esclavas y definen los servidores donde está hospedada la zona maestra.

70.3.6.1. Fichero named.conf Servidor DNS secundario.

```
zone "dominio.com" {
        type slave;
        file "dominio.com.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:

70.3.6.2. Fichero 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 "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;
        };
};
```

70.3.7. Seguridad adicional para transferencias de zona.

Cuando se gestionan dominios a través de redes públicas, es importante considerar que si se

tienen esquemas de servidores **maestros** y **esclavos**, siempre será más conveniente utilizar una **clave cifrada** en lugar de una dirección IP, debido a que esta última puede ser falsificada bajo ciertas circunstancias.

Comúnmente se definen las direcciones IP desde las cuales se permitirá transferencias de zonas, utilizando una configuración en el fichero **/var/named/chroot/etc/named.conf** como la ejemplificada a continuación, donde los servidores esclavos corresponden a los servidores con direcciones IP 192.168.1.11 y 192.168.1.12:

```
zone "mi-dominio.org" {
        type master;
        file "mi-dominio.org.zone";
        allow-update { none; }:
        allow-transfer { 192.168.1.11; 192.168.1.12; };
};
```

Lo anterior permite la transferencia de zona para los servidores con direcciones IP 192.168.1.11 y 192.168.1.12, los cuales utilizan la siguiente configuración en el fichero **/var/named/chroot/etc/named.conf**, ejemplificada a continuación, donde el servidor primario (zonas maestras) corresponde al servidor con dirección IP 192.168.1.1:

```
zone "mi-dominio.org" {
        type slave;
        file "mi-dominio.org.zone";
        masters { 192.168.1.1; };
};
```

El inconveniente del esquema anterior es que es fácil falsificar las direcciones IP. A fin de evitar que esto ocurra, el método recomendado será utilizar una clave cifrada que será validada en lugar de la dirección IP. La llave se crea con el mandato **dnssec-keygen**, especificando un algoritmo, que puede ser **RSAMD5** o **RSA**, **DSA**, **DH** (**D**iffie **H**ellman) o **HMAC-MD5**, el tamaño de la llave en octetos (bits), el tipo de la llave, que puede ser ZONE, HOST, ENTITY o USER y el nombre específico para la clave cifrada. DSA y RSA se utilizan para **DNS Seguro** (**DNSSEC**), en tanto que **HMAC-MD5** se utiliza para **TSIG** (**T**ransfer **SIG**nature o transferencia de firma). Lo más común es utilizar **TSIG**. En el siguiente ejemplo, se generará en el directorio de trabajo actual la clave **mi-dominio.org**, utilizando **/dev/random** como fuente de datos aleatorios, un algoritmo **HMAC-MD5** tipo **HOST** de 128 octetos (bits):

```
dnssec-keygen -r /dev/random -a HMAC-MD5 -b 128 -n HOST mi-dominio.org
```

Lo anterior devuelve una salida similar a la siguiente:

```
Kmi-dominio.org.+157+32322
```

Al mismo tiempo se generaran dos ficheros en el directorio **/var/named/chroot/var/named/**, que corresponderían a **Kmi-dominio.org.+157+32322.key** y **Kmi-dominio.org. +157+32322.private**. **Kmi-dominio.org.+157+32322.key** deberá tener un contenido como el siguiente, el cual corresponde al registro que se añade dentro del fichero de zona:

```
mi-dominio.org. IN KEY 512 3 157 NPuNuxvZAjtd3mriuygT8Q==
```

Kmi-dominio.org.+157+32322.private deberá tener un contenido como el siguiente:

```
Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: NPuNuxvZAjtd3mriuygT8Q==
```

En ambos casos, **NPuNuxvZAjtd3mriuygT8Q==** corresponde a la clave cifrada. Ambos deben tener la misma clave.

Los dos ficheros solo deben tener atributos de lectura para el usuario **named**.

```
chmod 400 Kmi-dominio.org.+157+32322.*
chown named.named Kmi-dominio.org.+157+32322.*
```

A fin de poder ser utilizados, ambos ficheros deben ser movidos hacia el directorio **/var/named/chroot/var/named/**.

```
mv Kmi-dominio.org.+157+32322.* /var/named/chroot/var/named
```

En el servidor primario (zonas maestras), se añade la siguiente configuración en el fichero **/var/named/chroot/etc/named.conf**:

```
key mi-dominio.org {
    algorithm HMAC-MD5;
    secret "NPuNuxvZAjtd3mriuygT8Q==";
};

zone "mi-dominio.org" {
        type master;
        file "mi-dominio.org.zone";
        allow-update { none; };
        allow-transfer { key mi-dominio.org; };
};
```

Los servidores esclavos utilizarían la siguiente configuración en el fichero **/var/named/chroot/etc/named.conf**, en donde se define la clave y que ésta será utilizada para realizar conexiones hacia el servidor primario (zonas maestras) (192.168.1.1, en el ejemplo):

```
key mi-dominio.org {
        algorithm HMAC-MD5;
        secret "NPuNuxvZAjtd3mriuygT8Q==";
};

server 192.168.1.1 {
        keys { mi-dominio.org; };
};

zone "mi-dominio.org" {
        type slave;
        masters { 192.168.1.1; };
};
```

70.3.7.1. Comprobaciones.

Tanto en el servidor primario (zonas maestras) como en los servidores esclavos, utilice el mandato **tail** para ver la salida del fichero **/var/log/messages**, pero solo aquello que contenga la cadena de caracteres **named**:

```
tail -f /var/log/messages |grep named
```

Al reiniciar el servicio **named** en servidor primario (zonas maestras), se debe mostrar una salida similar a la siguiente cuando un servidor esclavo realiza una transferencia:

```
Sep 10 01:57:40 servidor named[6042]: listening on IPv4 interface eth0,
192.168.1.64#53
Sep 10 01:57:40 servidor named[6042]: command channel listening on 127.0.0.1#953
Sep 10 01:57:40 servidor named[6042]: zone 0.in-addr.arpa/IN: loaded serial 42
Sep 10 01:57:40 servidor named[6042]: zone 0.0.127.in-addr.arpa/IN: loaded serial
1997022700
Sep 10 01:57:40 servidor named[6042]: zone 255.in-addr.arpa/IN: loaded serial 42
Sep 10 01:57:40 servidor named[6042]: zone
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loaded
serial 1997022700
Sep 10 01:57:40 servidor named[6042]: zone localdomain/IN: loaded serial 42
Sep 10 01:57:40 servidor named[6042]: zone localhost/IN: loaded serial 42
Sep 10 01:57:40 servidor named[6042]: zone mi-dominio.org/IN: loaded serial
2009091001
Sep 10 01:57:40 servidor named: Iniciación de named succeeded
Sep 10 01:57:40 servidor named[6042]: running
Sep 10 01:57:40 servidor named[6042]: zone mi-dominio.org/IN: sending notifies
(serial 2009091001)
Sep 10 01:59:49 servidor named[6042]: client 192.168.1.11#32817: transfer of 'mi-
dominio.org/IN': AXFR started
```

Al reiniciar el servicio **named** en los servidores esclavos, se debe mostrar una salida similar a la siguiente:

```
Sep 10 01:58:15 servidor named[5080]: listening on IPv4 interface eth0,
192.168.1.253#53
Sep 10 01:58:15 servidor named[5080]: command channel listening on 127.0.0.1#953
Sep 10 01:58:15 servidor named[5080]: zone 0.in-addr.arpa/IN: loaded serial 42
Sep 10 01:58:15 servidor named[5080]: zone 0.0.127.in-addr.arpa/IN: loaded serial
1997022700
Sep 10 01:58:15 servidor named[5080]: zone 255.in-addr.arpa/IN: loaded serial 42
Sep 10 01:58:15 servidor named[5080]: zone
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loaded
serial 1997022700
Sep 10 01:58:15 servidor named[5080]: zone localdomain/IN: loaded serial 42
Sep 10 01:58:15 servidor named[5080]: zone localhost/IN: loaded serial 42
Sep 10 01:58:15 servidor named[5080]: running
Sep 10 01:58:15 servidor named: Iniciación de named succeeded
Sep 10 01:58:15 servidor named[5080]: zone mi-dominio.org/IN: transferred serial
2009091001
Sep 10 01:58:15 servidor named[5080]: transfer of 'mi-dominio.org/IN' from
192.168.1.1#53: end of transfer
Sep 10 01:58:15 servidor named[5080]: zone mi-dominio.org/IN: sending notifies
(serial 2009091001)
```

70.3.8. 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 realizar 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:

```
Sep 10 02:15:15 servidor named[30618]: starting BIND 9.2.2 -u named
Sep 10 02:15:15 servidor named[30618]: using 1 CPU
Sep 10 02:15:15 servidor named: Iniciación de named succeeded
Sep 10 02:15:15 servidor named[30622]: loading configuration from '/etc/named.conf'
Sep 10 02:15:15 servidor named[30622]: no IPv6 interfaces found
Sep 10 02:15:15 servidor named[30622]: listening on IPv4 interface lo, 127.0.0.1#53
Sep 10 02:15:15 servidor named[30622]: listening on IPv4 interface eth0,
192.168.1.1#53
Sep 10 02:15:15 servidor named[30622]: command channel listening on 127.0.0.1#953
Sep 10 02:15:16 servidor named[30622]: zone 0.0.127.in-addr.arpa/IN: loaded serial 3
Sep 10 02:15:16 servidor named[30622]: zone 1.168.192.in-addr.arpa/IN: loaded serial
2009091001
Sep 10 02:15:16 servidor named[30622]: zone localhost/IN: loaded serial 1
Sep 10 02:15:16 servidor named[30622]: zone mi-dominio.com.mx/IN: loaded serial
2009091001
Sep 10 02:15:16 servidor named[30622]: running
Sep 10 02:15:16 servidor named[30622]: zone 1.168.192.in-addr.arpa/IN: sending
notifies (serial 2009091001)
Sep 10 02:15:16 servidor named[30622]: zone mi-dominio.com.mx/IN: sending notifies
(serial 2009091001)
```

71. 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/

71.1. Introducción.

71.1.1. ¿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.

71.1.2. 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 equipamiento 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/

71.1.2.1. 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.

71.2. Equipamiento lógico necesario.

Para poder llevar al cabo los procedimientos descritos en este y otros 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. No es conveniente utilizar un sistema con posibles vulnerabilidades como Servidor Intermediario.

Debe tomarse en consideración que, de ser posible, se debe utilizar **siempre** las versiones estables más recientes de todo equipamiento lógico que vaya a ser instalado para 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 otro equipamiento lógico.

71.2.1. 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
```

71.2.2. 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
```

71.2.3. 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 **2.6.18**. 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
```

71.3. SELinux y el servicio squid.

A fin de que SELinux permita al servicio **squid** que los clientes se conecten desde cualquier dirección IP, ejecutar lo siguiente.

```
setsebool -P squid_connect_any 1
```

Para que SELinux permita al servicio **squid** funcionar normalmente, haciendo que todo lo anteriormente descrito en esta sección pierda sentido, utilice el siguiente mandato:

```
setsebool -P squid_disable_trans 1
```

71.4. 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
```

71.5. 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**
- httpd_accel_host
- httpd_accel_port
- httpd_accel_with_proxy

71.5.1. Parámetro http_port: ¿Que 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
```

En el caso de Squid 2.6 y versiones posteriores (**CentOS 5**, **Red Hat Enterprise Linux 5** y **White Box Enterprise Linux 5**), el parámetro http_port se utiliza también para especificar si se utiliza un proxy transparente, especificando el parámetro **transparent**, de la siguiente forma:

```
#
#    You may specify multiple socket addresses on multiple lines.
#
# Default: http_port 3128
http_port 192.168.1.254:8080 transparent
```

71.5.2. 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
```

71.5.3. Parámetro cache_dir: ¿Cuanto 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.

71.5.4. 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
```

71.5.5. 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.

71.5.5.1. 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**.

71.5.5.2. 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.

71.5.6. 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.

71.5.6.1. 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**.

71.5.6.2. 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**.

71.5.7. 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
```

71.5.8. 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:

```
cache_peer 10.0.0.1 parent 8080 3130 proxy-only
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
```

71.6. Caché con aceleración.

En el caso de Squid 2.6 y versiones posteriores (**CentOS 5**, **Red Hat Enterprise Linux 5** y **White Box Enterprise Linux 5**), esta sección queda obsoleta, pues desaparecen httpd_accel_host, httpd_accel_port, httpd_accel_with_proxy y httpd_accel_uses_host_header.

En versiones de **Squid** 2.5 y anteriores, cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el caché de **Squid**. Si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, **Squid** mostrará el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet.

Esta función permite navegar rápidamente cuando los objetos ya están en el caché de **Squid** y además optimiza enormemente la utilización del ancho de banda.

La configuración de **Squid** como Servidor Intermediario (Proxy) Transparente solo requiere complementarse utilizando una regla de **iptables** que se encargará de re-direccionar peticiones haciéndolas pasar por el puerto 8080. La regla de **iptables** necesaria se describe más adelante en este documento.

71.6.1. Proxy Acelerado: Opciones para Servidor Intermediario (Proxy) en modo convencional.

En la sección **HTTPD-ACCELERATOR OPTIONS** deben habilitarse los siguientes parámetros:

```
httpd_accel_host virtual
httpd_accel_port 0
httpd_accel_with_proxy on
```

71.6.2. Proxy Acelerado: Opciones para Servidor Intermediario (Proxy) Transparente.

Si se trata de un **Servidor Intermediario** (Proxy) transparente en versiones de **Squid** 2.5 y anteriores, deben utilizarse las siguientes opciones, considerando que se hará uso del caché de un servidor **HTTP** (Apache) como auxiliar:

```
# Debe especificarse la IP de cualquier servidor HTTP en la
# red local o bien el valor virtual
httpd_accel_host 192.168.1.254
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

En el caso de Squid 2.6 y versiones posteriores (**CentOS 5**, **Red Hat Enterprise Linux 5** y **White Box Enterprise Linux 5**), todo lo anterior es reeemplazado por:

```
http_port 192.168.1.254:8080 transparent
```

71.6.3. Proxy Acelerado: Opciones para Servidor Intermediario (Proxy) Transparente para redes con Internet Exlorer 5.5 y versiones anteriores.

Si va a utilizar Internet Explorer 5.5 y versiones anteriores con un **Servidor Intermediario** (Proxy) transparente, es importante recuerde que dichas versiones tiene un pésimo soporte con los **Servidores Intermediarios** (Proxies) transparentes imposibilitando por completo la capacidad de refrescar contenido. Si se utiliza el parámetro **ie_refresh** con valor **on** puede hacer que se verifique en los servidores de origen para nuevo contenido para todas las peticiones **IMS-REFRESH** provenientes de Internet Explorer 5.5 y versiones anteriores.

```
# Debe especificarse la IP de cualquier servidor HTTP en la
# red local
httpd_accel_host 192.168.1.254
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
ie_refresh on
```

En el caso de Squid 2.6 y versiones posteriores (**CentOS 5**, **Red Hat Enterprise Linux 5** y **White Box Enterprise Linux 5**), solo es necesario establecer **http_port 192.168.1.254:8080 transparent** (visto al inicio del documento) y descomentar **ie_refresh** con el valor **on**:

```
ie_refresh on
```

Lo más conveniente es actualizar hacia Internet Explorer 6.x o definitivamente optar por otras alternativas. **Mozilla** es en un conjunto de aplicaciones para Internet, o bien **Firefox**, que es probablemente el mejor navegador que existe en el mercado. **Firefox** es un navegador muy ligero y que **cumple con los estándares**, y está disponible para Windows, Linux, Mac OS X y otros sistemas operativos.

71.7. 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.

71.8. Iniciando, reiniciando y añadiendo 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.

71.9. 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
```

71.10. 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/

71.10.1. 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**.

71.10.2. 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
```

72. Cómo configurar Squid: Acceso por autenticación

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

72.1. 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.

72.2. 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)

72.3. 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.

72.3.1. 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
```

72.3.1.1. 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.

72.3.2. 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.

72.3.2.1. 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.

72.3.2.2. 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.

72.4. 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
```

72.4.1. Finalizando procedimiento

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

```
service squid restart
```

73. 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/

73.1. 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.

73.2. 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.

73.3. 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*.

73.4. 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
```

73.4.1. 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*.

73.4.2. Finalizando procedimiento

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

```
service squid restart
```

74. 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/

74.1. 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.

74.2. Software requerido.

Para poder llevar la cabo los procedimientos descritos en este manual y documentos relacionados, usted necesitará tener instalado al menos squid-2.5STABLE1.

74.3. Definiendo elementos de la Lista de Control de Acceso.

Lo primero será generar una lista la cual contendrá direcciones Web 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*.

74.4. 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 Sitio de Red explicado en el documento Cómo configurar Squid: Restricción de acceso a Sitio 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
```

74.4.1. Finalizando procedimiento.

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

```
service squid restart
```

75. Cómo configurar Squid: Restricción de acceso por horarios

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

75.1. 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.

75.2. 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.

75.3. 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 defición 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.

75.3.1. Más ejemplos

75.3.1.1. 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
```

75.3.1.2. 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*.

75.3.2. Finalizando procedimiento

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

```
service squid restart
```

76. Cómo configurar squid con soporte para direcciones MAC.

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

76.1. Introducción.

76.1.1. 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 equipamiento lógico **libre**, está disponible el código fuente para quien así lo requiera. de modo predeterminado no está incluido el soporte para listas de control de acceso basadas sobre direcciones **MAC** (**M**edia **A**ccess **C**ontrol).

76.2. Equipamiento lógico necesario.

76.2.1. Instalación a través de yum.

Se requiere añadir el siguiente depósito **yum** como el fichero **/etc/yum.repos.d/AL-Server.repo**. Este depósito **yum** incluye el paquete **squid-arp**, mismo que a su vez incluye soporte para listas de control de acceso basadas sobre direcciones **MAC**.

```
[AL-Server]
name=Enterprise Linux $releasever - $basearch - AL Server
mirrorlist=http://www.alcancelibre.org/al/el5/al-server
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

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 squid-arp
```

Lo anterior instalará el paquete **squid-arp** y reemplazará al paquete **squid**. El paquete **squid-arp** es idéntico al paquete **squid** con la única diferencia de que el primero fue compilado con la opción **--enable-arp-acl**.

En otras distribuciones distintas a **CentOS 5**, **Red Hat Enterprise Linux 5** o **White Box Enterprise Linux 5**, se requiere desinstalar el paquete original y descargar los fuentes de **squid**

y compilar éstos con la opción **--enable-arp-acl**.

```
./configure --enable-arp-acl
make
make install
```

76.3. Procedimientos

Este documento considera que se ha leído a detalle el documento «*Cómo configurar Squid: Parámetros básicos para servidor de intermediación (Proxy)*». Se requiere se hayan configurado al menos los siguientes parámetros:

- **http_port**, ejemplo: `http_port 8080 transparent`
- **cache_dir**, ejemplo: `cache_dir ufs /var/spool/squid 1024 16 256`
- **error_directory**, ejemplo: `error_directory /usr/share/squid/errors/Spanish`

Se requiere además determinar los valores las siguientes variables que deberán ser reemplazadas por datos reales:

- Las direcciones **MAC** especificadas en los ejemplos.
- las direcciones **MAC** de todos los equipos de la **LAN** se pueden obtener, si se está realizando las operaciones desde un servidor que sirve de puerta de enlace, utilizando el mandato **arp** con la opción **-n**, es decir: **arp -n**.
- Alternativamente, la dirección **MAC** desde una estación trabajo con Windows se puede obtener la dirección **MAC** utilizando el mandato **ipconfig** con la opción **/all**: `ipconfig /all`
- Alternativamente, la dirección **MAC** desde una estación trabajo con Linux se puede obtener la dirección **MAC** utilizando el mandato **ifconfig**.

Fichero /etc/squid/listas/macsredlocal.

Crear un fichero denominado **/etc/squid/listas/macsredlocal**

```
vi /etc/squid/listas/macsredlocal
```

Donde el contenido será una lista de direcciones **MAC** a la cual se aplicarán reglas de control de acceso. Ejemplo:

```
00:01:80:41:9C:8A
00:08:A1:84:18:AD
00:16:E3:9D:CD:77
00:04:75:AA:2D:A1
00:19:D2:6B:41:45
00:13:10:8D:4A:EE
00:19:21:14:9B:0Dr
```

76.3.1. Fichero /etc/squid/squid.conf

Se edita el fichero **/etc/squid/squid.conf**:

```
vi /etc/squid/squid.conf
```

En éste se debe configurar la lista de control de acceso con un nombre que la identifique y diferencie claramente de las demás listas, asignado el tipo de lista como **arp**. En el siguiente ejemplo, se crea la lista de control de acceso denominada **macsredlocal** de tipo **arp** y cuyos elementos que la conforman están en el fichero **/etc/squid/listas/macsredlocal**:

```
acl macsredlocal arp "/etc/squid/listas/macsredlocal"
```

Se crea una regla de control de acceso que permita a los miembros de la lista de control de acceso hacer algo. En el siguiente ejemplo se define que está permitido el acceso a la lista **macsredlocal**:

```
http_access allow macsredlocal
```

Si se creo alguna lista para limitar el acceso hacia palabras y otra para extensiones, como se describe en los documentos «*Cómo configurar Squid: Restricción de acceso a Sitios de Red*» y «*Cómo configurar Squid: Restricción de acceso a contenido por extensión*», la regla de control de acceso podría quedar de la siguiente manera:

```
http_access allow macsredlocal !porno !extensiones
```

Si además se creo alguna lista para limitar los horarios de acceso, como se describe en el documento «*Cómo configurar Squid: Restricción de acceso por horarios*», la regla de control de acceso podría quedar de la siguiente manera:

```
http_access allow matutino macsredlocal !porno !extensiones
```

Cualquier otra forma de utilizar la lista de control de acceso con direcciones **MAC** dependerá de la imaginación del administrador.

76.4. Iniciar, detener y reiniciar el servicio squid.

Para ejecutar por primera vez el servicio **squid** con las configuraciones creadas, utilice:

```
service squid start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service squid restart
```

Para detener el servicio **squid** utilice:

```
service squid stop
```

Para hacer que el servicio de **squid** esté activo con el siguiente inicio del sistema, en todos los niveles de ejecución (2, 3, 4, y 5), se utiliza lo siguiente:

```
chkconfig squid on
```

77. Cómo instalar y configurar la herramienta de reportes Sarg.

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

77.1. Introducción.

Sarg (**S**quid **A**nalysis **R**eport Generator) es la más completa y fácil de utlizar herramienta para la generación de reportes a partir de las bitácoras de **Squid**. Permite ver con detalle la activida de todos los equipos y/o usuarios dentro de la red de áreal local, registrada en la bitácora de Squid.

URL: http://sarg.sourceforge.net/.

77.2. Equipamiento lógico necesario.

Este documento fue diseñado para ser puesto en práctica exclusivamente en **CentOS 5**, **Elastix 1.5**, **Red Hat Enterprise Linux 5** y **Whitebox Enterprise Linux 5** o sistemas operativos similares, basados sobre **Red Hat Enterprise Linux 5**.

Ingrese al sistema como el usuario **root**.

Proceda a configurar el depósito YUM de Alcance Libre que incluye el paquete modificado de squid con soporte para direcciones MAC:

```
cd /etc/yum.repos.d/
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo
cd -
```

Proceda a instalar **sarg** utilizando el siguiente mandato.

```
yum -y install sarg httpd
```

77.3. Procedimientos.

Configure el soporte al español para Sarg.

Edite con vim el fichero **/etc/sarg/sarg.conf**:

```
vim /etc/sarg/sarg.conf
```

Pulse la tecla **Insert**.

Localice la cadena de texto **language English**.

```
#               Russian_koi8
#               Russian_UFT-8
#               Russian_windows1251
#               Serbian
#               Slovak
#               Spanish
#               Turkish
#
language English

# TAG:  access_log file
#       Where is the access.log file
#       sarg -l file
#
#access_log /usr/local/squid/var/logs/access.log
access_log /var/log/squid/access.log
```

Reemplace la cadena de texto con **language Spanish**.

```
#               Russian_koi8
#               Russian_UFT-8
#               Russian_windows1251
#               Serbian
#               Slovak
#               Spanish
#               Turkish
#
language Spanish

# TAG:  access_log file
#       Where is the access.log file
#       sarg -l file
#
#access_log /usr/local/squid/var/logs/access.log
access_log /var/log/squid/access.log
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

Edite con vim el fichero **/etc/httpd/conf.d/sarg.conf**:

```
vim /etc/httpd/conf.d/sarg.conf
```

Pulse la tecla **Insert**.

Localice la línea **allow from 127.0.0.1**, la cual define que solo se puede acceder hacia el directorio **/sarg/** desde **127.0.0.1** (es decir, solo puede ser accedido como *http://127.0.0.1/sarg/*).

```
Alias /sarg /var/www/sarg
<Directory /var/www/sarg>
        DirectoryIndex index.html
        order deny,allow
        deny from all
        allow from 127.0.0.1
</Directory>
```

Defina que también se puede acceder al directorio **/sarg/** desde **192.168.123.0/24**, reemplazando por **allow from 127.0.0.1 192.168.123.0/24**.

```
Alias /sarg /var/www/sarg
<Directory /var/www/sarg>
        DirectoryIndex index.html
        order deny,allow
        deny from all
        allow from 127.0.0.1 192.168.123.0/24
</Directory>
```

Defina que el acceso hacia el directorio **/sarg/** (que en adelante podrá ser accedido como *http://**proxy.red-local.net**/sarg/* o bien *http://**192.168.123.123**/sarg/*) se permitirá solo a usuarios autorizados que autenticarán a través del fichero **/var/www/claves-sarg**.

```
Alias /sarg /var/www/sarg
<Directory /var/www/sarg>
        DirectoryIndex index.html
        order deny,allow
        deny from all
        allow from 127.0.0.1 192.168.123.0/24
        AuthName "Solo usuarios autorizados."
        AuthType Basic
        require valid-user
        AuthUserFile /var/www/claves-sarg
</Directory>
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

Genere con el mandato **touch** el fichero **/var/www/claves-sarg**:

```
touch /var/www/claves-sarg
```

Utilice el mandato **chmod** para definir que el fichero **/var/www/claves-sarg** solo tendrá permisos de lectura y escritura para la clase del usuario:

```
chmod 0600 /var/www/claves-sarg
```

Utilice el mandato **chown** para definir que el fichero **/var/www/claves-sarg** pertenece al usuario apache y grupo apache:

```
chown apache:apache /var/www/claves-sarg
```

Utilice el mandato **htpasswd** sobre el fichero **/var/www/claves-sarg** para crear el usuario virtual **administrador** y asignar a éste una clave de acceso que solo deberá conocer el administrador del servidor:

```
htpasswd /var/www/claves-sarg administrador
```

Inicie (o simplemente reinicie, si es necesario) el servicio **httpd**.

```
service httpd start
```

Si el servicio **httpd** inicia normalmente, proceda con el siguiente paso. Si hay fallas o errores, regrese en los pasos que sean necesarios y corrija los posibles errores antes de continuar.

Si el servicio **httpd** inició sin errores, utilice el mandato **chkconfig** para que el servicio **httpd** inicie automáticamente la próxima vez que arranque el sistema.

```
chkconfig httpd on
```

Permita a la red de área local generar actividad en el servidor durante algunos minutos y ejecute el mandato **sarg**.

```
sarg
```

Podrá ver en reporte generado manualmente en la dirección *http://**proxy.red-local.net**/sarg/ONE-SHOT/* o bien *http://**192.168.123.123**/sarg/ONE-SHOT/*.

Podrá ver un reporte generado automáticamente todos los días en la dirección *http://**proxy.red-local.net**/sarg/daily/* o bien *http://**192.168.123.123**/sarg/daily/*.

Los reportes de almacenarán en **/var/www/sarg/**, y pueden implicar una cantidad considerable de datos. Periódicamente ingrese a los subdirectorios en el interior de éste, principalmente el subdirectorio **daily** y elimine los reportes antiguos o que sean de poca utilidad, a fin de evitar se agote el espacio en disco duro.

78. 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/

78.0.1. 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
```

79. 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/

79.1. Introducción.

79.1.1. 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/

79.1.2. 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/

79.1.3. 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

79.1.4. 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).

79.2. Conceptos requeridos.

79.2.1. ¿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.

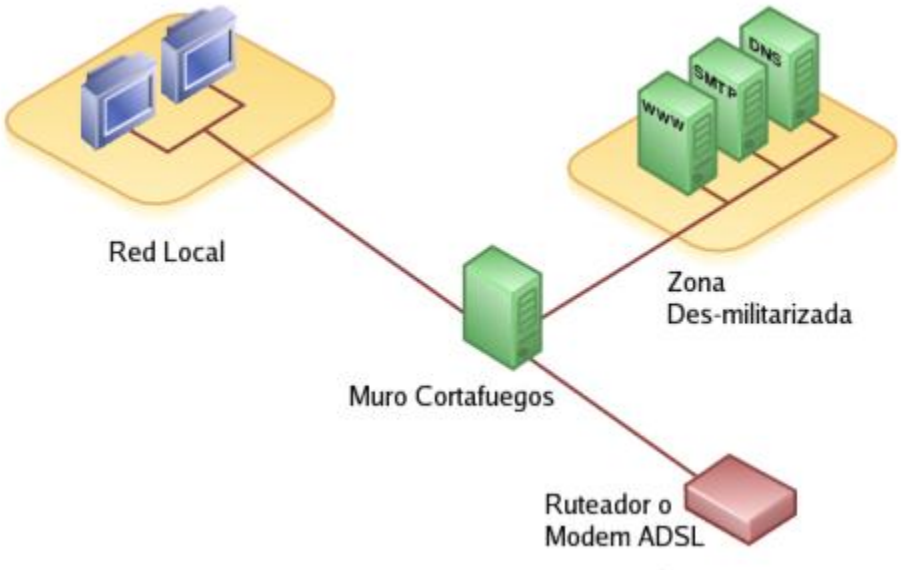


Diagrama de una Zona Desmilitarizada.
Imagen de dominio público tomada de Wikipedia y modificada con el Gimp.

79.2.2. ¿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).

79.2.3. ¿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.

79.2.4. ¿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**.

79.3. Procedimientos.

79.3.1. 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.alcancelibre.org/al/el/server/4/
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

Una vez configurado lo anterior, solo bastará utilizar:

```
yum -y install shorewall
```

79.3.2. 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
```

79.3.3. 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
```

79.3.4. 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
```

79.3.5. 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.

79.3.6. 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
```

79.3.7. 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.

79.3.7.1. 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
```

79.3.7.2. 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
```

79.3.7.3. 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
```

79.3.7.4. 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
```

79.4. 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
```

80. Cómo configurar un servidor de OpenVPN en CentOS 5

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

80.1. Introducción.

80.1.1. Acerca de OpenVPN.

OpenVPN es una solución de conectividad basada sobre equipamiento lógico (*software*): SSL(Secure Sockets Layer) VPN (Virtual Private Network, o red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación, jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre éstas el balanceo de cargas, entre otras muchas cosas más.

URL: http://openvpn.net

80.1.2. Breve explicación de lo que se logrará con este documento.

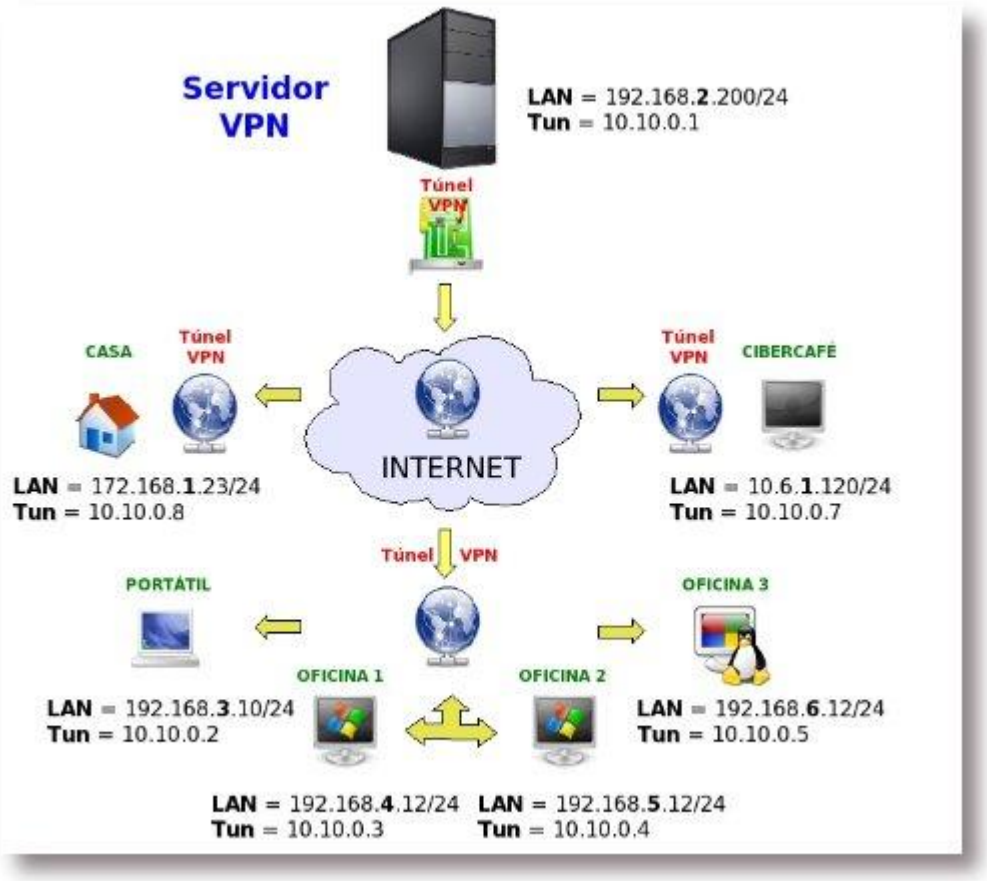
Este documento describe la configuración de una **VPN** tipo **Intranet**.

Este tipo de redes es creado entre una oficina central (servidor) y una o varias oficinas remotas (clientes). El acceso viene del exterior. Se utiliza este tipo de VPN cuando se necesita enlazar a los sitios que son parte de una compañía, en nuestro caso será compuesto por un servidor Central que conectará a muchos clientes VPN entre si.

La información y aplicaciones a las que tendrán acceso los directivos móviles en el VPN, no serán las mismas que aquellas en donde pueden acceder los usuarios que efectúan actividades de mantenimiento y soporte, esto como un ejemplo de lo que se podrá realizar con esta configuración.

Ademas de que podrá conectarse a través de **Terminal Server** (***en el caso de clientes Linux***) a terminales Windows de la red VPN así como de Clientes Windows a computadoras con el mismo sistema operativo (mediante RDP).

Nota Importante: Enfocado a esta configuración .. Una vez que los clientes (***Windows/Linux***) se conecten a la red VPN quedarán automáticamente sin conexión a Internet, lo cual NO podrán acceder a la red mundial. Esto puede ser modificable en el servidor VPN.



Servidor de Pasarela OpenVPN con clientes (Windows/Linux) remotos

El servidor VPN **hace de pasarela** para que todos los clientes (Windows/Linux) puedan estar **comunicados** a través del túnel OpenVPN, estos al conectarse por medio de Internet al túnel automáticamente quedan **sin linea**a la red mundial quedando como una **red local**, esto claro esta a través de la VPN.

Cada cliente se encuentra en lugares diferentes (ciudad/estado/país) con diferentes tipos de segmento de red, al estar conectados mediante el túnel VPN se crea un red virtual y se asigna un nuevo segmento de red proporcionada por el servidor principal en este caso con segmento (por ejemplo 10.10.0.0/255.255.255.0no 192.168.37.0/255.255.255.0).

80.2. Instalación del equipamiento lógico necesario.

Fedora 9 en adelante incluye el paquete **openvpn** en sus depósitos Yum, por lo que solo es necesario instalarlo desde la terminal a través del mandato **yum**. El siguiente procedimiento solo es necesario para **CentOS 5**.

80.2.1. Instalación en CentOS 5.

Como el usuario **root**, desde una terminal, crear el fichero **/etc/yum.repos.d/AL-Server.repo**, utilizando cualquier editor de texto. En el siguiente ejemplo se utiliza **vi**.

```
vi /etc/yum.repos.d/AL-Server.repo
```

Añadir a este **nuevo fichero** el siguiente contenido:

```
[AL-Server]
name=AL Server para Enterprise Linux $releasever
mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server
gpgcheck=1
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY
```

Importar la firma digital de **Alcance Libre** ejecutando lo siguiente desde la terminal:

```
rpm --import http://www.alcancelibre.org/al/AL-RPM-KEY
```

Instalar el equipamiento lógico (*software*) necesario,m que consiste en los paquetes RPM de OpenVPN, Shorewall y vim-enhanced (la versión mejorada de Vi):

```
yum -y install openvpn shorewall vim-enhanced
```

80.3. Procedimientos.

Si fuera necesario, cambiarse al usuario **root** utilizando el siguiente mandato:

```
su -l
```

A fin de poder utilizar inmediatamente la versión mejorada de **Vi** (instalado con el paquete **vim-enhanced**), ejecutar desde la terminal lo siguiente:

```
alias vi="vim"
```

Cambiarse al directorio, desde la terminal, ejecutar lo siguiente para cambiarse al directorio **/etc/openvpn**:

```
cd /etc/openvpn
```

NOTA: Todos los procedimientos necesarios para configurar un servidor con **OpenVPN** se realizan sin salir de **/etc/openvpn/**. Por favor, **evite cambiar de directorio** hasta haber finalizado los procedimientos descritos en este documento.

A fin de facilitar los procedimientos, se copiarán dentro del directorio **/etc/openvpn/** los ficheros **openssl.cnf**, **whichopensslcnf**, **pkitool** y **vars**, que se localizan en **/etc/openvpn/easy-rsa/2.0/**:

```
cp /usr/share/openvpn/easy-rsa/2.0/openssl.cnf ./
cp /usr/share/openvpn/easy-rsa/2.0/whichopensslcnf ./
cp /usr/share/openvpn/easy-rsa/2.0/pkitool ./
cp /usr/share/openvpn/easy-rsa/2.0/vars ./
```

Utilizar el editor de texto y abrir el fichero **/etc/openvpn/vars**:

```
vi /etc/openvpn/vars
```

De este fichero, solamente editar las últimas líneas, que corresponden a lo siguiente:

```
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
```

Reemplazar por calores reales, como los del siguiente ejemplo:

```
export KEY_COUNTRY="MX"
export KEY_PROVINCE="DF"
export KEY_CITY="Mexico"
export KEY_ORG="servidor.mi-dominio.com"
export KEY_EMAIL="fulanito@mi-dominio.com"
```

Se requiere ejecutar del siguiente modo el fichero **/etc/openvpn/vars** a fin de que carguen las variables de entorno que se acaban de configurar.

```
source /etc/openvpn/./vars
```

Cada vez que se vayan a generar nuevos certificados, debe ejecutarse el mandato anterior a fin de que carguen las variables de entorno definidas.

Se ejecuta el fichero **/usr/share/openvpn/easy-rsa/2.0/clean-all** a fin de limpiar cualquier firma digital que accidentalmente estuviera presente.

```
sh /usr/share/openvpn/easy-rsa/2.0/clean-all
```

Lo anterior realiza un **rm -fr** (eliminación recursiva) sobre el directorio **/etc/openvpn/keys**, por lo que se eliminarán todas los certificados y firmas digitales que hubieran existido con anterioridad.

A fin de crear el certificado del servidor, se crea un certificado:

```
sh /usr/share/openvpn/easy-rsa/2.0/build-ca
```

Para generar la firma digital, se utilizan los siguientes dos mandatos:

```
sh /usr/share/openvpn/easy-rsa/2.0/build-dh
sh /usr/share/openvpn/easy-rsa/2.0/build-key-server server
```

Finalmente se crean los certificados para los clientes. En el siguiente3 ejemplo se crean los certificados para **cliente1**, **cliente2**, **cliente3**, **cliente4**, **cliente5**, y **cliente6**:

```
sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente1
sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente2
sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente3
sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente4
sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente5
sh /usr/share/openvpn/easy-rsa/2.0/build-key cliente6
```

A fin de utilizar los certificados y que se configure el sistema, se crea con el editor de texto el fichero **/etc/openvpn/servidorvpn-udp-1194.conf**, donde *servidorvpn* se reemplaza por el nombre de anfitrión del sistema:

```
vi /etc/openvpn/servidorvpn-udp-1194.conf
```

Para la **VPN** se recomienda utilizar una red privada que sea poco usual, a fin de poder permitir a los clientes conectarse sin conflictos de red. Un ejemplo de una red poco utilizada sería 192.168.37.0/255.255.255.0, lo cual permitirá conectarse a la **VPN** a 253 clientes. Tomando en cuenta lo anterior, el contenido del fichero **/etc/openvpn/servidorvpn-udp-1194.conf**, debe ser el siguiente:

```
port 1194
proto udp
dev tun
#---- Seccion de llaves -----
ca keys/ca.crt
cert keys/server.crt
key keys/server.key
dh keys/dh1024.pem
#----------------------------
server 192.168.37.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status-servidorvpn-udp-1194.log
verb 3
```

Descripción de los parámetros anteriores:

Port: Especifica el puerto que será utilizado para que los clientes vpn puedan conectarse al servidor.

Proto: tipo de protocolo que se empleará en a conexión a través de VPN

dev: Tipo de interfaz de conexión virtual que se utilizará el servidor openvpn.

ca: Especifica la ubicación exacta del fichero de Autoridad Certificadora [.ca].

cert: Especifica la ubicación del fichero [.crt] creado para el servidor.

key: Especifica la ubicación de la llave [.key] creada para el servidor openvpn.

dh: Ruta exacta del fichero [.pem] el cual contiene el formato de Diffie Hellman (requirerido para **--tls-server**solamente).

server: Se asigna el rango IP virtual que se utilizará en la red del túnel VPN.

Ifconfig-pool-persist: Fichero en donde quedarán registrado las direcciones IP de los clientes que se encuentran conectados al servidor OpenVPN.

Keepalive 10 120 : Envía los paquetes que se manejan por la red una vez cada 10 segundos; y asuma que el acoplamiento es abajo si ninguna respuesta ocurre por 120 segundos.

comp-lzo: Especifica los datos que recorren el túnel vpn será compactados durante la trasferencia de estos paquetes.

persist-key: Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.

Persist-tun: Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down

status: fichero donde se almacenará los eventos y datos sobre la conexión del servidor [.log]

verb: Nivel de información (default=1). Cada nivel demuestra todo el Info de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.

0 --No muestra una salida excepto errores fatales. **1 to 4 –**Rango de uso normal. **5 --**Salida **R**y **W**caracteres en la consola par los paquetes de lectura y escritura, mayúsculas es usada por paquetes TCP/UDP minúsculas es usada para paquetes TUN/TAP.

Si **SELinux** está activo, es necesario que el directorio **/etc/openvpn** y sus contenidos, tengan los contextos apropiados de esta implementación de seguridad (system_u:object_r:**openvpn_etc_rw_t** para **ipp.txt** y **openvpn-status-servidorvpn-udp-1194.log** y system_u:object_r:**openvpn_etc_t** para el resto del contenido del directorio).

Se utiliza luego el mandato **restorecon** sobre el directorio **/etc/openvpn** a fin de asignar los contextos adecuados.

```
restorecon -R /etc/openvpn/
```

Se crean los ficheros **ipp.txt** y **openvpn-status-servidorvpn-udp-1194.log**:

```
cd /etc/openvpn/
touch ipp.txt
touch openvpn-status-servidorvpn-udp-1194.log
```

Estos últimos dos ficheros requieren se les asigne contexto de lectura y escritura (**openvpn_etc_rw_t**).

```
cd /etc/openvpn/
chcon -u system_u -r object_r -t openvpn_etc_rw_t ipp.txt
chcon -u system_u -r object_r -t openvpn_etc_rw_t openvpn-status-servidorvpn-udp-1194.log
```

Los anterior cambia los contextos a usuario de sistema (**system_u**), rol de objeto (**object_r**) y tipo configuración de OpenVPN de lectura y escritura (**openvpn_etc_rw_t**).

Para iniciar el servicio, se utiliza el mandato **service** del siguiente modo:

```
service openvpn start
```

Para que el servicio de OpenVPN esté activo en el siguiente inicio del sistema, se utiliza el mandato **chkconfig** de la siguiente forma:

```
chkconfig openvpn on
```

80.3.1. Configuración de muro cortafuegos con Shorewall.

El siguiente procedimiento considera que se ha configurado un muro cortafuegos apropiadamente, de acuerdo a las indicaciones descritas en el documento titulado **Cómo configurar un muro cortafuegos con Shorewall y tres interfaces de red**.

Independientemente del contenido, en el fichero **/etc/shorewall/zones**, se añade la zona **rem** con el tipo **ipv4**, antes de la última línea.

```
# OpenVPN ----
rem     ipv4
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Independientemente del contenido, en el fichero **/etc/shorewall/interfaces**, se añade la zona **rem** asociada a la interfaz **tun0**, con la opción **detect**, para detectar automáticamente el número de dirección **IP** de difusión (*broadcast*) y la opción **dhcp**. También debe definirse antes de la última línea del fichero.

```
# OpenVPN ----
rem     tun0            detect          dhcp
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Independientemente del contenido, en el fichero **/etc/shorewall/policy**, se añade la política deseada para permitir el acceso de los miembros de la **VPN** hacia las zonas que se consideren apropiadas. En el siguiente ejemplo, se define una política que permite el acceso de las conexiones originadas desde la zona **rem** hacia el cortafuegos, la red pública y la red local. Todo debe definirse antes de la última línea del fichero.

```
fw              all             ACCEPT
loc             all             ACCEPT
# OpenVpn ----
rem             fw              ACCEPT
rem             net             ACCEPT
rem             loc             ACCEPT
# ------------
net             all             DROP    info
all             all             REJECT  info
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Independientemente del contenido, en el fichero **/etc/shorewall/rules**, se debe abrir el puerto 1194 por UDP en el cortafuegos para las zonas desde las cuales se pretenda conectar clientes a la **VPN**

```
ACCEPT  net                     fw                      udp     1194
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Finalmente, se edita el fichero **/etc/shorewall/tunnels** a fin de definir el túnel SSL que será utilizado para el servidor de **VPN** y que permita conectarse desde cualquier ubicación.

```
#TYPE                   ZONE    GATEWAY         GATEWAY
#                                               ZONE
openvpnserver:1194      rem     0.0.0.0/0
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

En lugar de **0.0.0.0/0**, se puede especificar una dirección IP o bien una red desde la cual se quiera establecer las conexiones **VPN**.

Para aplicar los cambios, es necesario reiniciar **shorewall** con el mandato **service**, del siguiente modo:

```
service shorewall restart
```

80.3.2. Configuración de clientes Windows.

80.3.2.1. A través de OpenVPN GUI.

Instalar **OpenVPN GUI** desde http://openvpn.se/. Se requiere instalar la versión de desarrollo

1.0.3 de **OpenVPN GUI**, compatible con OpenVPN 2.1.x. El cliente es **estable**, siempre que se verifique que funcione adecuadamente la configuración utilizada antes de poner en marcha en un entorno productivo.

Crear el fichero **cliente1-udp-1194.ovpn**, con el siguiente contenido, donde es importante que las rutas definidas sean las correctas, y las diagonales invertidas sean dobles:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
#------ SECCION DE LLAVES --------
ca "C:\\Archivos de Programa\\OpenVPN\\config\\ca.crt"
cert "C:\\Archivos de Programa\\OpenVPN\\config\\cliente1.crt"
key "C:\\Archivos de Programa\\OpenVPN\\config\\cliente1.key"
ns-cert-type server
#---------------------------------
comp-lzo
verb 3
```

Descripción de los parámetros anteriores:

client: Especifica el tipo de configuración, en este caso tipo cliente OpenVPN.

Port: Especifica el puerto que será utilizado para que los clientes VPN puedan conectarse al servidor.

Proto: tipo de protocolo que se empleará en a conexión a través de VPN

dev: Tipo de interfaz de conexión virtual que se utilizará el servidor openvpn.

remote: Host remoto o dirección IP en el cliente, el cual especifica al servidor OpenVPN.

El cliente OpenVPN puede tratar de conectar al servidor con **host:port** en el orden especificado de las opciones de la opción **--remote**.

float: Este le dice a OpenVPN aceptar los paquetes autenticados de cualquier dirección, no solamente la dirección cuál fue especificado en la opción **--remote**.

resolv-retry: Si la resolución del nombre del anfitrión (*hostname*) falla para **-- remote**, la resolución antes de fallar hace una re-comprobación de n segundos.

nobind: No agrega bind a la dirección local y al puerto.

ca: Especifica la ubicación exacta del fichero de Autoridad Certificadora [.ca].

cert: Especifica la ubicación del fichero [.crt] creado para el servidor.

key: Especifica la ubicación de la llave [.key] creada para el servidor OpenVPN.

remote: Especifica el dominio o IP del servidor así como el puerto que escuchara las peticiones para servicio VPN.

comp-lzo: Especifica los datos que recorren el túnel VPN será compactados durante la trasferencia de estos paquetes.

persist-key: Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.

Persist-tun: Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down

verb: Nivel de información (default=1). Cada nivel demuestra toda la Información de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.

0 --No muestra una salida excepto errores fatales. **1 to 4 –**Rango de uso normal. **5 --**Salida **R**y **W**caracteres en la consola par los paquetes de lectura y escritura, mayúsculas es usada por paquetes TCP/UDP minúsculas es usada para paquetes TUN/TAP.

El cliente necesitará que los ficheros **ca.crt**, **cliente1.crt**, **cliente1.key** y **cliente1-udp-1194.ovpn** estén presentes en el directorio **"C:\Archivos de Programa\OpenVPN\config\"**. Estos ficheros fueron creados, a través de un procedimiento descrito en este documento, dentro del directorio **/etc/openvpn/keys/** del servidor.

Si se quiere que los clientes de la **VPN** se puedan conectar a la red local, es importante considerar las implicaciones de seguridad que esto conlleva si alguno de los certificados es robado, o bien el cliente se ve comprometido en su seguridad por una intrusión, virus, troyano o gusano. Es preferible que la red de la **VPN** sea independiente a la red local y cualquier otra red, uniendo los servidores y clientes a la **VPN**, independientemente de si éstos están en la red local o una red pública.

Si es imperativo hacer que los clientes de la **VPN** se conecten a la red local, la red desde la cual se conectan los clientes debe ser diferente a la red utilizada en la red local. Por ejemplo: si la red local detrás del servidor de **VPN** es 192.168.0.0/255.255.255.0, 10.0.0.0/255.0.0.0 o 172.16.0.0/255.255.0.0, los clientes que se conecten a la **VPN** detrás de un modem ADSL o Cable e intenten establecer conexiones con la red local, muy seguramente tendrán conflictos de red.

Para permitir a los clientes de la **VPN** poder establecer conexiones hacia la red local, se añaden las siguientes líneas en el fichero de configuración de OpenVPN para los clientes, y que definen la ruta para la red local y un servidor DNS que debe estar presente y configurado para permitir **consultas recursivas** a la red de la **VPN**:

```
route 192.168.0.0 255.255.255.0
dhcp-option DNS 192.168.0.1
```

Opcionalmente, también se puede definir un servidor Wins.

```
dhcp-option WINS 192.168.26.1
```

Ejemplo, considerando que la red local es **192.168.26.0/255.255.255.0**:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
route 192.168.26.0 255.255.255.0
dhcp-option DNS 192.168.26.1
dhcp-option WINS 192.168.26.1
#------ SECCION DE LLAVES --------
ca "C:\\Archivos de Programa\\OpenVPN\\config\\ca.crt"
cert "C:\\Archivos de Programa\\OpenVPN\\config\\cliente1.crt"
key "C:\\Archivos de Programa\\OpenVPN\\config\\cliente1.key"
ns-cert-type server
#---------------------------------
comp-lzo
```

```
verb 3
```

80.3.3. Clientes GNU/Linux.

80.3.3.1. A través del servicio openvpn.

Este es el método que funcionará en prácticamente todas las distribuciones de de GNU/Linux basadas sobre **Red Hat**, **CentOS** y **Fedora**. Se requiere instalar el paquete **openvpn**:

```
yum -y install openvpn
```

Para **CentOS 5**, se requiere haber configurado previamente el depósito de **AL Server**, descrito con anterioridad en este mismo documento.

Para los clientes con GNU/Linux utilizando el servicio **openvpn**, básicamente se utiliza el mismo fichero para **OpenVPN GUI** para Windows, pero definiendo rutas en el sistema de ficheros de GNU/Linux. Ejemplo:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
#------ SECCION DE LLAVES --------
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/cliente1.crt
key /etc/openvpn/keys/cliente1.key
ns-cert-type server
#---------------------------------
comp-lzo
verb 3
```

Este fichero se guarda como **/etc/openvpn/cliente1-udp-1194.ovpn**. Requiere que los certificados definidos en la configuración estén en las rutas especificadas dentro del directorio **/etc/openvpn/keys/**.

Para iniciar la conexión hacia la **VPN**, simplemente se inicia el servicio **openvpn**:

```
service openvpn start
```

Para que la conexión se establezca automáticamente cada vez que se inicie el sistema, se utiliza el mandado **chkconfig** de la siguiente manera:

```
chkconfig openvpn on
```

80.3.3.2. A través de NetworkManager.

NetworkManager es una implementación que permite a los usuarios configurar interfaces de red de todos los tipos, sin necesidad de contar con privilegios de administración en el sistema. Es

la forma más flexible, sencilla y práctica de conectarse a una red **VPN**.

Se requiere que los clientes Linux tengan instalado el paquete **NetworkManager-openvpn**, mismo que debe estar incluido en los depósitos Yum de **Fedora 9** en adelante y distribuciones recientes de GNU/Linux. **CentOS 5** carece del soporte para utilizar **NetworkManager-openvpn**, por lo que solo podrá conectarse a la **VPN** a través del método anterior, con el servicio **openvpn**.

Para instalar a través del mandato **yum** en distribuciones basadas sobre **Fedora 9** en adelante, se hace de la siguiente manera:

```
yum -y install NetworkManager-openvpn
```

Se puede reiniciar el sistema para que tengan efectos los cambios, o simplemente reiniciar el servicio **NetworkManager**:

```
service NetworkManager restart
```

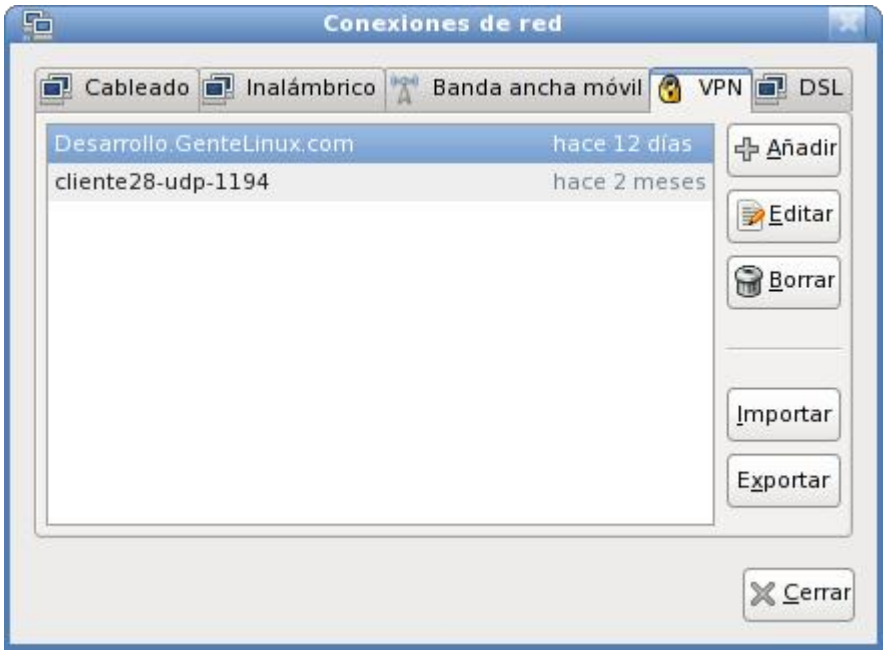
Lo anterior cerrará y volverá a establecer las conexiones de red existentes.

Al igual que el método anterior, para los clientes con GNU/Linux con NetworkManager, básicamente se utiliza el mismo fichero para **OpenVPN GUI** para Windows, pero definiendo rutas en el sistema de ficheros de GNU/Linux. Ejemplo:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
#------ SECCION DE LLAVES --------
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/cliente1.crt
key /etc/openvpn/keys/cliente1.key
ns-cert-type server
#--------------------------------
comp-lzo
verb 3
```

Este fichero se puede utilizar con la interfaz gráfica de **NetworkManager**. Solo hay que hacer clic sobre el icono en el **Área de notificación** del panel de GNOME y luego hacer clic en **Configurar VPN**.

En la ventana que abre a continuación, hay un botón que permite importar el fichero de configuración.



Si los certificados y firma digital son colocados en la ruta **/etc/openvpn/keys/** con SELinux activo, éstos funcionarán adecuadamente. Si los certificados y firma digital son almacenados dentro del directorio de inicio del usuarios, es necesario establecer la política **openvpn_enable_homedirs** con valor **1** (que equivale a **on**, o activa):

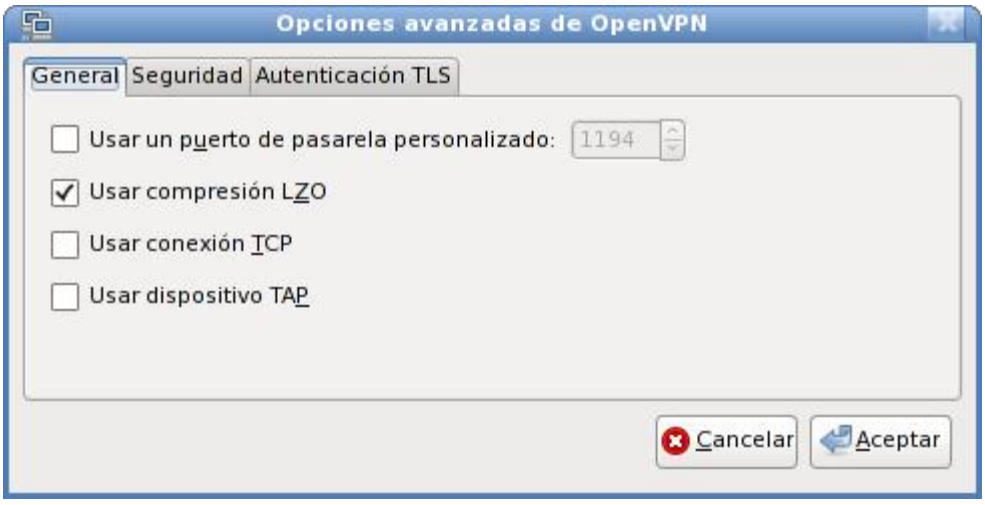
```
setsebool -P openvpn_enable_homedirs 1
```

Personalmente recomiendo crear una configuración nueva desde la interfaz de **NetworkManager**. Desde la ventana de redes VPN de la interfaz de **NetworkManager**, hacer clic en **Añadir**.

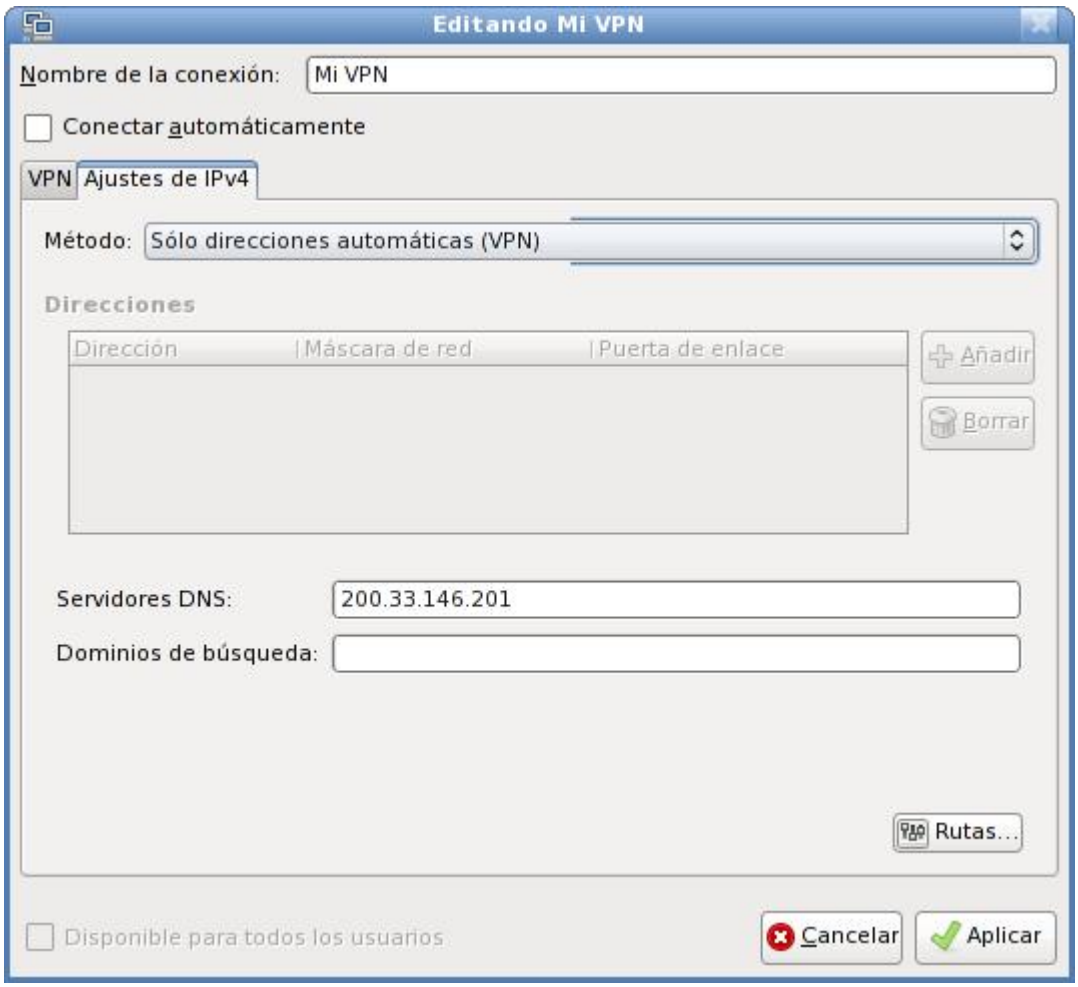
Aparecerá un diálogo donde se debe seleccionar que se trata de una **VPN** con **OpenVPN**.

En la siguiente ventana de diálogo, se define el nombre de la conexión, dirección IP o nombre del servidor donde está instalado OpenVPN, y los certificados a utilizar. Si se siguieron los procedimientos de ese documento, se **deja en blanco** el campo **Contraseña de clave privada**.

Luego, se hace clic en **Avanzado** para especificar que se utilizará compresión **LZO**.



Para evitar conflictos de conectividad, se hace clic en la pestaña **Ajustes IPV4**, y se define un servidor DNS que permita al cliente navegar a través de Internet y dentro de la red de la **VPN**.



Se hace clic en **Rutas** para abrir otra ventana de diálogo y se seleccionan las casillas de las opciones **Ignorar las rutas obtenidas automáticamente** y **Usar esta conexión solo para los recursos de su red**. Opcionalmente se pueden añadir las rutas estáticas para tener conectividad con la red local detrás del servidor de **VPN**, tomando en cuenta que la red local desde la cual se está conectado el cliente debe ser diferente a la de la red local detrás del servidor de **VPN**, a fin de evitar conflictos de red.

Finalmente se hace clic en aplicar. Para conectarse a la red **VPN**, solo basta hacer clic sobre el icono de **NetworkManager** en el **Área de notificación** del panel de GNOME y seleccionar la red **VPN** recién configurada.

80.4. Bibiliografía.

Este documento se basa sobre los manuales titulados VPN en servidor Linux y clientes Windows/Linux con OpenVPN + Shorewall [Parte 1] y VPN en servidor Linux y clientes Windows/Linux con OpenVPN + Shorewall [Parte 2], por **William López Jiménez**, publicados en **Alcance Libre**, cumpliendo cabalmente con los términos de la licencia **Creative Commons** Reconocimiento-NoComercial-CompartirIgual 2.1.

81. Cómo configurar SNMP.

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

81.1. Introducción.

81.1.1. 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.

81.1.2. 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/

81.2. Equipamiento lógico necesario.

81.2.1. 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
```

81.2.2. 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
```

81.3. 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
```

81.3.1.1. 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).

81.3.1.2. 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
```

81.3.1.3. 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
```

81.3.1.4. 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
```

81.3.1.5. 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)
```

81.3.2. 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
  ```

81.3.3. 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
```

81.3.4. 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 ejecución (2, 3, 4, y 5), se utiliza lo siguiente:

```
chkconfig snmpd on
```

81.4. 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
```

81.5. 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
```

82. Cómo configurar MRTG.

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

82.1. Introducción.

82.1.1. 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.

82.2. Equipamiento lógico necesario.

82.2.1. 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
```

82.2.2. 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
```

82.3. 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
```

82.4. 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.

83. Cómo instalar Java 1.5 en CentOS 5.

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

83.1. Introducción.

De modo predeterminado, **CentOS 5** y **Red Hat™ Enterprise Linux 5** incluyen la versión 1.4.2 de Java por GNU.org. Sin embargo, algunos desarrollos, sobre todo aplicaciones comerciales para **Apache Tomcat**, pueden requerir utilizar una versión distinta de Java. Este documento explica como instalar **JDK 1.5.0** de **Sun Microsystems** en **CentOS 5** y **Red Hat™ Enterprise Linux 5**.

83.2. Instalación del equipamiento lógico necesario.

83.2.1. Instalación a través de yum.

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 rpm-build gcc gcc-c++ redhat-rpm-config automake autoconf
```

83.3. Procedimientos.

83.3.1. Creación de usuario para utilizar rpmbuild.

Es poco conveniente y representa un alto riego utilizar rpmbuild como **root**. Por lo tanto es recomendable crear una cuenta de usuario destinada exclusivamente a utilizar el mandato **rpmbuild**.

```
su - root
useradd rpmbuilduser
passwd rpmbuilduser
```

83.3.2. Creación de estructura de directorios para rpmbuild.

A fin de poder trabajar cómodamente, se creará como usuario un conjuto de directorios que serán utilizados para crear paquetería RPM.

```
su - rpmbuilduser
mkdir -p ~/rpmbuild/{SOURCES,SRPMS,SPECS,RPMS,TMP,BUILD}
```

Utilizando **vi**, o cualquier otro editor detexto, configure el fichero **~/.rpmmacros** con el siguiente

contenido:

```
%_topdir /home/rpmbuilduser/rpmbuild
%_tmppath %{_topdir}/TMP
%_unpackaged_files_terminate_build 0
%packager               Mi nombre
%distribution           Mi distribución o área de trabajo.
%vendor                 Mi empresa.
```

Descargar el fichero **java-1.5.0-sun-1.5.0.15-1jpp.nosrc.rpm**, o bien una versión posterior a la edición de este documento, localizado en **http://mirrors.dotsrc.org/jpackage/5.0/generic/non-free/SRPMS/**.

A continuación, se debe descargar la más reciente versión de JDK de Sun Microsystems desde http://java.sun.com/products/archive/

Hacer ejecutable el fichero descargado utilizando el siguiente mandato:

```
chmod +x jdk-1_5_0_15-linux-i586.bin
```

Mover éste último dentro de **~/rpmbuild/SOURCES/**

```
mv jdk-1_5_0_15-linux-i586.bin ~/rpmbuild/SOURCES/
```

Reconstruir el paquete **java-1.5.0-sun-1.5.0.15-1jpp.nosrc.rpm** para generar los paquetges de Java 1.5.

```
rpmbuild --rebuild java-1.5.0-sun-1.5.0.15-1jpp.nosrc.rpm
```

Lo anterior, luego de algunos minutos, generará dentro del directorio **~/rpmbuild/RPMS/i586/** los siguientes paquetes:

- java-1.5.0-sun-1.5.0.15-1jpp.i586.rpm
- java-1.5.0-sun-alsa-1.5.0.15-1jpp.i586.rpm
- java-1.5.0-sun-demo-1.5.0.15-1jpp.i586.rpm
- java-1.5.0-sun-devel-1.5.0.15-1jpp.i586.rpm
- java-1.5.0-sun-fonts-1.5.0.15-1jpp.i586.rpm
- java-1.5.0-sun-jdbc-1.5.0.15-1jpp.i586.rpm
- java-1.5.0-sun-plugin-1.5.0.15-1jpp.i586.rpm
- java-1.5.0-sun-src-1.5.0.15-1jpp.i586.rpm

Para instalar, cambiarse al directorio **~/rpmbuild/RPMS/i586/** e instalar solo la paquetería requerida. Ejemplo:

```
cd ~/rpmbuild/RPMS/i586/
su
rpm -Uvh java-1.5.0-sun-1.5.0.15-1jpp.i586.rpm java-1.5.0-sun-alsa-1.5.0.15-
1jpp.i586.rpm java-1.5.0-sun-fonts-1.5.0.15-1jpp.i586.rpm java-1.5.0-sun-plugin-
1.5.0.15-1jpp.i586.rpm
exit
```

De modo predeterminado, el sistema utiliza la versión 1.4.2 de GNU.org.Se puede definir desde la terminal que versión de Java utilizar a través delmandato **alternatives** con la opción **--config**

java.

```
/usr/sbin/alternatives --config java
```

Lo anterior devuelve una salida similar a la siguiente:

```
Hay 2 programas que proporcionan 'java'.

  Selección    Comando
-----------------------------------------------
*+ 1           /usr/lib/jvm/jre-1.4.2-gcj/bin/java
   2           /usr/lib/jvm/jre-1.5.0-sun/bin/java

Presione Intro para mantener la selección actual[+], o escriba el
número de la selección:
```

Seleccione la versión **1.5** de de **Sun Microsystems** pulsando la tecla del número 2 y luego la tecla **ENTER**.

Para verificar que la versión de Java 1.5 ha sido instalada correctamente, solo basta ejecutar el siguiente mandato:

```
java -version
```

Para finalizar, si el sistema dispone de **Mozilla Firefox**, se puede configurar el complemento Java (Plugin Java) creando un enlace simbólico de **/usr/lib/jvm/jre-1.5.0-sun/plugin/i386/ns7/libjavaplugin_oji.so** dentro de **/usr/lib/mozilla/plugins/** de la siguiente manera:

```
ln -s /usr/lib/jvm/jre-1.5.0-sun/plugin/i386/ns7/libjavaplugin_oji.so
/usr/lib/mozilla/plugins/
```

84. Cómo instalar la complemento (plug-in) Flash Player para Firefox y otros navegadores.

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

84.1. Introducción

Los procedimientos descritos permitirán desde los navegadores Firefox, Epiphany, Galeon, Opera y Konqueror visualizar contenido de Internet hecho para Adobe™ Flash Player 10 (y versiones anteriores de éste) y Adobe™ FlashMX con extensiones *.swf y *.spl.

La versión 10 de Flash Player solo es compatible con **CentOS 5** y **Red Hat Enterprise Linux 5**, y versiones posteriores de éstos, así como versiones recientes de **Fedora**. **CentOS 4** y **Red Hat Enterprise Linux 4**, y las versiones anteriores de éstos, solo puede utilizar Flash Player 9.

84.2. Procedimientos.

84.2.1. Fedora, CentOS 5 y Red Hat Enterprise Linux 5.

84.2.1.1. Desde el navegador.

Simplemente acceda con el navegador hacia el siguiente enlace:

- **http://linuxdownload.adobe.com/adobe-release/adobe-release-i386-1.0-1.noarch.rpm**

Permita que el gestor de paquetes del sistema se encargue de la instalación proporcionado la clave de acceso del administrador del sistema.

84.2.1.2. Desde terminal de texto.

Abra una terminal de texto y cambie a **root** de la siguiente forma:

```
su -l
```

Descargue el fichero **adobe-release-i386-1.0-1.noarch.rpm** utilizando el siguiente mandato:

```
wget http://linuxdownload.adobe.com/adobe-release/adobe-release-i386-1.0-1.noarch.rpm
```

Instale el fichero **adobe-release-i386-1.0-1.noarch.rpm** utilizando el mandato **yum** de la siguiente manera:

```
yum -y localinstall adobe-release-i386-1.0-1.noarch.rpm
```

Una vez realizado lo anterior, se procede a instalar el complemento Flash Player utilizando el siguiente mandato:

```
yum -y install flash-plugin
```

84.2.2. CentOS 4 y Red Hat Enterprise Linux 4.

Para CentOS 4 y Red Hat Enterprise Linux 4, y versiones anteriores de éstos, solo es posible hacer la instalación de Flash Player 9 desde terminal de texto.

Abra una terminal de texto y cambie a **root** de la siguiente forma:

```
su -l
```

Ejecute el siguiente mandato parta instalar el paquete **compat-libstdc++-33** del cual depende el complemento de Flash Player 9:

```
yum -y install compat-libstdc++-33
```

Descargue el fichero **install_flash_player_9.tar.gz** utilizando el siguiente mandato:

```
wget
http://download.macromedia.com/pub/flashplayer/installers/current/9/install_flash_pla
yer_9.tar.gz
```

Descomprimir el fichero **install_flash_player_9.tar.gz** utilizando el mandato **tar** de la siguiente manera:

```
tar zxvf install_flash_player_9.tar.gz
```

Cambiarse al directorio descomprimido **install_flash_player_9_linux** utilizando el siguiente mandato:

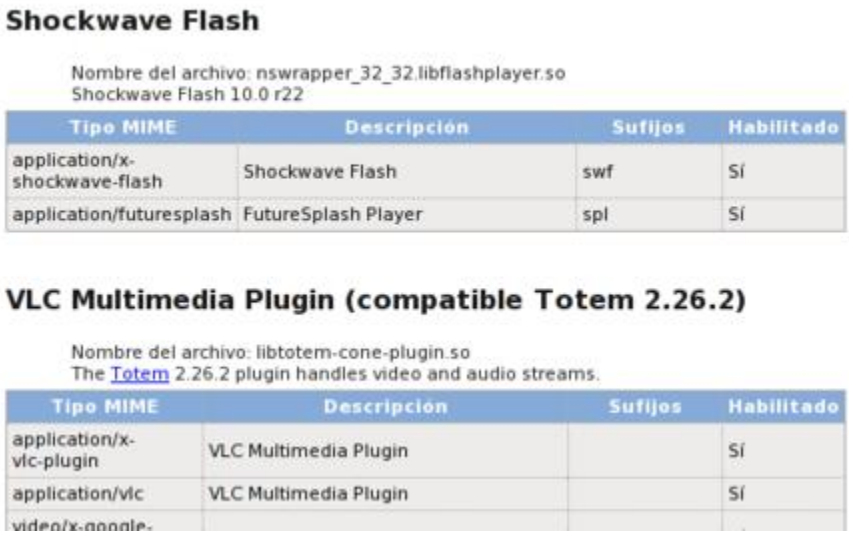
```
cd install_flash_player_9_linux
```

Copie el fichero **libflashplayer.so** dentro del directorio **/usr/lib/mozilla/plugins/** utilizando el siguiente mandato:

```
cp libflashplayer.so /usr/lib/mozilla/plugins/
```

84.3. Comprobaciones.

Abra Firefox, Epiphany o Galeon y en la barra de direcciones tecle **about:plugins**. Pulse la tecla <ENTER>. Deberá aparecer la información acerca de los complementos instalados para el navegador, y entre éstos deberá aparecer la información correspondiente al complemento (*plug-in*) Adobe™ Flash.



Shockwave Flash

Nombre del archivo: nswrapper_32_32.libflashplayer.so
Shockwave Flash 10.0 r22

Tipo MIME	Descripción	Sufijos	Habilitado
application/x-shockwave-flash	Shockwave Flash	swf	Sí
application/futuresplash	FutureSplash Player	spl	Sí

VLC Multimedia Plugin (compatible Totem 2.26.2)

Nombre del archivo: libtotem-cone-plugin.so
The Totem 2.26.2 plugin handles video and audio streams.

Tipo MIME	Descripción	Sufijos	Habilitado
application/x-vlc-plugin	VLC Multimedia Plugin		Sí
application/vlc	VLC Multimedia Plugin		Sí
video/x-google-			

Información sobre el complemento de Adobe™ Flash.

85. Cómo configurar escáner en red

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

85.1. Introducción.

85.1.1. 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/

85.1.2. 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/

85.2. Equipamiento lógico necesario.

85.2.1. Instalación del servicio saned.

85.2.1.1. 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
```

85.2.1.2. 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
```

85.2.2. Instalación del cliente Xsane.

85.2.2.1. 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
```

85.2.2.2. 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
```

85.3. Procedimientos

85.3.1. 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.

85.3.2. 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.

86. 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/

86.1. 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**).

86.2. 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 selective`	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.
-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
```

87. Cómo crear un disco con instalación personalizada de CentOS 5.

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

87.1. Instalación de equipamiento lógico necesario.

Se requiere la herramienta **mkisofs** para poder crear imágenes ISO, la herramienta system-config-kickstart para crear un fichero de configuración con parámetros personalizados para el programa de instalación, y el mandato **createrepo** para regenerar el depósito yum en caso de que se añadan paquetes nuevos o actualizados a la instalación.

```
yum -y install mkisofs system-config-kickstart createrepo
```

La herramienta **system-config-kickstart** esta incluida en todas las versiones de **CentOS**, **Fedora** y **Red Hat Enterprise Linux**, así como las distribuciones de GNU/Linux derivadas de éstas.

87.2. Procedimientos.

87.2.1. Creación de fichero de configuración de instalación personalizada.

Se utiliza el programa **system-config-kickstart**, que consiste en un programa que simula las opciones de configuración del programa de instalación de CentOS 5. Al finalizar, se guarda un fichero, que puede ser nombrado como **ks.cfg**,y que será utilizado posteriormente en este documento.

Si se carece de **system-config-kickstart** o bien ésta tiene un mal funcionamiento, lo siguiente corresponde a una configuración de ejemplo que establece la instalación desde **la unidad lectora de CD/DVD**, instalación en idioma **español**, con teclado con disposición **Español**, interfaz **eth0** configurada por **DHCP**, clave de acceso para el usuario root será **123qwe**, cortafuegos habilitado con el puerto 22 por TCP abierto, SELinux funcionará en modo **enforcing**, zona horaria de la **ciudad de México**, instalación de grub en **/dev/sda**, y la instalación de los grupos de paquetes **Core** (núcleo y componentes básicos del sistema operativo), **Base**(herramientas básicas del sistema operativo), **Editors** (editores de texto), **Fonts** (tipografías), **GNOME Desktop** (escritorio de GNOME), **Graphical Internet** (programas gráficos para Internet), **Java** (soporte para Java), **Office** (OpenOffice.org y otros programas para documentos), **Printing** (soporte para impresión), **Sound and Video** (programas para sonodo y vídeo) y **Spanish Support** (soporte al español):

```
# Kickstart file automatically generated by anaconda.
```

```
install
cdrom
lang es_ES.UTF-8
keyboard es
network --device eth0 --bootproto dhcp
rootpw --iscrypted $1$Fvs3oU5c$4ff89riowPb1EmJ7O.QtD0
firewall --enabled --port=22:tcp
authconfig --enableshadow --enablemd5
selinux --enforcing
timezone --utc America/Mexico_City
bootloader --location=mbr --driveorder=sda
# The following is the partition information you requested
# Note that any partitions you deleted are not expressed
# here so unless you clear all partitions first, this is
# not guaranteed to work
#clearpart --linux
#part /boot --fstype ext3 --size=200 --onpart=sda1
#part / --fstype ext3 --size=1024 --ondisk=sda2 --grow --maxsize=55000
#part swap --ondisk=sda3 --size=2048
%packages
@base
@core
@editors
@fonts
@gnome-desktop
@graphical-internet
@java
@office
@printing
@sound-and-video
@spanish-support
```

Lo anterior solo deja la configuración de particiones como único procedimiento a realizar durante la instalación. Se recomienda dejar de este modo a fin de evitar eliminación accidental de particiones existentes en el disco duro.

87.2.2. Creación del directorio de trabajo y contenido del mismo.

El primer paso consiste en crear un directorio de trabajo donde haya espacio suficiente, es decir aproximadamente 3.6 GB para el directorio de trabajo y otros 3.6 GB para crear la nueva imagen de DVD. Por tanto, se requiere un mínimo de 7.2 GB de espacio libre en disco duro. En el siguiente ejemplo se utiliza **~/centos5-personal**:

```
mkdir ~/centos5-personal
```

Se inserta el DVD de CentOS 5 y se deja que el sistema asigne el punto de montaje dentro de /media/ o bien se monta manualmente. Si se monta manualmente, se puede utilizar el siguiente procedimiento:

```
mkdir /media/centos5
mount /dev/cdrom /media/centos5
```

Se copia completo el contenido del DVD de CentOS 5 en el directorio de trabajo definido previamente:

```
cp -r /media/centos5/* ~/centos5-personal/
```

También se debe copiar también el fichero **.discinfo** que está en el DVD.

```
cp -r /media/centos5/.discinfo ~/centos5-personal/
```

Corregir el fichero **.discinfo** que se copió dentro de **~/centos5-personal/**, con cualquier editor de texto, y cambiar **/home/buildcentos/CENTOS/5.2/en/i386/CentOS** por **CentOS/CentOS**

Copiar el fichero **ks.cfg** creado con **system-config-kickstart** dentro del directorio de trabajo **~/centos5-personal/**:

```
cp /donde/este/ks.cfg ~/centos5-personal/
```

Editar el fichero **~/centos5-personal/isolinux/isolinux.cfg** y añadir el parámetro **ks=cdrom:/ks.cfg** a la definición que se desee utilizar por omisión. Por ejemplo, se tiene el siguiente contenido en isolinux.cfg:

```
default linux
prompt 1
timeout 600
display boot.msg
F1 boot.msg
F2 options.msg
F3 general.msg
F4 param.msg
F5 rescue.msg
label linux
  kernel vmlinuz
  append initrd=initrd.img
label text
  kernel vmlinuz
  append initrd=initrd.img text
label ks
  kernel vmlinuz
  append ks initrd=initrd.img
label local
  localboot 1
label memtest86
  kernel memtest
  append -
```

Solo se necesita añadir **ks=cdrom:/ks.cfg** a la primera línea de **append**, que corresponde al arranque predeterminado del disco de instalación.

```
default linux
prompt 1
timeout 600
display boot.msg
F1 boot.msg
F2 options.msg
F3 general.msg
F4 param.msg
F5 rescue.msg
label linux
  kernel vmlinuz
  append initrd=initrd.img ks=cdrom:/ks.cfg
label text
  kernel vmlinuz
```

```
  append initrd=initrd.img text
label ks
  kernel vmlinuz
  append ks initrd=initrd.img
label local
  localboot 1
label memtest86
  kernel memtest
  append -
```

Puede resultar más conveniente añadir una **nueva definición de arranque**, a fin de que se deje intacto el arranque por defecto, y alternativamente se pueda cargar el fichero **ks.cfg** al invocar desde el dialogo de **boot:** esta definición.

```
default linux
prompt 1
timeout 600
display boot.msg
F1 boot.msg
F2 options.msg
F3 general.msg
F4 param.msg
F5 rescue.msg
label linux
  kernel vmlinuz
  append initrd=initrd.img
label text
  kernel vmlinuz
  append initrd=initrd.img text
label ks
  kernel vmlinuz
  append ks initrd=initrd.img
label local
  localboot 1
label memtest86
  kernel memtest
  append -
label mi-arranque
  kernel vmlinuz
  append initrd=initrd.img ks=cdrom:/ks1.cfg
```

Para utilizar lo anterior, al posteriormente iniciar el DVD de instalación personalizado, en el diálogo de **boot:** se ingresa:

```
boot: mi-arranque
```

87.2.3. Añadir equipamiento lógico adicional.

Si se desea añadir equipamiento lógico (*software*) adicional, por ejemplo las más recientes actualizaciones, puede hacerse copiando éste en el directorio **~/centos5-personal/CentOS**, y regenerando el depósito yum local. A fin de respetar los grupos de paquetes y poder disponer de un fichero con las especificaciones de los grupos de paquetes, debe respaldarse primero el fichero **comps.xml** que está dentro de **~/centos5-personal/repodata**.

```
mkdir -p ~/respaldos/
cp ~/centos5-personal/repodata/comps.xml ~/respaldos/
```

Este fichero puede ser modificado con cualquier editor de texto para reflejar los cambios de paquetes nuevos que se quiera incluir a la instalación.

Se añaden los paquetes adicionales o actualizados en **~/centos5-personal/CentOS**:

```
cp /donde/estén/paquetes/*.rpm ~/centos5-personal/CentOS
```

A fin de evitar conflictos con las firmas digitales y evitar tener que modificar el programa de instalación, solo se recomienda utilizar paquetes RPM firmados por CentOS, es decir, los paquetes RPM de las actualizaciones de CentOS.

A fin de poder regenerar el depósito, se utiliza el mandato **createrepo** con la opción **-g** para indicar la ruta del fichero **comps.xml** que se respaldó previamente, y la ruta del directorio de trabajo.

```
createrpo -g ~/respaldos/comps.xml ~/centos5-personal/
```

Lo anterior crea un nuevo directorio **~/centos5-personal/repodata** que incluirá los siguientes ficheros:

- comps.xml
- filelists.xml.gz
- other.xml.gz
- primary.xml.gz
- repomd.xml

Si alguno de los anteriores está ausente, se deben repetir el procedimiento verificando la sintaxis y rutas utilizadas con **createrepo**.

87.2.4. Creación de la imagen ISO.

Una vez terminadas las modificaciones, se crea la imagen ISO:

```
cd ~/centos5-personal/

mkisofs -A "CentOS_5.2_Final_Personal" -o ~/mi-dvd-centos5.iso -b
isolinux/isolinux.bin -c isolinux/boot.cat -no-emul-boot -boot-load-size 4 -boot-
info-table -R -J -v -T ~/centos5-personal
```

La imagen ISO resultante en **~/mi-dvd-centos5.iso** se puede grabar de inmediato desde cualquier herramienta gráfica para este fin, como imagen ISO, y jamás como fichero. Se puede utilizar **K3b**, **XCDroast** o **GNOME Toaster**.

Si solo se dispone de una terminal, la imagen de DVD recién creada se puede grabar con **growisofs**, de la siguiente manera:

```
growisofs -dvd-compat -Z /dev/dvd=mi-dvd-centos5.iso
```

El programa de instalación utilizado en CentOS 5 pudiera fallar debido a las modificaciones hechas, por lo que es importante realizar varias pruebas del nuevo disco de instalación antes de utilizarlo en algún sistema en producción u otros fines que involucren operación crítica.

Es importante recordar que si se va a comercializar o distribuir esta imagen ISO recién creada, se deben respetar los derechos de autor, logotipos y la marca de **CentOS**. Las modificaciones necesarias para el programa de instalación, que consiste en reemplazar las referencias de CentOS y las imágenes de logotipos, se detallarán en un documento que publicaremos posteriormente.

88. Ejercicios

88.1. Ejercicio NFS

88.1.1. Introducción

Haga equipo con algún compañero de curso a fin de poder realizar el procedimiento, pruebas y depuración entre si.

88.1.2. Procedimientos

88.1.2.1. 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
```

88.1.2.2. 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
```

88.2. 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.

88.2.1. 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 especificando *una barra invertida* como secuencia de escape para el espacio posterior. 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 nuevo directorio **/var/samba/contabilidad**:

   ```
   mkdir -p /var/samba/contabilidad
   ```

7. Configure el directorio para que SELinux permita utilizarlo como contenido que será compartido a través de Samba:

```
chcon -t samba_share_t /var/samba/contabilidad
```

8. Genere el grupo de trabajo:

```
groupadd contabilidad
```

9. 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
```

10. 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
```

11. 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/
```

12. Reinicie el servicio de Samba:

```
service smb restart
```

13. 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
```

14. Realice cualquier tipo de transferencia utilizando mget o mput desde el intérprete smb. Al terminar, utilice **exit** para salir.

88.3. 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 «**www**.**mi-dominio.org**» asociado a la dirección IP 192.168.**10**.**n**., donde n corresponde al último octeto de su dirección IP y en este ejercicio será un número entre el 1 y el 254.

- 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.

88.3.1. Procedimientos

1) Modifique el fichero **/etc/hosts** y proceda a resolver de manera local la dirección IP y el nombre que tendrá el servidor en la red 192.168.10.0, añadiendo lo siguiente, donde **n** corresponde al último octeto de su dirección IP:

```
192.168.10.n     www.mi-dominio.org  mail.mi-dominio.org       mi-dominio.org
192.168.10.n     ftp.mi-dominio.org  dns.mi-dominio.org
```

2) Proceda a crear el fichero de configuración del dispositivo virtual en el fichero **/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 ejecutando lo siguiente:

```
mkdir -m 1755 /var/www/mi-dominio
mkdir -m 3775 /var/www/mi-dominio/public_html
mkdir -m 0755 /var/www/mi-dominio/{etc,logs,mail}
```

5) Genera la cuenta de usuario que será utilizada para administrar el sitio de red virtual:

```
useradd -s /sbin/nologin -d /var/www/mi-dominio mi-dominio
usermod -c “Administrador de mi-dominio” mi-dominio
passwd mi-dominio
```

6) Configure los permisos apropiados a **/var/www/mi-dominio** y su contenido, ejecutando lo siguiente:

```
chown root:apache /var/www/mi-dominio
chown mi-dominio:apache /var/www/mi-dominio/public_html
chown mi-dominio:apache /var/www/mi-dominio/etc
chown mi-dominio:mi-dominio /var/www/mi-dominio/mail
chown root:root /var/www/mi-dominio/logs
chcon -t httpd_sys_content_t /var/www/mi-dominio/public_html
```

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/mi-dominio/public_html
              ServerName www.mi-dominio.org
              ServerAlias mi-dominio.org
              ServerAdmin webmaster@mi-dominio.org
              ErrorLog /var/www/mi-dominio/logs/error_log
              CustomLog /var/www/mi-dominio/logs/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
```

88.3.2. Comprobaciones

Reinicie Apache® y pruebe publicar un documento HTML utilizando cualquier herramienta para publicación de red, como puede ser Bluefish, Komposer, Dreamweaver, Frontpage o cualquier editor HTML y publicando a través de FTP, haciendo uso de la cuenta FTP de **mi-dominio**. 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 www.mi-dominio.org</title>
</head>
<body>
<h1>Bienvenido a www.mi-dominio.org</h1>
<p>&iexcl;Hola mundo!</p>
</body>
</html>
```

3. Publique como el usuario **mi-dominio** el documento anterior utilizando el mandato ftp:

```
ftp ftp.mi-dominio.org
Connected to amdk6 (192.168.1.1).
220 Bienvenido al servidor FTP de Alcance Libre.
Name (ftp.mi-dominio.org:fulano):mi-dominio
331 Please specify the password.
Password:
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>cd public_html
ftp>put index.html
ftp>bye
```

4. Finalmente visualice la página **www.mi-dominio.org** principal utilizando elinks.

```
elinks http://www.mi-dominio.org/
```

88.4. 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, dns, mail, y ftp del dominio «que se le especifique».
- Un sitio de red virtual denominado «**www**.**su-nombre.com**» con alias «**su-nombre.com**» asociado a la dirección IP 192.168.**20**.**n**, donde **n** corresponde al último octeto de su dirección IP y en este ejercicio será un número entre el 1 y el 254.
- 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.

88.4.1. Procedimientos

1) Añada el siguiente contenido en el fichero **/etc/hosts** la resolución local del nombre de dominio del sitio de red virtual asociado a la dirección IP definida para el mismo, donde **n** corresponde al último octeto de su dirección IP:

```
192.168.20.n   www.su-nombre.com     mail.su-nombre.com    ftp.su-nombre.com
192.168.20.n   dns.su-nombre.com     su-nombre.com
```

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, añadiendo lo siguiente, donde **n** corresponde al último octeto de su dirección IP:

```
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 **su-nombre.com**.zone, que servirá para resolver la zona de reenvío para el dominio «**su-nombre.com**» con los sub-dominios www, dns, mail, y ftp:

```
$TTL 86400
@     IN     SOA    curso.alcancelibre.org.   usuario.gmail.com. (
                          2009080301 ; número de serie
                          28800 ; tiempo refresco
                          7200 ; tiempo entre reintentos
                          604800 ; expiración
                          86400 ; tiempo total de vida
                          )
@                   IN     NS     curso.alcancelibre.org.
@                   IN     MX     10     mail
@                   IN     TXT    “v=spf1 a mx -all”
@                   IN     A      192.168.20.n
www                 IN     A      192.168.20.n
mail                IN     A      192.168.20.n
dns                 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 “su-nombre.com” {
       type master;
       file “su-nombre.com.zone”;
       allow-update { none; };
};
```

6) Cambie la pertenencia del fichero de zona al usuario «named» y los contextos de SELinux de usuario de sistema (**system_u**), rol de objeto (**object_r**) y tipo zona del servicio **named** (**named_zone_t**), ejecutando lo siguiente:

```
cd/var/named/chroot/var/named/
chown named.named su-nombre.com.zone
chcon -u system_u -r object_r -t named_zone_t su-nombre.com.zone
cd -
```

7) Reinicie el servicio de servidor de nombres ejecutando lo siguiente:

```
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 su-nombre.com 127.0.0.1
dig @127.0.0.1 su-nombre.com
dig @127.0.0.1 su-nombre.com 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 alcancelibre.org
search su-nombre.com
nameserver 127.0.0.1
```

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/su-nombre
mkdir -m 3755 /var/www/su-nombre/public_html
mkdir -m 0755 /var/www/su-nombre/{logs,etc,mail}
chcon -t httpd_sys_content_t /var/www/su-nombre/public_html
```

12) Genere la cuenta de usuario que será utilizada para administrar el sitio de red virtual:

```
useradd -s /sbin/nologin -d /var/www/su-nombre su-nombre
usermod -c “Su Nombre Completo” su-nombre
passwd su-nombre
```

13) Configure los permisos apropiados a **/var/www/su-nombre** y los directorios en su interior utilizando **lo siguientes mandatos**:

```
chown root:apache /var/www/su-nombre
chown su-nombre:apache /var/www/su-nombre/public_html
chown su-nombre:apache /var/www/su-nombre/etc
chown su-nombre:su-nombre /var/www/su-nombre/mail
chown root:root /var/www/su-nombre/logs
```

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/su-nombre/public_html
       ServerName www.su-nombre.com
       ServerAlias su-nombre.com
       ServerAdmin webmaster@su-nombre.com
       ErrorLog /var/www/su-nombre/logs/error_log
       CustomLog /var/www/su-nombre/logs/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 **su-nombre.com** y mail.**su-nombre.com** en el interior del fichero **/etc/mail/local-host-names** con el siguiente contenido:

```
su-nombre.com
mail.su-nombre.com
```

18) Configure el dominio virtual **su-nombre.com** a fin de que Sendmail permita enviar correo para el mismo en el fichero **/etc/mail/relay-domain**s con el siguiente contenido:

```
su-nombre.com
```

19) Genere los nuevos ficheros necesarios para los dominios virtuales en Sendmail, si es que aún existen:

```
touch /etc/mail/{virtusertable,genericstable,generics-domains}
```

20) Si no ha hecho aún, para habilitar la re-escritura de las cuentas de correo, añada en el fichero **/etc/mail/sendmail.mc,** debajo del parámetro **FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable.db')dnl** las siguientes dos líneas de configuración resaltadas en negrita:

```
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) Si el parámetro **MASQUERADE_AS** está definido con otro dominio distinto al que está configurando, añada también en el fichero **/etc/mail/sendmail.mc** la excepción de enmascaramiento (MASQUERADE_EXCEPTION) para su dominio virtual, justo debajo del parámetro MASQUERADE_AS:

```
MASQUERADE_EXCEPTION(`su-nombre.com')dnl
```

22) Genere la cuenta de correo virtual denominada webmaster@**su-nombre.com** como alias de la cuenta local su-nombre, modificando el fichero **/etc/mail/virtusertable** del siguiente modo:

```
webmaster@su-nombre.com         su-nombre
```

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@**su-nombre.com** al correo emitido desde la cuenta local **su-nombre**, modificando el fichero **/etc/mail/genericstable** del siguiente modo:

```
su-nombre        webmaster@su-nombre.com
```

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:

```
   su-nombre.com
```

27)Reinicie el servidor de Sendmail:

```
service sendmail restart
```

28) Ejecutando «**edquota su-nombre**», asigne una cuota de 300 MB (307200 kb) al usuario **su-nombre**:

```
Disk quotas for user su-nombre (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
```

88.4.2. Comprobaciones

Reinicie Apache® y pruebe publicar un documento HTML utilizando cualquier herramienta para publicación de red, como puede ser Bluefish, Komposer, Dreamweaver, Frontpage o cualquier editor HTML y publicando a través de FTP, haciendo uso de la cuenta FTP de **su-nombre** en el URL **ftp://su-nombre@su-nombre.com/public_html/**

Visualice desde el navegador el sitio de red virtual que se configuró.

Pruebe enviar correo a la cuenta virtual **webmaster@su-nombre.com** y leer dicho correo a través de POP3 o IMAP desde la cuenta de **su-nombre**.

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.su-nombre.com</title>
</head>
<body>
<h1>Bienvenido a www.su-nombre.com</h1>
<p>&iexcl;Hola mundo!</p>
</body>
</html>
```

3. Publique como el usuario ***su-nombre*** el documento anterior utilizando ftp:

```
ftp ftp.su-nombre.com
Connected to amdk6 (192.168.1.1).
220 Bienvenido al servidor FTP de Alcance Libre.
Name (ftp.su-nombre.com:fulano):su-nombre
331 Please specify the password.
Password:
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>cd public_html
ftp>put index.html
ftp>bye
```

4. Finalmente, visualice la página **www.su-nombre.com** principal de utilizando el navegador elinks.

```
elinks http://www.su-nombre.com/
```

5. Utilice **mutt** y envíe un mensaje al usuario **webmaster@su-nombre.com**.

```
echo “Mensaje de prueba" | mutt -s “Mensaje de prueba"  webmaster@su-
nombre.com
```

6. Verifique la cuenta de correo de **su-nombre** a través de **cualquier** cliente de correo electrónico o bien el correo con interfaz HTTP.

```
elinks http://www.su-nombre.com/webmail/
```

88.5. Ejercicio: Servidor Intermediario (Proxy)

88.5.1. 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. Configure la política de SELinux para permitir conexiones desde cualquier dirección:

   ```
   setsebool -P squid_connect_any 1
   ```

3. Cambie al directorio /etc/squid

   ```
   cd /etc/squid
   ```

4. Genere el subdirectorio listas:

   ```
   sudo mkdir listas/
   ```

5. 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}
   ```

6. Listar las propiedades del fichero que será utilizado para almacenar las claves de acceso:

   ```
   ls -l listas/claves
   ```

7. Cambiar atributos de lectura y escritura solo para el usuario propietario:

   ```
   sudo chmod 600 listas/claves
   ```

8. Cambiar el propietario del fichero de claves de acceso hacia el usuario **squid**:

   ```
   sudo chown squid.squid listas/claves
   ```

9. Listar **de nuevo** las propiedades del fichero que será utilizado para almacenar las claves de acceso, y observar cambios:

```
ls -l listas/claves
```

10. 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
```

11. Editar el fichero listas/libres:

```
sudo vim listas/libres
```

Poner como único contenido la dirección IP de su máquina.

12. Editar el fichero listas/redlocal:

```
sudo vim listas/redlocal
```

Poner como contenido las direcciones IP del resto de la LAN. Un renglón por IP.

13. 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
babosas
orgasm
petarda
```

14. Editar el fichero listas/extensiones:

```
sudo vim listas/extensiones
```

15. Poner como contenido:

```
\.avi$
\.mp2$
\.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$
```

16. Editar el fichero listas/inocentes:

```
sudo vim listas/inocentes
```

Poner como contenido:

```
.alcancelibre.org
.google.com.mx
.eluniversal.com.mx
.milenio.com.mx
.edu.mx
.gob.mx
```

17. Editar el fichero squid.conf:

```
sudo vim squid.conf
```

18. Desde vim, ejecutar la siguiente búsqueda:

```
/http_port 3128
```

Reemplazar por:

```
http_port 192.168.0.XXX:8080
```

Donde **192.168.0.XXX** corresponde a la dirección IP de su servidor.

19. 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
```

20. 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
```

21. Desde vim, realizar la siguiente búsqueda:

```
/#acl password proxy_auth REQUIRED
```

Descomentar la línea, quitando el símbolo #

22. 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
```

23. 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
```

24. 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
```

25. 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. Si no devuelve errores pero el servicio falla al iniciar, examinar **/var/log/squid/squid.out** y realizar correcciones:

```
sudo tail -f /var/log/squid/squid.out
```

26. Recargar la configuración de Squid a fin de verificar si hubo errores no fatales:

```
sudo service squid reload
```

Si hay errores, realizar correcciones pertinentes.

27. 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.

28. 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**.

89. Ejercicio: Servidor DNS dinámico, servidor DHCP, Servidor Intermediario (Proxy) y Shorewall.

89.1. Introducción.

Este ejercicio está diseñado para ser puesto en práctica en **CentOS 5**, **Elastix 1.5**, **Red Hat Enterprise Linux 5** y **Whitebox Enterprise Linux 5** o sistemas operativos similares, basados sobre **Red Hat Enterprise Linux 5**. Requiere haber estudiado en su totalidad los siguientes documentos:

- Cómo configurar un servidor DHCP en una LAN.
- Cómo configurar un servidor de nombres de dominio (DNS).
- Cómo configurar Squid: Parámetros básicos para servidor de intermediación (Proxy).
- Cómo configurar Squid: Restricción de acceso a Sitios de Red.
- Cómo configurar squid con soporte para direcciones MAC.
- Cómo instalar y configurar la herramienta de reportes Sarg.
- Cómo configurar un muro cortafuegos con Shorewall y tres interfaces de red.

Durante este ejercicio se configurará un servidor DNS dinámico y un servidor DHCP, ambos utilizando la misma firma digital a fin de permitir a los clientes actualizar sus registros en el servidor DNS, un servidor intermediario (Proxy) con **Squid** y un muro cortafuegos con **Shorewall**.

89.1.1. Política: cerrar todo y abrir solo lo necesario.

Durante este ejercicio se crearán solo tres listas de control de acceso para Squid. La lista que será denominada **libres** permitirá acceder libremente y sin restricciones hacia Internet. La lista que será denominada **red-local** solo podrá acceder a los sitios de Internet cuyos dominios estén definidos en la lista denominada **sitios-libres**. Es decir, se aplicará una política estricta que cerrará el acceso a quienes estén definidos en la lista **red-local** permitiendo solo acceder a lista lista de sitios de Internet controlada por el administrador.

El muro cortafuegos se configurará a través de Shorewall y solo permitirá la salida a la red de área local (LAN) para acceder a los servicios de DNS, NTP, FTP-Data, FTP, HTTP, HTTPS, SMTP, SMTP Submission, SMTPS, POP3, IMAP, POP3S e IMAPS.

El ejercicio considera que se dispone de dos interfaces de red en dos diferentes dispositivos, y que **eth0** se utiliza para acceder hacia Internet y **eth1** se utiliza para acceder hacia la red de área local (LAN). Cualquier servicio distinto a DNS, NTP, FTP-Data, FTP, HTTP, HTTPS, SMTP, SMTP Submission, SMTPS, POP3, IMAP, POP3S e IMAPS, estará bloqueado hacia Internet para la red de área local (LAN). Es decir, estarán bloqueados para la red de área local (LAN) los diversos servicios de mensajería instantánea, redes entre iguales (P2P), BitTorrent, Limewire y muchos otros servicios más.

89.2. Equipamiento lógico necesario.

Ingrese al sistema como el usuario **root**.

Proceda a limpiar la configuración de cualquier ejercicio anterior, restaurando el fichero de

configuración predeterminado de Squid y eliminando el directorio de listas, si acaso éste existiese:

```
cp -a /etc/squid/squid.conf.default /etc/squid/squid.conf
rm -fr /etc/squid/listas
```

Proceda a instalar los paquetes **httpd**, **dhcp**, **bind**, **bind-chroot**, **caching-nameserver**, la versión mejorada de Vi (paquete **vim-enhanced**), la herramienta de descargas **wget** y el navegador para modo texto **lynx**:

```
yum -y install httpd dhcp bind bind-chroot caching-nameserver
yum -y install vim-enhanced wget lynx
```

Proceda a configurar el depósito YUM de Alcance Libre que incluye el paquete modificado de squid con soporte para direcciones MAC:

```
cd /etc/yum.repos.d/
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo
cd -
```

Proceda a instalar **sarg**, paquete que consiste en una herramienta de reportes para Squid, squid-arp, paquete modificado por Alcance Libre y que consiste en Squid con soporte para direcciones MAC, así como también el paquete **shorewall**, el cual será utilizado para configurar posteriormente el muro cortafuegos, y el paquete **webmin**, herramienta que se utilizará al terminar todos los procedimientos para administrar el servidor completo desde una interfaz HTTPS.

```
yum -y install sarg squid-arp shorewall webmin
```

89.3. Procedimientos

89.3.1. Modificación de la interfaz de acceso hacia Internet.

1. En caso de utilizar una interfaz con dirección IP estática, ignore este paso y los 3 siguientes.

   Si la interfaz **eth0** obtiene sus parámetros de red a través de DHCP, edite con vim el fichero **/etc/sysconfig/network-scripts/ifcfg-eth0**.

   ```
   vim /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

2. Pulse la tecla **Insert**.

   Modifique el valor del parámetro **PEERDNS** de **yes** a **no** a fin de evitar que se modifique automáticamente el fichero **/etc/resolv.conf** cuando inicie el sistema o se refresque la conexión DHCP. Evite modificar el valor del parámetro **HWADDR**, el valor **XX:XX:XX:XX:XX:XX** corresponde a la dirección MAC **específica** del dispositivo **eth0**.

   ```
   DEVICE=eth0
   HWADDR=XX:XX:XX:XX:XX:XX
   ONBOOT=yes
   BOOTPROTO=dhcp
   ```

```
PEERDNS=no
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

3. Reinicie el servicio **network** a fin de que surtan efecto los cambios.

```
service network restart
```

4. Pulse la tecla **Insert**.

Edite con vim el fichero **/etc/resolv.conf** y asegúrese de que esté definido un servidor DNS válido para poder acceder hacia Internet. El valor **123.123.123.123** debe corresponder a la dirección IP del servidor DNS del proveedor de servicio de acceso hacia Internet o del modem ADSL.

```
search gateway.2wire.net
nameserver 123.123.123.123
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

Configuración de servidor DNS.

1. Se debe crear el directorio **/var/named/chroot/var/named/dynamics** y configurar éste para qué pertenezca al usuario y grupo **named**, tenga permisos de lectura, escritura y ejecución para el usuario y grupo **named** (770) y tenga los contextos de SELinux de usuario de sistema (**system_u**), rol de objeto (**object_r**) y tipo cache del servicio **named** (**named_cache_t**) a fin de permitir escritura en este directorio.

```
cd /var/named/chroot/var/named/
mkdir dynamics/
chmod 770 dynamics/
chown named.named dynamics/
chcon -u system_u -r object_r -t named_cache_t dynamics/
cd -
```

2. Genere con el mandato **touch** el fichero **/var/named/chroot/var/named/dynamics/red-local.net.zone**:

```
touch /var/named/chroot/var/named/dynamics/red-local.net.zone
```

3. Edite con vim el fichero **/var/named/chroot/var/named/dynamics/red-local.net.zone**:

```
vim /var/named/chroot/var/named/dynamics/red-local.net.zone
```

4. Pulse la tecla **Insert**.

Añada el siguiente contenido, donde **proxy.red-local.net** corresponde al nombre de anfitrión del servidor que se está configurando, **red-local.net** corresponde al nombre del dominio de la red de área local con la que se está trabajando y **192.168.123.123**

corresponde a la dirección IP del servidor para la interfaz **eth1**:

```
$TTL 86400
@               IN      SOA     proxy.red-local.net.    root.red-local.net. (
                2009081501 ; número de serie
                28800 ; tiempo refresco
                7200 ; tiempo entre reintentos
                604800 ; tiempo que expira la zona si deja de resolver
                86400 ; tiempo total de vida
                )
@               IN      NS      proxy.red-local.net.
@               IN      A       192.168.123.123
proxy           IN      A       192.168.123.123
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

5. Configure los permisos del fichero **/var/named/chroot/var/named/dynamics/red-local.net.zone** para que éste pertenezca a el usuario y grupo **named** y tenga los contextos de SELinux de usuario de sistema (**system_u**), rol de objeto (**object_r**) y tipo zona del servicio **named** (**named_zone_t**):

```
cd /var/named/chroot/var/named/dynamics/
chown named:named red-local.net.zone
chcon -u system_u -r object_r -t named_zone_t red-local.net.zone
cd -
```

6. Genere con el mandato **touch** el fichero **/var/named/chroot/var/named/dynamics/123.168.192.in-addr.arpa.zone**:

```
touch /var/named/chroot/var/named/dynamics/123.168.192.in-addr.arpa.zone
```

7. Edite con vim el fichero **/var/named/chroot/var/named/dynamics/123.168.192.in-addr.arpa.zone**:

```
vim /var/named/chroot/var/named/dynamics/123.168.192.in-addr.arpa.zone
```

8. Pulse la tecla **Insert**.

   Añada el siguiente contenido, donde **proxy.red-local.net** corresponde al nombre de anfitrión del servidor que se está configurando, **red-local.net** corresponde al nombre del dominio de la red de área local con la que se está trabajando y **123** corresponde al último octeto de la dirección IP del servidor para la interfaz **eth1**:

```
$TTL 86400
@               IN      SOA     proxy.red-local.net.    root.red-local.net. (
                2009081501 ; número de serie
                28800 ; tiempo refresco
                7200 ; tiempo entre reintentos
                604800 ; tiempo que expira la zona si deja de resolver
                86400 ; tiempo total de vida
                )
@               IN      NS      proxy.red-local.net.
123             IN      PTR     proxy.red-local.net.
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

9. Configure los permisos del fichero **/var/named/chroot/var/named/dynamics/123.168.192.in-addr.arpa.zone** para que éste pertenezca a el usuario y grupo **named** y tenga los contextos de SELinux de usuario de sistema (**system_u**), rol de objeto (**object_r**) y tipo zona del servicio **named** (**named_zone_t**):

```
cd /var/named/chroot/var/named/dynamics/
chown named:named 123.168.192.in-addr.arpa.zone
chcon -u system_u -r object_r -t named_zone_t 123.168.192.in-addr.arpa.zone
cd -
```

10. Genere con el mandato **touch** el fichero **/var/named/chroot/etc/named.conf**:

```
touch /var/named/chroot/etc/named.conf
```

11. Edite con vim el fichero **/var/named/chroot/etc/named.conf**:

```
vim /var/named/chroot/etc/named.conf
```

12. Pulse la tecla **Insert**.

Añada o modifique el contenido para que incluya todo lo siguiente, donde 192.168.**123**.0/**24** corresponde a la dirección IP y máscara de subred (en formato de bits) de la red de área local (LAN) con la cual está trabajando, **red-local.net** corresponde al nombre de dominio que se utiliza en la red de área local (LAN) con la cual se está trabajando y **123.168.192.in-addr.arpa** corresponde a la zona de resolución inversa del RFC1918 para la red de área local (LAN) con la cual está trabajando. Modifique la lista de servidores DNS del parámetro **forwarders** para que correspondan a los servidores DNS de su proveedor de acceso hacia Internet.

```
acl "red-local" {
                127.0.0.1/32;
                192.168.123.0/24;
                };
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-recursion { red-local; };
        allow-query  { red-local; };
        forwarders { 200.33.146.193; 200.33.146.193; 200.33.146.217; };
        forward first;
};
include "/etc/named.rfc1912.zones";
include "/etc/rndc.key";
zone "red-local.net" {
        type master;
        file "/var/named/dynamics/red-local.net.zone";
        allow-update { key "rndckey"; };
};
zone "123.168.192.in-addr.arpa" {
```

```
        type master;
        file "/var/named/dynamics/123.168.192.in-addr.arpa.zone";
        allow-update { key "rndckey"; };
};
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

13. Utilizando el mandato **chcon**, configure los contextos de SELinux para el fichero **/var/named/chroot/etc/named.conf**, definiendo éste con rol de objeto (**object_r**), usuario de sistema (**system_u**) y fichero de configuración del servicio **named** (**named_conf_t**):

```
chcon -u system_u -r object_r -t named_conf_t /var/named/chroot/etc/named.conf
```

14. Inicie (o simplemente reinicie, si es necesario) el servicio **named**.

```
service named start
```

15. Si el servicio **named** inicia normalmente, proceda con el siguiente paso. Si hay fallas o errores, regrese en los pasos que sean necesarios y corrija los posibles errores antes de continuar.

16. Si el servicio **named** inició sin errores, utilice el mandato **chkconfig** para que el servicio **named** inicie automáticamente la próxima vez que arranque el sistema.

```
chkconfig named on
```

17. Edite con vim el fichero **/etc/resolv.conf**:

```
vim /etc/resolv.conf
```

18. Pulse la tecla **Insert**.

    Modifique el contenido para defina como único servidor DNS a **127.0.0.1** y defina el dominio predeterminado para la red de área local (LAN) con la que se está trabajando:

```
search red-local.net
nameserver 127.0.0.1
```

    Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

Configuración de servidor DHCP.

1. Edite con vim el fichero **/etc/dhcpd.conf**:

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

2. Pulse la tecla **Insert**.

Añada o modifique el contenido para que incluya todo lo siguiente, donde **proxy.red-local.net** corresponde al nombre de anfitrión del servidor que se está configurando, **192.168.123.0** corresponde a la dirección IP de la red de área local (LAN) con la cual está trabajando, **255.255.255.0** corresponde a la máscara de subred en formato decimal de la red de área local (LAN) con la cual está trabajando, **123.168.192.in-addr.arpa** corresponde a la zona de resolución inversa del RFC1918 para la red de área local (LAN) con la cual está trabajando, **192.168.123.123** corresponde a la dirección IP del servidor que está configurando, **192.168.123.255** corresponde a la dirección IP de difusión (*broadcast*) de la red de área local (LAN) con la cual está trabajando, **red-local.net** corresponde al nombre de dominio que se utiliza en la red de área local (LAN) con la cual se está trabajando y **192.168.123.100** y **192.168.123.199** corresponden al los límites inferior y superior del rango de direcciones IP que se van a asignar de manera dinámica.

```
include "/var/named/chroot/etc/rndc.key";
server-identifier proxy.red-local.net;
ddns-update-style interim;
ddns-domainname "red-local.net.";
ddns-rev-domainname "123.168.192.in-addr.arpa.";
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option domain-name "red-local.net";
option ip-forwarding off;
zone localdomain. {
        primary 127.0.0.1;
        key rndckey;
}
subnet 192.168.123.0 netmask 255.255.255.0 {
        option routers 192.168.123.123;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.123.255;
        option domain-name-servers 192.168.123.123;
        option ntp-servers 200.23.51.205, 132.248.81.29, 148.234.7.30;
        range 192.168.123.100 192.168.123.199;
        zone  123.168.192.in-addr.arpa. {
                primary 192.168.123.123;
                key rndckey;
        }
        zone red-local.net. {
                primary 192.168.123.123;
                key rndckey;
        }
}
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

3. Edite con vim el fichero **/etc/sysconfig/dhcpd**:

```
vim /etc/sysconfig/dhcpd
```

4. Pulse la tecla **Insert**.

Modifique el contenido estableciendo **eth1** como argumentos para el servicio **dhcpd**, con la finalidad de que éste solo funcione a través de la interfaz **eth1**, la cual corresponde a la interfaz por donde accederá la red de área local (LAN).

```
# Command line options here
DHCPDARGS=eth1
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

5. Inicie (o simplemente reinicie, si es necesario) el servicio **dhcpd**.

```
service dhcpd start
```

6. Si el servicio **dhcpd** inicia normalmente, proceda con el siguiente paso. Si hay fallas o errores, regrese en los pasos que sean necesarios y corrija los posibles errores antes de continuar.

7. Si el servicio **dhcpd** inició sin errores, utilice el mandato **chkconfig** para que el servicio **dhcpd** inicie automáticamente la próxima vez que arranque el sistema.

```
chkconfig dhcpd on
```

Configuración de Squid.

1. Configure la política de SELinux para permitir conexiones desde cualquier dirección:

```
setsebool -P squid_connect_any 1
```

2. Cambie al directorio /etc/squid

```
cd /etc/squid
```

3. Genere el subdirectorio **listas**:

```
mkdir listas/
```

4. Genere los ficheros que se utilizarán para las listas de control de acceso y claves de acceso:

```
touch listas/{libres,red-local,sitios-libres}
```

5. Editar el fichero listas/libres:

```
vim listas/libres
```

6. Pulse la tecla **Insert**.

Poner como único contenido la dirección MAC de su máquina (por ejemplo: **00:01:03:DC:67:23**).

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

7. Pulse la tecla **Insert**.

   Editar el fichero listas/red-local y añadir a este todas las direcciones MAC del resto de los equipos de la red de área local (LAN):

   ```
   vim listas/red-local
   ```

   Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

8. Editar el fichero listas/sitios-libres:

   ```
   vim listas/sitios-libres
   ```

9. Pulse la tecla **Insert**.

   Añada como contenido lo siguiente, sustituyendo los dominios en negrita por dominios reales:

   ```
   .red-local.net
   .mis-empresas.com.mx
   .mis-proveedores.com.mx
   .mis-clientes.com
   .mis-bancos.com
   .mis-fabricantes-de-computadoras.com
   .mis-periodicos-favoritos.com
   .mis-antivirus.com
   .google.com.mx
   .docs.google.com
   .maps.google.com
   .alcancelibre.org
   .centos.org
   .fedoraproject.org
   .redhat.com
   .clamav.net
   .mozilla.com
   .adobe.com
   .java.sun.com
   .wikipedia.org
   .edu.mx
   .gob.mx
   .windowsupdate.com
   ```

   Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

10. Editar el fichero squid.conf:

    ```
    vim squid.conf
    ```

11. Desde vim, realice la búsqueda de la cadena **http_port 3128** ejecutando:

    ```
    /http_port 3128
    ```

Reemplazar por:

```
#       If you run Squid on a dual-homed machine with an internal
#       and an external interface we recommend you to specify the
#       internal address:port in http_port. This way Squid will only be
#       visible on the internal address.
#
# Squid normally listens to port 3128
http_port 192.168.123.123:8080 transparent
#  TAG: https_port
#       Usage:  [ip:]port cert=certificate.pem [key=key.pem] [options...]
#
```

Donde **192.168.123.123** corresponde a la dirección IP para la red de área local (LAN) del servidor que se está configurando.

12. Desde vim, realizar la búsqueda de la cadena **10 16 256** ejecutando lo siguiente:

```
/100 16 256
```

Reemplazar:

```
# cache_dir ufs /var/spool/squid 100 16 256
```

Por:

```
cache_dir ufs /var/spool/squid 512 16 256
```

13. Desde vim, realizar la siguiente búsqueda:

```
/acl to_localhost dst 127.0.0.0
```

14. **Debajo** de ésta línea que acaba de buscar y localizar, agregar lo siguiente:

```
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 to_localhost dst 127.0.0.0/8
acl red-local arp "/etc/squid/listas/red-local"
acl libres arp "/etc/squid/listas/libres"
acl sitios-libres dstdomain "/etc/squid/listas/sitios-libres"
acl SSL_ports port 443
acl Safe_ports port 80-90 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
```

15. Desde vim, realizar la siguiente búsqueda:

```
/http_access deny all
```

16. **Arriba** de la línea que acaba de buscar y localizar, agregar lo siguiente:

```
# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks
# And finally deny all other access to this proxy
http_access allow localhost
http_access allow sitios-libres red-local
http_access allow libres
http_access deny all
#  TAG: http_access2
#       Allowing or Denying access based on defined access lists
```

17. Configure el soporte al español para los mensajes de error que mostrará Squid.

    Desde vim, realizar la siguiente búsqueda:

    ```
    /# error_directory
    ```

    Reemplazar lo siguiente:

    ```
    #error_directory /usr/share/squid/errors/English
    #
    #Default:
    # error_directory /usr/share/squid/errors/English
    #  TAG: maximum_single_addr_tries
    #       This sets the maximum number of connection attempts for a
    ```

    Por:

    ```
    #error_directory /usr/share/squid/errors/English
    #
    #Default:
    error_directory /usr/share/squid/errors/Spanish
    #  TAG: maximum_single_addr_tries
    #       This sets the maximum number of connection attempts for a
    ```

    Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

18. Reinicie o, en su defecto, inicie la configuración de Squid a fin de verificar si hubo errores fatales:

    ```
    service squid restart
    ```

    Si hay errores, corregirlos. Si no devuelve errores pero el servicio falla al iniciar, examinar **/var/log/squid/squid.out** y realizar correcciones:

    ```
    tail -f /var/log/squid/squid.out
    ```

19. Recargar la configuración de Squid a fin de verificar si hubo errores no fatales:

    ```
    service squid reload
    ```

Si hay errores, realizar correcciones pertinentes.

20. Añada el servicio **squid** a los servicios de arranque del sistema:

```
chkconfig squid on
```

21. Realizar comprobaciones utilizando navegador en modo texto:

Defina la dirección IP del servidor que acaba de configurar como el valor para la variable de entorno **http_proxy**:

```
export http_proxy="http://192.168.123.123:8080/"
```

Donde **192.168.123.123** corresponde a la dirección IP del servidor que acaba de configurar.

22. Genere un alias para el mandato **lynx** que especifique se se acepten todas las galletas de todos los sitios cuando sea necesario:

```
alias lynx="lynx -cookies -trace"
```

23. 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 cualquier sitio en Internet mientras que la dirección MAC del propio servidor esté incluida en la lista **libres**, es decir el fichero **/etc/squid/listas/libres**.

24. Realice las comprobaciones para las restricciones de acceso que solo permiten acceder hacia los sitios de Internet cuyos dominios están definidos en la lista **sitios-libres**. Tiene una de dos opciones:

    a. Si existe otro servidor con idéntica configuración, defina ahora la dirección IP de éste como el valor de la variable de entorno **http_proxy**:

    ```
    export http_proxy="http://dirección IP otro servidor similar:8080/"
    ```

    b. Si solo existe el servidor que se acaba de configurar, edite de nuevo **squid.conf**:

    ```
    vim squid.conf
    ```

    Realice al siguiente búsqueda:

    ```
    /http_access allow libres
    ```

    Reemplace **http_access allow libres** por lo siguiente, a fin de que la lista **libres** solo pueda acceder a los sitios de Internet cuyo dominio esté en la lista **sitios-libres**, es decir el fichero **/etc/squid/listas/sitios-libres**:

```
http_access allow sitios-libres libres
```

Recargue la configuración de Squid.

```
service squid reload
```

Defina la dirección IP del servidor que acaba de configurar como el valor para la variable de entorno **http_proxy**:

```
export http_proxy="http://192.168.123.123:8080/"
```

Donde **192.168.123.123** corresponde a la dirección IP del servidor que acaba de configurar.

NOTA: Al terminar **las pruebas**, es importante revierta **este último cambio** a fin de restablecer la política de salida libre a quienes estén en la lista **libres**.

25. Utilice el navegador **lynx** realizando una búsqueda a través de Google México para la palabra **sex**:

```
lynx "http://www.google.com.mx/search?q=sexo"
```

Lo anterior deberá permitir realizar la búsqueda pero solo permitiendo el ingreso cualquier sitio de Internet cuyo dominio esté incluido en la lista **sitios-libres**, es decir el fichero **/etc/squid/listas/sitios-libres**.

26. A fin de concluir el ejercicio, elimine los valores de la variable de entorno **http_proxy**:

```
unset http_proxy
```

Configuración de Shorewall.

1. Si todo lo anterior funcionó correctamente, continúe con la configuración de **Shorewall**. En caso contrario, regrese sobre los pasos que sean necesarios hasta hacer las correcciones necesarias.

2. Cambie al directorio **/etc/shorewall**:
```
cd /etc/shorewall
```

3. Edite con vim el fichero **shorewall.conf**:

```
vim shorewall.conf
```

4. Pulse la tecla **Insert**.

Cambie **STARTUP_ENABLED=No** por **STARTUP_ENABLED=yes**:

```
STARTUP_ENABLED=Yes
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

5. Edite con vim el fichero **zones**.

```
vim zones
```

6. Pulse la tecla **Insert**.

Debajo de la zona **fw** y antes de la última línea, la cual deberá respetar y jamás modificar o colocar datos después de ésta, añada las zonas **net** y **loc** definiendo que son del tipo **ipv4**:

```
fw              firewall
net             ipv4
loc             ipv4
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

7. Edite con vim el fichero **interfaces**:

```
vim interfaces
```

8. Pulse la tecla **Insert**.

Defina que la zona **net** corresponderá a la interfaz **eth0**, con auto-detección de dirección de difusión (*broadcast*) y con opciones de **dhcp** y **blacklist** (para el uso del fichero de lista negra). Repita del mismo modo para la zona **loc**, pero definiendo que corresponde a la interfaz **eth1**:

```
net     eth0            detect          dhcp,blacklist
loc     eth1            detect          dhcp,blacklist
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

9. Edite con vim el fichero **masq**:

```
vim masq
```

10. Pulse la tecla **Insert**.

Defina que todo el tráfico proveniente de la interfaz eth1 será enmascarado con la dirección IP de la interfaz eth0:

```
eth0            eth1
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

11. Edite con vim el fichero **blacklist**:

```
vim blacklist
```

12. Pulse la tecla **Insert**.

Defina estará en lista negra la dirección IP **208.81.191.110**, que corresponde a meebo.com, un servicio que ofrece un cliente HTTP para mensajería instantánea para el servicio MSN Messenger, bloqueando solo las conexiones TCP hacia éste a través de el puerto 443:

```
208.81.191.110          tcp     80,443
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

Nota: Puede repetir esta operación para otros sitios de Internet que ofrezcan clientes HTTP para los diversos servicios de mensajería instantánea a través de HTTPS (puerto 443).

13. Edite con vim el fichero **policy**:

```
vim policy
```

14. Pulse la tecla **Insert**.

Defina como políticas predeterminadas que la zona **fw** puede acceder hacia cualquier otra zona, que se descartarán (**DROP**) las conexiones provenientes desde la zona **net** hacia cualquier otra zona guardando en la bitácora del sistema toda la actividad descartada, y que se rechazarán (**REJECT**) conexiones provenientes desde la zona **loc** hacia cualquier otra zona guardando en la bitácora del sistema toda la actividad rechazada.

```
fw              all             ACCEPT
net             all             DROP            info
loc             all             REJECT          info
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

15. Edite con vim el fichero **rules**:

```
vim rules
```

16. Pulse la tecla **Insert**.

Defina que todo el tráfico proveniente de la red de área local (LAN) (zona **loc**) será redirigido al puerto 8080 del servidor que acaba de configurar cuando las conexiones sean

solo por TCP para pueto 80 (**HTTP**).

```
REDIRECT        loc             8080            tcp     80
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

17. Defina que la red de área local (LAN) (zona **loc**) podrá acceder hacia Internet (zona **net**) solo a los servicios de DNS, NTP, FTP-Data, FTP, HTTPS, SMTP, SMTP Submission, SMTPS, POP3, IMAP, POP3S e IMAPS.

```
REDIRECT        loc             8080            tcp     80
ACCEPT          loc             net             tcp     20,21,25,443
ACCEPT          loc             net             tcp     25,465,587
ACCEPT          loc             net             tcp     110,143,993,995
ACCEPT          loc             net             tcp     53,123
ACCEPT          loc             net             udp     53,123
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

18. Defina que la red de área local (LAN) (zona **loc**) podrá acceder hacia el cortafuegos (zona **fw**) para a los servicios de SSH, DNS, HTTP y Webmin (en caso de estar instalado).

```
REDIRECT        loc             8080            tcp     80
ACCEPT          loc             net             tcp     20,21,25,443
ACCEPT          loc             net             tcp     25,465,587
ACCEPT          loc             net             tcp     110,143,993,995
ACCEPT          loc             net             tcp     53,123
ACCEPT          loc             net             udp     53,123
ACCEPT          loc             fw              tcp     22,53,80,10000
ACCEPT          loc             fw              udp     53
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Pulse la tecla **Esc**, guarde cambios y salga de vim pulsando la combinación de teclas **:x** y luego la tecla ⏎ (**ENTER**).

19. Inicie el servicio **shorewall**.

```
service shorewall start
```

20. Si el servicio **shorewall** inicio normalmente, proceda con el siguiente paso. Si hay fallas o errores, regrese en los pasos que sean necesarios y corrija los posibles errores antes de continuar.

21. Si el servicio **shorewall** inició sin errores, utilice el mandato **chkconfig** para que el servicio **shorewall** inicie automáticamente la próxima vez que arranque el sistema.

```
chkconfig shorewall on
```

22. Para realizar pruebas, se necesita configurar un equipo que acceda desde la interfaz **eth1** y que use la dirección IP del servidor que acaba de configurar como **puerta de enlace predeterminada**. Es importante recordar que cualquier servicio distinto a DNS, NTP, FTP-Data, FTP, HTTP, HTTPS, SMTP, SMTP Submission, SMTPS, POP3, IMAP, POP3S e IMAPS, estará bloqueado para la red de área local (LAN).

Instalar y configurar la herramienta de reportes Sarg.

Por favor, siga los procedimientos descritos en el documento titulado Cómo instalar y configurar la herramienta de reportes Sarg.

90. Ejercicio: 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/public_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/public_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/public_html
/var/www/cursolamp/Desktop/public_html
```

8. Configure apache para que utilice el dominio **www.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 www.dominio-red-local
            ServerAlias www
            DocumentRoot /var/www/cursolamp/public_html/
            ServerAdmin cursolamp@mail.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/public_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://**www.dominio-redlocal**/ejemplo-includes.php.

```
   elinks  http://www.dominio-redlocal/ejemplo-includes.php
```

91. Ejercicio: 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 ejecución 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 ejecución 2, 3, 4 y 5. Se deshabilitarán las seis terminales solamente en el nivel de ejecución 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 CentOS (2.6.18-128.2.1.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-128.2.1.el5 ro root=LABEL=/
        initrd /initrd-2.6.18-128.2.1.el5.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:

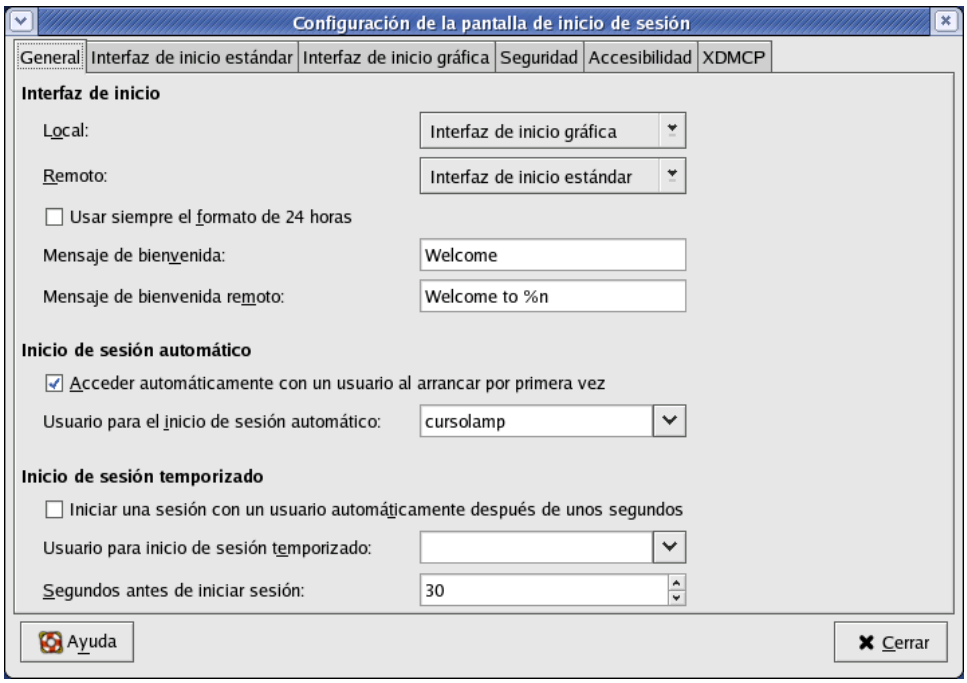
```
title CentOS (2.6.18-128.2.1.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-128.2.1.el5 ro root=LABEL=/ rhgb quiet
        initrd /initrd-2.6.18-128.2.1.el5.img
```

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