# Guía de Administración de Linux en el CIE

Héctor Daniel Cortés González hdcg@cie.unam.mx v1.0a, 19 Octubre 1999

Este documento establece los detalles específicos de la instalación de Linux en el Centro de Investigación en Energía, con el fin de facilitar la administración y el mantenimiento de los sistemas, estebleciendo un ambiente común mínimo indispensable, sin quitarle libertad al usuario para personalizar su ambiente.

## Índice General

# 1 Introducción

Con el incremento en el número de servidores y estaciones de trabajo Linux se hace necesario establecer un conjunto de Guías para facilitar la labor de mantenimiento. Esto es debido a la gran flexibilidad del sistema para adaptarse a múltiples usos y configuraciones: sistemas de rescate totalmente operacionales basados en discos portátiles ZIP de 100 MB, hasta poderosas Estaciones de Trabajo para Cálculo Numérico, pasando por Servidores de Archivos, Servidores de Internet, Computadoras Personales, y en breve Clusters Beowulf.

Esta guía se concentra en las configuraciones para Servidores de Archivos, Servidores de Internet y Computadoras Personales. Esta guía no sustituye a la Guía de Instalación de *Red Hat*, ni otras fuentes de información como *LuCAS* `<http://lucas.linux.org.mx/>` o *LDP* `<http://www.linuxdoc.org/>`.

La última versión de este documento se encuentra en `<http://xalli.cie.unam.mx/Linux/linuxcie.html>`.

## 1.1 Cómo aplicar los cambios en esta guía

Cuando se requiere ejecutar una orden se presentará de la siguiente forma:

```
# ls -CAF
```

En la mayor parte de los casos, se utiliza la orden específica, en otros puede ser necesario realizar algunos cambios menores, como el número de versión de un paquete más reciente a esta guía.

Cuando se hace referencia a una orden Unix, se utiliza también la sección del manual correspondiente, como en `man(1)`.

Cuando se requiere cambiar un archivo de configuración, de ser posible se muestra el archivo de diferencias resultado de la orden `diff -u`. Para cambiar el archivo de configuración se aplican las diferencias con la orden `patch` como sigue:

```
# patch < inittab.diff
```

En la mayoría de los casos, los cambios son simples y pueden ser aplicados con cualquier editor de texto.

## 1.2 Depósito de archivos

Para facilitar el mantenimiento de los sistemas se ha establecido un depósito de archivos en `nfs://xalli.cie.unam.mx/home/ftp/pub/Linux/`

En este depósito se tienen las últimas actualizaciones de *RedHat*, aplicaciones adicionales, como `LyX`, `xemacs` y algunos *plug-ins* para `netscape`, el conjunto de programas seguros `ssh` y `pgp`, y los núcleos del sistema más recientes, en las versiones 2.2 y 2.3.

Para utilizarlos, basta con añadir el sistema de archivos mediante

```
# mount -r xalli:/home/ftp/pub/Linux /mnt
```

# 2 Instalación

## 2.1 Distribución

En el CIE se utilizará la distribución *RedHat* 6.0, en las versiones i386 y alpha.

## 2.2 El Reloj del BIOS

El reloj del BIOS en los equipos Linux tendrá el tiempo universal coordinado (UTC).

## 2.3 Particiones

Se recomienda utilizar el siguiente esquema de particiones:

| Partición | Tamaño | Directorio |
|---|---|---|
| /dev/hda1 | 1024MB | / |
| /dev/hda4 | 128MB | swap |
| /dev/hda5 | 128MB | /tmp |
| /dev/hda6 | 128MB | /var |
| /dev/hda7 | 1024MB | /usr/local |
| /dev/hda8 | Resto del Disco | /home |

Este esquema asegura una administración más simple, evitando que el sistema quede bloqueado por archivos del usuario almacenados en `/tmp`, archivos de registro muy grandes en `/var`, o muchas aplicaciones del usuario en `/usr/local`, dejando el resto del espacio del disco duro para los directorios de trabajo de los usuarios `/home`.

### 2.3.1 Otras particiones

En el caso de equipos con servicios especiales, es recomendable utilizar una partición adicional dedicada a proporcionar dicho servicio. En el caso de `mazatl` se tienen particiones reservadas para el correo entrante `/var/spool/mail` y saliente `/var/spool/mqueue`, en `xalli` se tienen particiones para el servicio de archivos de windows `/home/samba` y el caché de web `/var/spool/squid`.

### 2.3.2 Particiones de Swap

En el caso de los equipos dedicados al cálculo numérico, puede ser necesario utilizar un mayor espacio de swap. No se debe crear una partición mayor a 128 MB. sino que deben crearse tantas particiones de hasta 128

MB como sean necesarias, de ser posible en diferentes dispositivos en diferentes controladores. La memoria virtual proporcionada por las particiones de swap no sustituye a la memoria real, y siempre que sea posible, debe recomendarse la instalación de más memoria física.

## 2.4 runlevels

Se han modificado los niveles de ejecución de *RedHat*: los niveles 0, 1 y 6 se dejan sin cambio, mientras que los niveles 2 al 5 se modifican quedando de la siguiente manera:

- 0: `shutdown`: para apagar el sistema.
- 1: `single user`: para labores de mantenimiento y recuperación
- 2: `multiuser without network`: para estaciones de trabajo personales en modo texto (wired, isn't it?).
- 3: `full multiuser with network`: para servidores en modo texto
- 4: `same as 2 with X11`: para estaciones de trabajo personales en modo gráfico
- 5: `same as 3 with X11`: para servidores en modo gráfico
- 6: `reboot`: para reiniciar el sistema.

De esta forma, en lugar de tener tres niveles diferentes, se tienen dos niveles en dos opciones: multiusuario con/sin red, con/sin X11, para un total de cuatro niveles.

Para permitir este esquema, se requiere cambiar el archivo `/etc/inittab` y los directorios de inicio en `/etc/rc.d`. Para `/etc/inittab` se pueden aplicar los siguientes cambios:

```
--- inittab.orig        Sat Oct 16 12:42:15 1999
+++ inittab     Sat Oct 16 12:43:50 1999
@@ -9,13 +9,13 @@
 # Default runlevel. The runlevels used by RHS are:
 # 0 - halt (Do NOT set initdefault to this)
 # 1 - Single user mode
-# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
-# 3 - Full multiuser mode
-# 4 - unused
-# 5 - X11
+# 2 - Multiuser, without network services
+# 3 - Full multiuser mode with network services
+# 4 - Same as 2, with X11
+# 5 - Same as 3, with X11
 # 6 - reboot (Do NOT set initdefault to this)

-id:3:initdefault:
+id:5:initdefault:

 # System initialization.
 si::sysinit:/etc/rc.d/rc.sysinit
@@ -49,9 +49,9 @@
```

```
 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
+#5:2345:respawn:/sbin/mingetty tty5
+#6:2345:respawn:/sbin/mingetty tty6

 # Run xdm in runlevel 5
 # xdm is now a separate service
-x:5:respawn:/etc/X11/prefdm -nodaemon
+x:45:respawn:/etc/X11/prefdm -nodaemon
```

En `/etc/rc.d` se requiere hacer idénticos `rc4.d` y `rc5.d` a `rc2.d` y `rc3.d` respectivamente mediante las siguientes órdenes:

```
# cd /etc/rc.d
# rm -rf rc[45].d
# ln -s rc2.d rc4.d
# ln -s rc3.d rc5.d
```

Es importante mencionar que con este esquema los cambios realizados a los niveles 2 y 3 se reflejarán automáticamente en los niveles 4 y 5.

# 3 Servicios no necesarios

Los servicios no necesarios deben deshabilitarse o en caso de comprometer la seguridad del sistema, deben borrarse.

## 3.1 rsh

La serie de servicios proporcionadas por `rsh(1)` pueden comprometer la seguridad del sistema, y deben ser sustituidos por `ssh` (v. 4.1 (ssh).

```
# rpm -e rsh
```

## 3.2 kernel-pcmcia-cs

`kernel-pcmcia-cs` permite a Linux utilizar el hardware basado en las tarjetas PCMCIA, de amplia difusión en computadoras portátiles. En las computadoras de escritorio este paquete no es necesario y puede ser removido con:

```
# rpm -e kernel-pcmcia-cs
```

### 3.3 sendmail

`sendmail` sólo debe ser instalado en equipos cuya función primaria sea el correo electrónico, y debe ser borrado para evitar ataques SPAM con la orden:

```
# rpm -e sendmail
```

La eliminación de `sendmail` no impide que el usuario pueda utilizar agentes locales de correo como `pine(1)`, `elm(1)`, `xmh(1)`, `balsa`, o `netscape-communicator`.

## 4 Servicios adicionales

Los paquetes mencionados en esta sección pueden ser encontrados en el depósito de archivos.

### 4.1 ssh

Los servicios `rsh(1)` y `rcp(1)` deben ser sustituidos por `ssh(1)` para evitar comprometer la seguridad del sistema. `telnet(1)` y `ftp(1)` también pueden ser sustituidos por `ssh`.

`ssh` proporciona un medio de comunicación seguro sobre enlaces inseguros mediante el cifrado de datos. Con varios niveles de autentificación, `ssh` es la herramienta ideal tanto para la administración remota de los sitemas, como para su uso cotidiano, así como la transferencia de archivos.

`ssh` consta de varios paquetes que no se incluyen en la distribución típica de *RedHat* por restricciones a la exportación de software criptográfico. Se tiene una versión internacional en el depósito de archivos (v. 1.2 ()).

```
# rpm -ivh ssh-1.2.26-5i.i386.rpm
# rpm -ivh ssh-server-1.2.26-5i.i386.rpm
# rpm -ivh ssh-clients-1.2.26-5i.i386.rpm
# rpm -ivh ssh-extras-1.2.26-5i.i386.rpm
```

Una vez instalado `ssh`, es necesario añadir en `/etc/services` la línea de identificación del servicio:

```
--- services.orig       Sat Oct 16 15:12:59 1999
+++ services    Sat Oct 16 15:13:19 1999
@@ -26,6 +26,7 @@
 ftp-data       20/tcp
 ftp            21/tcp
+ssh            22/tcp
 telnet         23/tcp
 smtp           25/tcp          mail
```

Para conservar la compatibilidad con aplicaciones que utilizan `rsh` es necesario dirigir las peticiones `rsh` y `rcp` hacia `ssh` y `scp` respectivamente:

```
# cd /usr/bin
# ln -s ssh1 rsh
# ln -s scp1 rcp
```

Por último, es necesario asegurarnos que el servicio se ejectue en los niveles 2 y 3:

```
# chkconfig --level 23 sshd on
```

## 4.2 xntp

Todos los sistemas Unix en el CIE tienen sus relojes sincronizados. El servidor maestro del tiempo es `xalli`. Los sistemas no-Linux utilizan `timed(8)` en modo esclavo. Los servidores Linux utilizan `xntpd(8)`.

A diferencia de `timed`, donde el tiempo es un promedio acordado entre todos los eqiupos en la red local, `xntpd` toma el tiempo a partir de servidores maestros conectados a fuentes confiables, como relojes atómicos, o dispositivos gps. De modo que no solamente todos los equipos tienen la misma hora, sino que además, es la hora exácta.

Para instalar `xntpd` se deben seguir los siguientes pasos:

1. Se instala el paquete con la orden:

   ```
   # rpm -ivh xntp3-5.93-12.i386.rpm
   ```

2. Se cambia el archivo de configuración `/etc/ntp.conf` por:

   ```
   multicastclient
   driftfile /etc/ntp/drift
   ```

3. Se sincronizan los relojes con:

   ```
   # ntpdate xalli
   # clock -w -u
   ```

4. Se echa a andar el cliente, que conservará sincronizado el reloj del sistema:

   ```
   # /etc/rc.d/init.d/xntpd start
   ```

5. Por último, se configura el servicio para que encienda automáticamente:

   ```
   # chkconfig --level 23 xntpd on
   ```

`xntpd` conserva en sincronía el reloj del sistema, el cual es diferente al RTC *(Real Time Clock)* o reloj del BIOS. Por lo general, el *RTC* es extremadamente inexacto. Como los sistemas Linux pueden permanecer funcionando por largos períodos, es necesario conservar en sincronía el *RTC* para el caso en que sea necesario reiniciar el sistema. La forma más simple es usar `cron(8)`.

*RedHat* tiene un esquema de administración de tareas períodicas muy bien diseñado. Se pueden establecer tareas en períodos de una hora, un día, una semana y un mes, sin tener que modificar la configuración de `cron`.

Para conservar el *RTC* en sincronía, añadimos el archivo `clock.cron` en `/etc/cron.daily` mediante las siguientes órdenes:

```
# cd /etc/cron.daily
# echo "clock -w -u" > clock.cron
# chmod u+x clock.cron
```

# 5 Modificación de servicios

Una de las virtudes de Linux es su gran flexibilidad para su configuración. De allí que se requieran hacer al menos los siguientes cambios para tener un ambiente uniforme en el CIE.

## 5.1 issue

El mensaje de identificación de *RedHat* proporciona el nombre de la distribución instalada, información que puede ser utilizada para atacar al sistema. Dicho mensaje se almacena en los archivos `/etc/issue` y `/etc/issue.net` al momento de iniciar el sistema mediante el programa `/etc/rc.d/rc.local`.

Debe modificarse `/etc/rc.d/rc.local` para que quede como sigue:

```
#!/bin/bash

# This will overwrite /etc/issue at every boot.  So, make any changes you
# want to make to /etc/issue here or you will lose them when you reboot.
cat > /etc/issue << -EOF-

Centro de Investigación en Energía
Welcome to $(uname -srm)
-EOF-

cp -f /etc/issue /etc/issue.net
echo >> /etc/issue

# Aquí se pueden añadir otros servicios locales
```

## 5.2 inetd

`inetd(8)` es el programa que escucha las peticiones de conexión de equipos remotos. Los equipos configurados como estaciones de trabajo personales no deberían proporcionar servicios de red. De ser posible debe ser deshabilitado mediante

```
# chkconfig --level 23 inetd off
```

Cuando no es posible tomar esta medida radical, es necesario reducir el número de servicios proporcionados por `inetd` al mínimo y configurar `tcpd` (v. 5.3 (tcpd)).

## 5.3 tcpd

`tpcd(8)` proporciona un mecanismo de seguridad elemental para los servicios proporcionados por `inetd(8)`. Se requiere configurar dos archivos: `/etc/hosts.allow` y `/etc/hosts.deny`.

Existen varias estrategias de configuración para `tpcd`, que pueden consultarse en `hosts_access(5)`. En el CIE utilizamos una estrategia simple: se confía plenamente en los equipos de la red local y en `ssh`, y no confiamos en ningún equipo externo. `mazatl` tiene una estrategia mucho más abierta, y mucho más susceptible a ataques del exterior, pero es más fácil cuidar a una sóla maquina, que estar cuidando a todas al mismo tiempo.

*RedHat* instala archivos de control `/etc/hosts.{allow,deny}` sin reglas de acceso. Se tienen que añadir las siguientes reglas a los archivos correspondientes:

```
--- hosts.deny.orig     Sat Oct 16 16:14:48 1999
+++ hosts.deny  Sat Oct 16 16:15:05 1999
@@ -7,3 +7,4 @@
 # the new secure portmap uses hosts.deny and hosts.allow.  In particular
 # you should know that NFS uses portmap!

+ALL: ALL
--- hosts.allow.orig    Sat Oct 16 16:16:42 1999
+++ hosts.allow Sat Oct 16 16:16:57 1999
@@ -4,3 +4,5 @@
 #              by the '/usr/sbin/tcpd' server.
 #

+ALL: 127. 132.248.30.
+sshd: ALL
```

## 5.4 samba

`samba(7)` permite a los equipos Unix, incluyendo Linux, proporcionar servicios de red para windows. No es una tarea sencilla, y requiere de varios programas de apoyo y el archivos de configuración `/etc/smb.conf` es complejo. Se puede aprender más de las opciones mencionadas en `smb.conf(5)`

```
--- /etc/smb.conf.orig  Thu Jul 22 10:40:06 1999
+++ /etc/smb.conf       Mon Oct 18 13:28:54 1999
@@ -15,22 +15,22 @@
 [global]

 # workgroup = NT-Domain-Name or Workgroup-Name
-   workgroup = MYGROUP
+   workgroup = CC

 # server string is the equivalent of the NT Description field
-   server string = Samba Server
+   server string = I. M. Boring, PhD

 # This option is important for security. It allows you to restrict
 # connections to machines which are on your local network. The
 # following example restricts access to two C class networks and
 # the "loopback" interface. For more examples of the syntax see
 # the smb.conf man page
-;   hosts allow = 192.168.1. 192.168.2. 127.
+   hosts allow = 127. 148.218.30.

 # if you want to automatically load your printer list rather
 # than setting them up individually then you'll need this
    printcap name = /etc/printcap
-   load printers = yes
+   load printers = no
```

```
 # It should not be necessary to spell out the print system type unless
 # yours is non-standard. Currently supported print systems include:
@@ -43,10 +43,10 @@

 # this tells Samba to use a separate log file for each machine
 # that connects
-   log file = /var/log/samba/log.%m
+   log file = /var/log/samba/%m

 # Put a capping on the size of the log files (in Kb).
-   max log size = 50
+   max log size = 16

 # Security mode. Most people will want user level security. See
 # security_level.txt for details.
@@ -87,6 +87,11 @@
 # See speed.txt and the manual pages for details
    socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

+# More optimization options
+   keep alive = 60
+   dead time = 5
+   debug level = 1
+
 # Configure Samba to use multiple interfaces
 # If you have multiple network interfaces then you must list them
 # here. See the man page for details.
@@ -102,7 +107,7 @@
 # Browser Control Options:
 # set local master to no if you don't want Samba to become a master
 # browser on your network. Otherwise the normal election rules apply
-;   local master = no
+   local master = no

 # OS Level determines the precedence of this server in master browser
 # elections. The default value should be reasonable
@@ -156,7 +161,7 @@

 # WINS Server - Tells the NMBD components of Samba to be a WINS Client
 #      Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
-;   wins server = w.x.y.z
+   wins server = 132.248.30.3

 # WINS Proxy - Tells Samba to answer name resolution queries on
 # behalf of a non WINS capable client, for this to work there must be
```

### 5.4.1 Servidores de Archivos

Algunos equipos Linux en el CIE están configurados para proporcionar servicios de archivos para la red de Windows. Estos equipos también están configurados como servidores maestros para los nombres de windows:

```
Grupo   Servidor
-----   --------
CC      MAZATL
MES     COAMITL
FT      TOCATL
TEYM    NELLI
SE      HUIPILLI
```

En estos equipos, se requiere la siguiente configuración adicional:

```
--- smb.conf.orig       Mon Oct 18 13:32:07 1999
+++ smb.conf    Mon Oct 18 13:33:15 1999
@@ -107,20 +107,20 @@
 # Browser Control Options:
 # set local master to no if you don't want Samba to become a master
 # browser on your network. Otherwise the normal election rules apply
-   local master = no
+   local master = yes

 # OS Level determines the precedence of this server in master browser
 # elections. The default value should be reasonable
-;   os level = 33
+   os level = 33

 # Domain Master specifies Samba to be the Domain Master Browser. This
 # allows Samba to collate browse lists between subnets. Don't use this
 # if you already have a Windows NT domain controller doing this job
-;   domain master = yes
+   domain master = yes

 # Preferred Master causes Samba to force a local browser election on startup
 # and gives it a slightly higher chance of winning the election
-;   preferred master = yes
+   preferred master = yes

 # Use only if you have an NT server on your network that has been
 # configured at install time to be a primary domain controller.
```

Para añadir más directorios compartidos consulte `smb.conf(5)`.

## 5.5 logrotate

*RedHat* establece un mecanismo de rotación de las bitácoras del sistema mediante `logrotate(8)`. Se puede configurar para que las bitácoras antiguas se almacenen comprimidas para ahorrar espacio en disco. Esto es especialmente útil en equipos que requieren poca atención del administrador.

```
--- logrotate.conf.orig Mon Oct 18 16:51:07 1999
+++ logrotate.conf      Mon Oct 18 16:51:37 1999
@@ -12,7 +12,7 @@
 create
```

```
 # uncomment this if you want your log files compressed
-#compress
+compress

 # RPM packages drop log rotation information into this directory
 include /etc/logrotate.d
```

### 5.6 fstab

Los equipos Linux asignados como estaciones de trabajo personales tienen ciertas características que hacen deseable la modificación del archivo `/etc/fstab`. Estas modificaciones **no deben** aplicarse en otras configuraciones.

En los equipos multiusuario, sólo `root` puede poner y quitar sistemas de archivos mediente las órdenes `mount(8)` y `umount(8)`. Pero en las estaciones de trabajo personales esta restricción no es aplicable, pues `root` también es el usuario primario del sistema. Por lo tanto, es posible añadir la opción `user` en `/etc/fstab` para permitirle al usuario poner y quitar sistemas de archivos como diskettes, zips y discos compactos.

```
--- fstab.orig  Sat Oct 16 16:30:33 1999
+++ fstab       Sat Oct 16 16:30:52 1999
@@ -4,8 +4,8 @@
 /dev/hda7              /usr/local              ext2    defaults        1 2
 /dev/hda8              /home                   ext2    defaults        1 2
 /dev/hda4              swap                    swap    defaults        0 0
-/dev/fd0               /mnt/floppy             ext2    noauto          0 0
-/dev/cdrom             /mnt/cdrom              iso9660 noauto,ro       0 0
-/dev/hdd4              /mnt/zip                ext2    noauto          0 0
+/dev/fd0               /mnt/floppy             ext2    noauto,user     0 0
+/dev/cdrom             /mnt/cdrom              iso9660 noauto,ro,user  0 0
+/dev/hdd4              /mnt/zip                ext2    noauto,user     0 0
 none                   /proc                   proc    defaults        0 0
 none                   /dev/pts                devpts  gid=5,mode=620  0 0
```

Si se añade al panel de gnome el applet "drive mount"es facilita la tarea de poner y quitar estos medios removibles.

## 6 Mantenimiento

El mantenimiento de un sistema Linux puede ser desde una tarea trivial en equipos con poca actividad, hasta extremadamente compleja en equipos con múltiples configuraciones y servicios. Afortunadamente en el CIE no se tienen equipos con dicho grado de complejidad. La mayor parte del tiempo, estas tareas se reducen al monitoreo del espacio en disco, la revisión de las bitácoras del sistema y la actualización de los paquetes, especialmente aquellas relacionadas con la corrección de problemas de seguridad.

### 6.1 mkupdates

Para facilitar la actualización del sistema, se ha escrito el guión de shell `mkupdates` que revisa el depósito de archivos y aplica las actualizaciones encontradas. Este programa es suceptible a mejorarse, especialmente en lo referente a las dependencias entre paquetes, la actualización del kernel y el paquete `rpm`. El resultado del guión puede ser revisado en los archivos `mkupdates.out` y `mkupdates.err`, correspondientes a `stdout` y `stderr`.

```
#!/bin/bash

BASEDIR=/mnt/updates/6.0/i386/

exec |tee -i $0.out
exec 2>$0.err

for f in $(ls -1 $BASEDIR)
do
p=$(echo $f | sed -e 's/\.i386\.rpm//')
q=$(echo $p | sed -e 's/-[^-]*-[^-]*$//')
r=$(rpm -q $q) || continue
case $q in
  kernel*)
        echo "New kernel version!!"
        continue
  ;;
  rpm*)
        echo "New RPM version!!"
        continue
  ;;
esac
test "$p" = "$r" || rpm -Uvh $BASEDIR/$f
done
```

Por el momento, las actualizaciones del kernel y el paquete `rpm` deben realizarse manualmente.

## 6.2 Nuevas versiones de RedHat

Cuando se encuentre disponible una nueva versión de *RedHat*, primero debe ser probada por el Equipo de Trabajo de la Unidad de Cómputo, con el fin de familiarizarse con las nuevas características del sistema, especialmente aquellas consideradas como experimentales o de prueba, antes de ser instalada en forma masiva en el resto de los servidores.