TEST COMPLETO DE ADMINISTRACIÓN DE LINUX

La base de este taller será el archivo comprimido LINUXCognos.rar, el mismo que será descomprimido en tres oportunidades. Así tendremos operables tres servidores, un {SC} Servidor de Correos (eth0 Bridged), un {SW} Servidor de Páginas Web (eth0 Bridged) y un {SP} Servidor Proxy Squid (eth0 Bridged, eth1 Nat [192.168.190.100]).

Asimismo, debe realizar la instalación de una {WS} Estación de Trabajo Gnome (eth0 Nat [192.168.190.101] y Gateway el Servidor Proxy Squid), debe ser una estación de trabajo y NO un servidor, la forma de verificar que ha instalado una estación de trabajo será que el resultado al ejecutar los siguientes comandos será vacío:

```
# rpm –qa | grep httpd
# rpm –qa | grep sendmail
# rpm –qa | grep mysql
# rpm –qa | grep squid
```

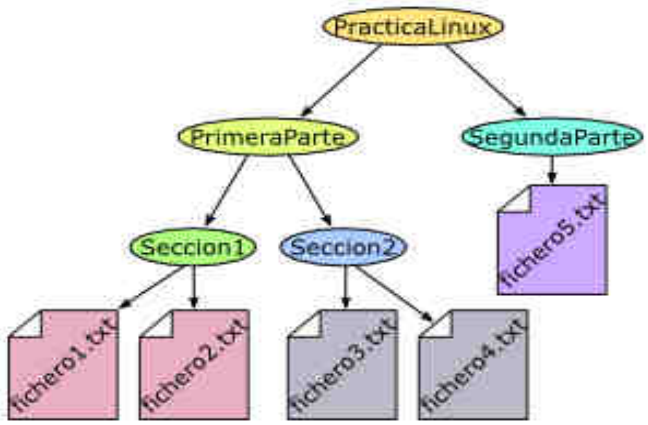
1) Crear los siguientes grupos:

- En el servidor SC crear los grupos: gruposc1, gruposc2 y gruposc3.
- En el servidor SW crear los grupos: gruposw1, gruposw2 y gruposw3.
- En el servidor SP crear los grupos: gruposp1, gruposp2 y gruposp3.

2) Crear los siguientes usuarios en los grupos indicados:

- cregistro1, cregistro2 en el gruposc1.
- cregistro3, cregistro4 en el gruposc2.
- cregistro5, cregistro6 en el gruposc2.
- wregistro1, wregistro2 en el gruposw1.
- wregistro3, wregistro4 en el gruposw2.
- wregistro5, wregistro6 en el gruposw2.
- pregistro1, pregistro2 en el gruposp1
- pregistro3 en el gruposp2
- pregistro4 en el gruposp3

2) Crear la siguiente estructura de directorios y archivos necesarios en los HOME DIRECTORY de los usuarios: cregistro1, wregistro1 y pregistro1.



3) Los archivos fichero*.txt del servidor SC deben poder leerse y ejecutarse por cualquier usuario pero no modificarse. La asignación de permisos se realizará desde el directorio /home/cregistro1.

4) Los archivos fichero*.txt del servidor SW deben poder leerse y ejecutarse solamente por el dueño y por los usuarios del grupo pero nada para el resto de los usuarios. La asignación de permisos se realizará desde el directorio /tmp.

5) Los archivos fichero*.txt del servidor SP deben poder leerse, modificarse y ejecutarse solamente por el usuario dueño y nada para los usuarios del grupo ni el resto de usuarios. La asignación de permisos se realizará desde el directorio /home/pregistro1/PracticaLinux/SegundaParte/.

6) En el equipo SC, como usuario “root” recuperar el archivo:
http://www.clasespersonales.com/solodatos.rar
y copiarlo en el directorio /tmp

7) En el equipo SW, como usuario “root” recuperar el archivo:
http://www.clasespersonales.com/deptos.sql
y copiarlo en el directorio /root

8) En el equipo SP, empaquetar los archivos /etc/passwd, /etc/shadow y /etc/group; con el nombre "micopia" y copiarlo en el directorio /tmp

9) En el equipo SP implementar un proceso de empaquetado (tar), compresión(bzip2), y copia de los archivos /etc/passwd, /etc/shadow y /etc/group; para que se ejecute 3 veces al día, a horas 9:00, 13:00 y 19:00. Cada copia debe tener un identificador de la hora y la fecha, para que no se solapen las copias de un mismo día y de otros días.

10) En el servidor SP, crear un script "paquete" para empaquetar y comprimir un archivo existente y sin importar de donde este el archivo, lleve el resultado siempre al directorio /tmp/resbkp, asimismo deberás tener cuidado con los permisos, pues el comando "paquete" lo puede ejecutar el super usuario o cualquier usuario. Además, el script debe validar que el archivo a comprimir y empaquetar exista. Si llaman al script especificando el nombre de archivo, entonces valida, empaqueta y comprime; pero si llaman al script sin parámetro, entonces, pedir al usuario que introduzca un nombre de archivo, para luego validar, empaquetar y comprimir.

Ejemplo 1:

paquete <ENTER>
Archivo: miarchivo <ENTER>
El archivo miarchivo.tar.gz fue copiado al directorio /tmp/resbkp

Ejemplo 2:

paquete <ENTER>
Archivo: miarchivo <ENTER>
El archivo especificado NO existe

Ejemplo 3:

$ paquete miarchivo <ENTER>
El archivo miarchivo.tar.gz fue copiado al directorio /tmp/resbkp

11) Instalar el servidor de Correos con el nombre de máquina de acuerdo a la tabla que se especifica al final de este ejercicio. Luego enviar un correo desde "root" a "cregistro1", de "cregistro1" a "cregistro2", de "cregistro3" al correo electrónico reynaldozeballos@gmail.com y de "cregistro4" al correo electrónico reynaldozeballos@hotmail.com

Usuario	Servidor Correos
Yola	cognos1.com
Darling	cognos2.com
Abel	cognos3.com
Fernando	cognos4.com
Eddy	cognos5.com
Willy	cognos6.com
Abraham	cognos7.com
Galo	cognos8.com
René	cognos9.com

12) Instalar el servidor Web, con el nombre de servidor de acuerdo a la tabla del anterior ejercicio, pero aumentando por delante el texto "web", así por ejemplo, Yolita instalará el servidor WEB con el nombre "webcognos1.com".

13) Bajar los siguiente archivos desde el servidor clasespersonales.com:

```
wget http://www.clasespersonales.com/menulnx.htm
wget http://www.clasespersonales.com/centosm.JPG
wget http://www.clasespersonales.com/centosc.JPG
wget http://www.clasespersonales.com/centosp.JPG
wget http://www.clasespersonales.com/correoslnx.htm
wget http://www.clasespersonales.com/proxylnx.htm
wget http://www.clasespersonales.com/apachelnx.htm
wget http://www.clasespersonales.com/sendmail.css
wget http://www.clasespersonales.com/lnxhdd.htm
wget http://www.clasespersonales.com/lnxmysql.htm
wget http://www.clasespersonales.com/lnxsquid.htm
```

14) Realizar los pasos necesarios para que el usuario "wregistro1", implemente su propio sitio web con el mismo conjunto de archivos

indicados en el ejercicio del punto 13. Para diferenciar ambos, agregue su nombre completo en la página "index.htm" que será una copia del menulnx.htm, su nombre debe sobresalir en la página, por la cual deberás utilizar las etiquetas <H1> y </H1>

15) Realizar las configuraciones necesarias para que los usuarios del SW, del SC y del SP, puedan ingresar al SW, especificando en la dirección del explorador el texto:

http://intranet y http://intranet/~wregistro1

16) Con la información de la siguiente tabla:

USUARIO	CBBA 190.186.18.162	SC 190.186.90.204	LP 190.129.67.38
Yola	cognos1	cognos	desarrollo
Darling	cognos2	cognos	desarrollo
Abel	cognos3	cognos	desarrollo
Fernando	cognos4	cognos	desarrollo
Eddy	cognos5	cognos	desarrollo
Willy	cognos6	cognos	desarrollo
Abraham	cognos7	cognos	desarrollo
Galo	cognos8	cognos	desarrollo
René	cognos9	cognos	desarrollo

Ingresar en cada servidor y crear un archivo con su nombre y apellido y hora de proceso, que contenga un refrán. P.Ej. Nombre de archivo: rzeballos1033, Contenido: "A caballo regalado no se le miran los dientes"

17) El usuario pregistro1 deberá copiarse el archivo "quemensaje" del servidor de Cochabamba, este archivo se encuentra en el directorio /tmp

18) El usuario pregistro3 deberá copiarse el archivo "mensaje" del servidor de Santa Cruz, el archivo está en el directorio /tmp

19) El usuario pregistro4 deberá copiarse el archivo "otromensaje" del servidor de La Paz, el archivo está en el directorio /tmp

20) Instalar el servidor Proxy SQUID en el puerto 7272, permitiendo a toda su red para que ingresen a internet y restringiendo los siguientes sitios web: www.facebook.com, www.fulltono.com, www.taringa.com, www.mocosoft.com

21) Configurar la estación GNOME para que ingrese a internet a través del servidor SQUID instalado.

22) Reiniciar el servidor proxy squid y la estación Gnome, y verificar que las configuraciones realizadas sigan vigentes, es decir, la estación Gnome tiene internet a través del Servidor Proxy Squid, y que los sitios web indicados en el punto 20, no pueden ser accesados por la estación.

23) Agregar un disco duro de 1GB al servidor Web, este nuevo disco duro deberá colgarse en el directorio /u y deberá montarse automáticamente cada vez que el servidor WEB se reinicie.

24) Toda vez que nos conectamos a un servidor utilizando el Secure Shell, se generá un fingerprint único, realice una tabla donde coloque los nombres de servidores instalados, incluyendo los servidores de Cochabamba, Santa Cruz y La Paz, y especifique los fingerprint generados para cada servidor. El código de cada servidor se llama fingerprint y se genera dentro del directorio ".ssh" en el archivo denominado know_hosts, por lo cual deberá consultar estos archivos para tener los fingerprints de cada servidor.

25) En el servidor proxy squid, como usuario "root" concatenar los archivos /etc/passwd, /etc/shadow y /etc/group con el nombre archivosesenciales y almacenarlo en el directorio /tmp

26) Tenga cuidado de registrar todos los comandos utilizados para lograr concluir esta práctica. Transcriba los comandos, sus observaciones y algunas notas con el nombre "ejercicio" y envíelo por correo electrónico con el usuario "root" a las cuentas de correo electrónicos: reynaldozeballos@hotmail.com y a reynaldozeballos@gmail.com