16.2 Ejercicio de laboratorio: Revisión integral

En este ejercicio de laboratorio, practicará y demostrará sus conocimientos y habilidades.

Resultados:
Complete las siguientes tareas y califique satisfactoriamente el sistema serverX con **lab sa1-review grade** como usuario root en serverX.

Reinicie la máquina de serverX.

Ejecute el **lab sa1-review setup** como usuario root en serverX.

1. Use comandos Bash para completar las siguientes tareas en la máquina serverX:

    - Muestre las 12 primeras líneas del archivo `/usr/bin/clean-binary-files` y envíe el resultado al archivo `/home/student/headtail.txt`.

    - Muestre las últimas nueve líneas del archivo `/usr/bin/clean-binary-files` y agregue el resultado al archivo `/home/student/headtail.txt`.

    a. Muestre las 12 primeras líneas del archivo `/usr/bin/clean-binary-files` y envíe el resultado del comando al archivo `/home/student/headtail.txt`.

    ```
    [student@serverX ~]$ head -n 12 /usr/bin/clean-binary-files >/home/student/headtail.txt
    ```

b. Muestre las últimas nueve líneas del archivo `/usr/bin/clean-binary-files` y agregue el resultado del comando al archivo `/home/student/headtail.txt`.

```
[student@serverX ~]$ tail -n 9 /usr/bin/clean-binary-files >>/home/student/headtail.txt
```

2. Existen 10 sistemas Linux nuevos que requieren de archivos de documentos de cambios. Complete las siguientes tareas en serverX para crearlos:

- Cree archivos vacíos con el nombre de archivo `system_changes-machine`*`Y`*`-month_`*`Z`*`.txt` en el directorio `/home/student` en la máquina de serverX como usuario student. Reemplace *Y*con el número de máquina y reemplace *Z* con los meses *jan*, *feb* y *mar*.
- Cree el directorio `/home/student/syschanges` con los subdirectorios `jan`, `feb` y `mar`.
- Clasifique todos los archivos recién creados por mes en el subdirectorio correspondiente.
- Elimine todos los archivos creados recientemente relacionados con las máquinas 9 y 10 porque el hardware fue reemplazado en forma permanente.

a. Cree un total de 30 archivos con nombres tales como `system_changes-machine`*`Y`*`-month_`*`Z`*`.txt` . Reemplace *Y* con el número de máquina y reemplace *Z* con los meses *jan*, *feb* y *mar*.

```
[student@serverX ~]$ touch ~student/system_changes-machine{1..10}-month_{jan,feb,mar}.txt
```

b. Cree el directorio `/home/student/syschanges` con los subdirectorios `jan`, `feb` y `mar`.

```
[student@serverX ~]$ mkdir -p /home/student/syschanges/{jan,feb,mar}
```

c. Clasifique todos los archivos recién creados por mes en el subdirectorio correspondiente.

```
[student@serverX ~]$ mv ~student/system_changes-machine*jan.txt /home/student/syschanges/jan/
[student@serverX ~]$ mv ~student/system_changes-machine*feb.txt /home/student/syschanges/feb/
[student@serverX ~]$ mv ~student/system_changes-machine*mar.txt /home/student/syschanges/mar/
```

d. Elimine todos los archivos creados recientemente relacionados con las máquinas 9 y 10.

```
[student@serverX ~]$ rm -f /home/student/syschanges/*/system_changes-machine{9,10}*.txt
```

3. Use las páginas de manual para investigar cómo desactivar el uso de colores en el resultado. Incluya la opción relevante del comando **ls** en el archivo de texto `/home/student/lscolor.txt`en serverX.

a. Busque la opción relevante en la página de manual **ls**(1) para determinar cómo evitar que ls proporcione un resultado colorido. ¿Cuál es la opción correcta?

```
[student@serverX ~]$ man ls
```

ls utiliza **--color=never** para desactivar los colores en el resultado del comando.

b. Cree el archivo de texto `/home/student/lscolor.txt` con la opción **ls** para desactivar el resultado colorido.

```
[student@serverX ~]$ echo "--color=never" >/home/student/lscolor.txt
```

4. Copie el archivo `/home/student/vimfile.txt` para `/home/student/longlisting.txt` en serverX. Use el editor **vim** para cambiar el archivo `/home/student/longlisting.txt` según los siguientes requisitos:

- Elimine la columna de propietario de archivo. No elimine ningún espacio.
- Elimine las filas `Documentos` e `Imágenes`.
- Guarde el archivo cuando haya finalizado la edición.

a. Copie el archivo `/home/student/vimfile.txt` en `/home/student/longlisting.txt`.

```
[student@serverX ~]$ cp /home/student/vimfile.txt /home/student/longlisting.txt
```

b. Edite el archivo con Vim para aprovechar el *modo visual*.

```
[student@serverX ~]$ vim /home/student/longlisting.txt
```

c. Elimine la columna *propietario* del archivo.

Use las teclas de flecha para ubicar el cursor en el primer carácter de la columna de propietario del grupo. Ingrese el modo visual con **Ctrl**+**v**. Use las teclas de flecha para ubicar el cursor en el último carácter de la columna de propietario del grupo. Elimine la selección con **x**.

d. Elimine las filas `Documentos` e `Imágenes`. Esta vez, ingrese el modo visual con una **V** mayúscula, que selecciona automáticamente las líneas completas.

Use las teclas de flecha para ubicar el cursor en cualquier carácter de la fila `Documentos`. Ingrese el modo visual con una **V** mayúscula. Se selecciona la línea completa, como se muestra en la captura de pantalla. Elimine la selección con **x**. Repita estos pasos para la fila `Imágenes`.

e. Guarde el archivo y salga del editor.

Presione la tecla "esc" e ingrese ":wq" para escribir el archivo y salir de **vim**.

5. Cambie la configuración y agregue usuarios nuevos y un grupo nuevo, según los siguientes requisitos:

- Cambie los parámetros de configuración del sistema predeterminados para los usuarios creados recientemente a fin de garantizar que sus contraseñas se cambien por lo menos cada 60 días.
- Cree un grupo nuevo con el nombre **instructores** con un GID de 30 000.
- Cree tres usuarios nuevos: **gorwell**, **rbradbury** y **dadams**, con la contraseña **firstpw**.
- Agregue los usuarios nuevos al grupo **instructors** complementario. El grupo principal debería permanecer como el grupo privado del usuario.
- Configure las tres cuentas recientemente creadas para que venzan en 60 días a partir de hoy.
- Cambie la directiva de contraseña para la cuenta **gorwell** a fin de solicitar una contraseña nueva cada 10 días.
- Obligue a los tres usuarios creados recientemente a que cambien sus contraseñas la primera vez que inicien sesión.

a. Cambie los parámetros de configuración del sistema predeterminados para los usuarios creados recientemente a fin de garantizar que sus contraseñas se cambien por lo menos cada 60 días.

```
[student@serverX ~]$ sudo vim /etc/login.defs
[student@serverX ~]$ cat /etc/login.defs
...Output omitted...
PASS_MAX_DAYS 60
PASS_MIN_DAYS 0
PASS_MIN_LEN 5
PASS_WARN_AGE 7
...Output omitted...
```

b. Cree un grupo nuevo con el nombre instructores con un GID de 30 000.

```
[student@serverX ~]$ sudo groupadd -g 30000 instructors
[student@serverX ~]$ tail -5 /etc/group
stapdev:x:158:
pesign:x:989:
tcpdump:x:72:
slocate:x:21:
instructors:x:30000:
```

c. Cree tres usuarios nuevos: **gorwell**, **rbradbury** y **dadams** con la contraseña **firstpw** y agréguelos al grupo complementario **instructors**. El grupo principal debería permanecer como el grupo privado del usuario.

```
[student@serverX ~]$ sudo useradd -G instructors gorwell
[student@serverX ~]$ sudo useradd -G instructors rbradbury
[student@serverX ~]$ sudo useradd -G instructors dadams
[student@serverX ~]$ tail -5 /etc/group
slocate:x:21:
instructors:x:30000:gorwell,rbradbury,dadams
gorwell:x:1001:
rbradbury:x:1002:
dadams:x:1003:
[student@serverX ~]$ sudo passwd gorwell
Changing password for user gorwell.
New password: firstpw
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: firstpw
passwd: all authentication tokens updated successfully.
```

```
[student@serverX ~]$ sudo passwd rbradbury
[student@serverX ~]$ sudo passwd dadams
```

d. Determine la fecha en 60 días en el futuro y establezca esa fecha como fecha de vencimiento de cada una de las tres cuentas de usuario nuevas.

```
[student@serverX ~]$ date -d "+60 days"
Mon April  5 11:49:24 EDT 2014
[student@serverX ~]$ sudo chage -E 2014-04-05 gorwell
[student@serverX ~]$ sudo chage -E 2014-04-05 rbradbury
[student@serverX ~]$ sudo chage -E 2014-04-05 dadams
```

e. Cambie la directiva de contraseña para la cuenta **gorwell** a fin de solicitar una contraseña nueva cada 10 días.

```
[student@serverX ~]$ sudo chage -M 10 gorwell
[student@serverX ~]$ chage -l gorwell
Last password change                                    : Feb 04, 2014
Password expires                                        : Feb 14, 2014
Password inactive                                       : never
Account expires                                         : April 05, 2014
Minimum number of days between password change          : 0
Maximum number of days between password change          : 10
Number of days of warning before password expires       : 7
```

f. Obligue a los tres usuarios creados recientemente a que cambien sus contraseñas la primera vez que inicien sesión.

```
[student@serverX ~]$ sudo chage -d 0 gorwell
[student@serverX ~]$ sudo chage -d 0 rbradbury
[student@serverX ~]$ sudo chage -d 0 dadams
```

6. Cree el directorio compartido `/home/instructors` en serverX según los siguientes requisitos:

- El directorio es propiedad del usuario root y los instructores del grupo.
- Establezca los permisos en el directorio `/home/instructors` para que tenga el SETGID bit establecido en el directorio, para que el propietario y el grupo tengan permisos totales de lectura, escritura y ejecución, y otros usuarios tengan permiso de lectura del directorio.

a. Abra una ventana de terminal y conviértase en usuario root en serverX.

[student@serverX ~]$ **su -**
Password: **redhat**
[root@serverX ~]#

b. Cree el directorio `/home/instructors`.

```
[root@serverX ~]# mkdir /home/instructors
```

c. Cambie los permisos del grupo en el directorio `/home/instructors` para que pertenezca a los instructores de grupo.

```
[root@serverX ~]# chown :instructors /home/instructors
```

d. Establezca los permisos en el directorio `/home/instructors` para que sea un directorio GID bit establecidos (2), para que el propietario (7) y el grupo (7) tengan permisos totales de lectura, escritura y ejecución, y otros usuarios tengan permisos de lectura (4) del directorio.

```
[root@serverX ~]# chmod 2774 /home/instructors
```

e. Compruebe que los permisos hayan sido establecidos correctamente.

```
[root@serverX ~]# ls -ld /home/instructors
drwxrwsr--. 2 root instructors 1024 Dec 9 1:38 /home/instructors
```

7. Determine cuál es el proceso que usa la mayoría de los recursos del CPU en serverX y finalícelo.

   a. En una ventana de terminal, ejecute la utilidad **top**. Modifique el tamaño de la ventana para que sea lo más alta posible. La utilidad top clasifica todos los procesos según la utilización del CPU. El proceso cpuhog es el que tiene el uso más elevado del CPU.

```
[root@serverX ~]# top
top - 12:47:46 up  2:02,  3 users,  load average: 1.67, 1.25, 0.73
Tasks: 361 total,   6 running, 355 sleeping,   0 stopped,   0 zombie
%Cpu(s): 98.5 us,  1.4 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
KiB Mem:   2043424 total,   897112 used,  1146312 free,     1740 buffers
KiB Swap:  4079612 total,        0 used,  4079612 free.   296276 cached Me
  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 4019 root      20   0    4156     76      0 R 57.5  0.0   2:54.15 cpuhog
 2492 student   20   0 1359500 168420  37492 S 16.8  8.2   3:55.58 gnome-shell
 1938 root      20   0  189648  35972   7568 R  1.9  1.8   0:29.66 Xorg
 2761 student   20   0  620192  19688  12296 S  0.4  1.0   0:04.48 gnome-termi+
 salida truncada
```

   b. Salga de la pantalla de **top**.

      Presione **q** para salir.

   c. Finalice el proceso cpuhog con la línea de comandos. Confirme que los procesos ya no se muestren en **top**.

```
[root@serverX ~]# pkill cpuhog
```

8. Detenga el servicio de impresión cups, que está actualmente en ejecución en serverX. El servicio no debería iniciarse en forma automática en el arranque del sistema.

   a. Detenga el servicio `cups`.

   ```
   [student@serverX ~]$ sudo systemctl stop cups
   [student@serverX ~]$ sudo systemctl status cups
   ```

   b. Configure el servicio **cups** para que no se inicie en el momento de arranque del sistema.

   ```
   [student@serverX ~]$ sudo systemctl disable cups
   [student@serverX ~]$ sudo systemctl status cups
   ```

9. Configure el servicio ssh en serverX según los siguientes requisitos:

   - El usuario student en serverX puede iniciar sesión con una llave pública SSH para la cuenta student en desktopX.
   - Inhabilite el inicio de sesión de **ssh** para el usuario root y la autenticación de SSH con contraseña en serverX.

   a. Genere la clave pública de SSH en serverX como usuario student.

   ```
   [student@serverX ~]$ ssh-keygen
   ```

   b. Instale la clave pública de SSH (generada previamente en serverX) en la cuenta `student` de desktopX.

   ```
   [student@serverX ~]$ ssh-copy-id desktopX
   /usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
   ```

/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
student@desktopX's password: **student**
Number of key(s) added: 1
Now try logging into the machine, with: "ssh 'student@desktopX'"
and check to make sure that only the key(s) you wanted were added.

c. Inicie sesión, luego cambie a la cuenta root, en la máquina virtual serverX.

```
[student@serverX ~]$ su -
```

d. Personalice el servicio de ssh en serverX mediante la inhabilitación de las conexiones SSH para el usuario root y solo permita el inicio de sesión con clave.

Establezca los parámetros de archivo de configuración necesarios en `/etc/ssh/sshd_config`:

PermitRootLogin no
PasswordAuthentication no

e. Reinicie el servicio sshd en serverX.

```
[root@serverX ~]# systemctl restart sshd
```

f. En otra ventana de terminal en desktopX, valide que el usuario root no pueda conectarse a serverX con el comando **ssh**. Debería fallar porque inhabilitamos los inicios de sesión de root con el servicio de ssh.

```
[student@desktopX ~]$ ssh root@serverX
```
Password: **redhat**
Permission denied, please try again.
Password: **redhat**
Permission denied, please try again.
Password: **redhat**
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

10. Su máquina serverX ha sido reubicada en las Bahamas. Tienen que implementar los siguientes cambios en la máquina de serverX:

    - Cambie la zona horaria en la máquina de serverX para que coincida con Bahamas y verifique que la zona horaria se haya modificado en forma adecuada.

    a. Identifique la zona horaria correcta para Bahamas en serverX.

    ```
    [root@serverX ~]# tzselect
    Please identify a location so that time zone rules can be set correctly.
    Please select a continent or ocean.
    1) Africa
    2) Americas
    3) Antarctica
    4) Arctic Ocean
    5) Asia
    6) Atlantic Ocean
    7) Australia
    8) Europe
    9) Indian Ocean
    10) Pacific Ocean
    11) none - I want to specify the time zone using the Posix TZ format.
    #? 2
    Please select a country.
    1) Anguilla                 28) Haiti
    2) Antigua & Barbuda        29) Honduras
    3) Argentina                30) Jamaica
    4) Aruba                    31) Martinique
    5) Bahamas                  32) Mexico
    6) Barbados                 33) Montserrat
    ... output omitted ...
    26) Guatemala               53) Virgin Islands (US)
    ```

```
27) Guyana
#? 5
The following information has been given:
 Bahamas
Therefore TZ='America/Nassau' will be used.
Local time is now: Fri Mar  7 09:38:50 EST 2014.
Universal Time is now: Fri Mar  7 14:38:50 UTC 2014.
Is the above information OK?
1) Yes
2) No
#? 1
You can make this change permanent for yourself by appending the line
TZ='America/Nassau'; export TZ
to the file '.profile' in your home directory; then log out and log in again.
Here is that TZ value again, this time on standard output so that you
can use the /usr/bin/tzselect command in shell scripts:
America/Nassau
```

b. Cambie la zona horaria a Estados Unidos/Nassau en serverX.

```
[root@serverX ~]# timedatectl set-timezone America/Nassau
```

c. Compruebe que la zona horaria se haya configurado correctamente en serverX.

```
[root@serverX ~]# timedatectl
      Local time: Wed 2014-04-09 18:21:06 CEST
  Universal time: Wed 2014-04-09 16:21:06 UTC
        RTC time: Wed 2014-04-09 16:21:06
        Timezone: America/Nassau (CEST, +0200)
     NTP enabled: yes
NTP synchronized: no
RTC in local TZ: no
      DST active: yes
```

Last DST change: DST began at
Sun 2014-03-30 01:59:59 CET
Sun 2014-03-30 03:00:00 CEST
Next DST change: DST ends (the clock jumps one hour backwards) at
Sun 2014-10-26 02:59:59 CEST
Sun 2014-10-26 02:00:00 CET

11. Registre el comando para mostrar todas las entradas del diario de **systemd** registradas entre las 9:05:00 y las 9:15:00 en el archivo `/home/student/systemdreview.txt`.

```
[root@serverX ~]# echo "journalctl --since 9:05:00 --until 9:15:00" >/home/student/systemdreview.txt
```

12. Configure **rsyslogd** mediante el agregado de una regla al archivo de configuración creado recientemente `/etc/rsyslog.d/auth-errors.conf` para registrar todos los mensajes de autenticación que se graban en el recurso authpriv con el alerta de prioridad, y también más alto en el archivo `/var/log/auth-errors`. Pruebe la directiva de registro agregada recientemente con el comando **logger**.

    a. Agregue la directiva para registrar los mensajes de syslog **authpriv.alert** en el archivo `/var/log/auth-errors` en el archivo de configuración `/etc/rsyslog.d/auth-errors.conf`.

    ```
    [root@serverX ~]# echo "authpriv.alert /var/log/auth-errors" >/etc/rsyslog.d/auth-errors.conf
    ```

    b. Reinicie el servicio **rsyslog** en serverX.

    ```
    [root@serverX ~]# systemctl restart rsyslog
    ```

    c. Use **logger** para crear una nueva entrada de registro para `/var/log/auth-errors` en serverX.

    ```
    [root@serverX ~]# logger -p authpriv.alert "Logging test authpriv.alert"
    ```

    d. Verifique que el mensaje enviado a syslog con el comando **logger** aparezca en el archivo `/var/log/auth-errors`, en serverX en la terminal con **tail /var/log/auth-errors**.

```
[root@serverX ~]# tail /var/log/auth-errors
Feb 13 11:21:53 server1 root: Logging test authpriv.alert
```

13. Cree una conexión de red estática nueva con los parámetros de configuración que están en la siguiente tabla. Asegúrese de reemplazar la *X* con el número correcto para sus sistemas.

    - Configure la conexión nueva para que se inicie en forma automática.
    - Otras conexiones no deberían iniciarse automáticamente.
    - Modifique la conexión nueva para que también use la dirección 10.0.X.1/24.
    - Configure el archivo `hosts` para que 10.0.X.1 pueda denominarse como "myhost".
    - Configure el nombre del host en el servidor *X*.example.com.

Parámetro	Configuración
Nombre de la conexión	revisión
Dirección IP	172.25.*X*.11/16
Dirección de puerta de enlace	172.25.*X*.254
Dirección DNS	172.25.254.254

    a. Cree una conexión de red estática nueva con los parámetros de configuración que están en la tabla. Asegúrese de reemplazar la *X* con el número correcto para sus sistemas.

```
[root@serverX ~]# nmcli con add con-name review ifname eth0 type ethernet ip4 172.25.X.11/24
gw4 172.25.X.254
[root@serverX ~]# nmcli con mod "review" ipv4.dns 172.25.254.254
```

b. Configure la conexión nueva para que se inicie en forma automática. Otras conexiones no deberían iniciarse automáticamente.

```
[root@serverX ~]# nmcli con mod "review" connection.autoconnect yes
[root@serverX ~]# nmcli con mod "System eth0" connection.autoconnect no
```

c. Modifique la conexión nueva para que también use la dirección 10.0.X.1/24.

```
[root@serverX ~]# nmcli con mod "review" +ipv4.addresses 10.0.X.1/24
```

O, de lo contrario:

```
[root@serverX ~]# echo "IPADDR1=10.0.X.1" >> /etc/sysconfig/network-scripts/ifcfg-review
[root@serverX ~]# echo "PREFIX1=24" >> /etc/sysconfig/network-scripts/ifcfg-review
```

d. Configure el archivo `hosts` para que 10.0.X.1 pueda denominarse como "myhost"..

```
[root@serverX ~]# echo "10.0.X.1  myhost" >> /etc/hosts
```

e. Configure el nombre del host en el servidor *X*.example.com.

```
[root@serverX ~]# hostnamectl set-hostname serverX.example.com
```

14. Sincronice el árbol de directorio `/etc` en serverX para el directorio `/configbackup` en serverX.

a. Para poder crear el directorio de destino `/configbackup`, cambie a la cuenta de usuario root con el comando **su**.

```
[student@serverX ~]$ su -
Password: redhat
[root@desktopX ~]#
```

b. Cree el directorio de destino para los archivos de configuración de serverX.

```
[root@serverX ~]# mkdir /configbackup
```

c. Use el comando **rsync** para sincronizar el árbol de directorio `/etc` en serverX para el directorio `/configsync` en serverX. Tenga en cuenta que solo el usuario root puede leer todo el contenido del directorio `/etc` en serverX.

```
[root@serverX ~]# rsync -av /etc /configbackup
...
```

15. Cree un archivo con el nombre `/root/configuration-backup-server.tar.gz` con el directorio `/configbackup` como contenido.

a. Guarde el directorio `/configbackup` en el archivo `/root/configuration-backup-server.tar.gz`.

```
[root@serverX ~]# tar czf /root/configuration-backup-server.tar.gz /configbackup
```

16. Para preparar el árbol de directorio archivado a fin de compararlo con los archivos de configuración usados en forma activa y actual en serverX, extraiga los contenidos del archivo `/root/configuration-backup-server.tar.gz` en el directorio `/tmp/configcompare/` en serverX.

a. Conéctese a la máquina de serverX como usuario root con **ssh**.

```
[root@desktopX ~]# ssh root@serverX
Password: redhat
[root@serverX ~]#
```

b. Cree el directorio de destino `/tmp/configcompare/` donde se extraerá los contenidos del archivo `/root/configuration-backup-server.tar.gz`.

```
[root@serverX ~]# mkdir /tmp/configcompare
```

c. Cambie el directorio de destino `/tmp/configcompare/` en serverX.

```
[root@serverX ~]# cd /tmp/configcompare
[root@serverX configcompare]#
```

d. Extraiga los contenidos del archivo `/root/configuration-backup-server.tar.gz` en el directorio `/tmp/configcompare/` de serverX.

```
[root@serverX configcompare]# tar xzf /root/configuration-backup-server.tar.gz
```

17. Realice las siguientes tareas en la máquina de serverX:

- Use **ssh** para ejecutar el comando **hostname** en desktopX como usuario student. Envíe el resultado del comando **hostname** al archivo `/tmp/scpfile.txt` en desktopX.
- Use **scp** para copiar el archivo `/tmp/scpfile.txt` desde desktopX hacia `/home/student/scpfile.txt`.

a. Use **ssh** para ejecutar el comando **hostname** en desktopX como usuario student. Envíe el resultado del comando **hostname** al archivo `/tmp/scpfile.txt` en desktopX.

```
[root@serverX ~]# ssh student@desktopX 'hostname >/tmp/scpfile.txt'
```

b. Use **scp** para copiar el archivo `/tmp/scpfile.txt` desde desktopX hacia `/home/student/scpfile.txt` en la máquina que tiene instalado serverX.

```
[root@serverX ~]# scp root@desktopX:/tmp/scpfile.txt /home/student/
```

18. Cree el archivo `/etc/yum.repos.d/localupdates.repo` para habilitar el repositorio “Updates” que está en la máquina content. Debería acceder al contenido que está en la siguiente URL: http://content.example.com/rhel7.0/x86_64/errata. *No* controle las firmas de GPG.

Cree el archivo `/etc/yum.repos.d/localupdates.repo` con el siguiente contenido:

[updates]
name=Red Hat Updates
baseurl=http://content.example.com/rhel7.0/x86_64/errata
enabled=1
gpgcheck=0

19. Configure serverX para que respete los requisitos de software específico.

    - El paquete `núcleo` debe actualizarse a la versión más reciente.
    - Debe instalarse el paquete `xsane-gimp`.
    - Debe instalarse el paquete `rht-system`.
    - Por motivos de seguridad, serverX no debe tener instalado el paquete `wvdial`.

    a. Actualice el paquete `núcleo`.

       yum update kernel

    b. Instale el paquete `xsane-gimp`..

       yum install xsane-gimp

    c. Instale el paquete `rht-system`..

       yum install rht-system

    d. Por motivos de seguridad, serverX no debe tener instalado el paquete `wvdial`.

       yum remove wvdial

20. Genere un informe de uso con el comando **du** del directorio `/usr/share/fonts` en serverX y guarde el resultado en el archivo `/home/student/dureport.txt`.

```
[root@serverX ~]# du /usr/share/fonts >/home/student/dureport.txt
```

21. Identifique y monte un sistema de archivos agregado recientemente por UUID en el directorio `/mnt/datadump` en serverX.

    a. Identifique el sistema de archivos agregados recientemente con el comando **blkid** en serverX.

    ```
    [root@serverX ~]# blkid
    /dev/vda1: UUID="46f543fd-78c9-4526-a857-244811be2d88" TYPE="xfs"
    /dev/vdb1: UUID="a84f6842-ec1d-4f6d-b767-b9570f9fcdc0" TYPE="xfs"
    ```

    b. Cree el punto de montaje `/mnt/datadump` en serverX.

    ```
    [root@serverX ~]# mkdir /mnt/datadump
    ```

    c. Monte el sistema de archivos de UUID en el directorio `/mnt/datadump` en la máquina de serverX.

    ```
    [root@serverX ~]# mount UUID="a84f6842-ec1d-4f6d-b767-b9570f9fcdc0" /mnt/datadump
    ```

22. Cree el enlace blando `/root/mydataspace`, que apunte al directorio `/mnt/datadump` en serverX.

```
[root@serverX ~]# ln -s /mnt/datadump /root/mydataspace
```

23. Registre el comando para encontrar todos los enlaces flexibles en serverX que tengan `datos` como parte de su nombre en el archivo `/home/student/find.txt`.

```
[root@serverX ~]# echo "find / -type l -name '*data*'" >/home/student/find.txt
```

24. Cuando esté listo para controlar su trabajo, ejecute **lab sa1-review grade** en `serverX`.

```
[root@serverX ~]# lab sa1-review grade
```

Back Continue to next Lesson