Capacitación integral y práctica que resuelve los problemas del mundo real

Red Hat System Administration II

Manual del alumno (ROLE)

RH134-RHEL7-es-3-20170803

RED HAT SYSTEM ADMINISTRATION II

Red Hat Enterprise Linux 7 RH134
Red Hat System Administration II
Edición 3 20170803

Autores: Wander Boessenkool, Bruce Wolfe, Scott McBrien, George Hacker, Chen Chang
Editor: Steven Bonneville

Colaboradores: Rob Locke, Bowe Strickland, Forrest Taylor, Rudolf Kastl

Revisores: Michael Phillips, Lars Bohnsack, Michael Bashford, Clint Tinsley

Encargados del mantenimiento: Anuj Verma, Mary Tomson, Michael Jarrett

Convenciones del documento

Notas y advertencias

Nota

Las "notas" son consejos, atajos o enfoques alternativos para una tarea determinada. Omitir una nota no debería tener consecuencias negativas, pero quizás se pase por alto algún truco que puede simplificar una tarea.

Referencias

En las "referencias", se describe el lugar donde se puede encontrar documentación externa relevante para un tema.

Importante

En los cuadros “importantes”, se detallan cosas que se olvidan con facilidad: cambios de configuración que solo se aplican a la sesión actual o servicios que se deben reiniciar para poder aplicar una actualización. Omitir un cuadro con la etiqueta “Importante” no provocará pérdida de datos, pero puede causar irritación y frustración.

Advertencia

No se deben omitir las “advertencias”. Es muy probable que omitir las advertencias provoque la pérdida de datos.

Introducción

Red Hat System Administration II

Este curso está diseñado específicamente para estudiantes que hayan completado el curso Red Hat System Administration I (RH124). Red Hat System Administration I (RH134) se centra en las tareas principales necesarias para convertirse en un administrador de Linux de tiempo completo y validar esas habilidades mediante el examen de Administrador de sistemas certificado de Red Hat. Este curso aborda en detalle la administración de Linux empresarial, que incluye sistemas de archivos y partición, volúmenes lógicos, SELinux, funciones de firewall y solución de problemas.

Objetivos del curso

- Ampliar las habilidades obtenidas durante el curso de Red Hat System Administration I (RH124).
- Desarrollar las habilidades necesarias para un administrador de sistemas Red Hat Enterprise Linux con certificación RHCSA.

Destinatarios

- Este curso está diseñado particularmente para estudiantes que hayan completado el curso Red Hat System Administration I (RD124). Por la organización de los temas, no es adecuado que un estudiante use RH134 como punto de entrada del plan de estudios. Se alienta a los estudiantes que no hayan tomado un curso de Red Hat anterior a tomar System Administrations I si no conocen Linux o el curso RHCSA Fast Track (RH200) si tienen experiencia con la administración de Linux empresarial.

Requisitos previos

- Haber realizado el curso de Red Hat System Administration I (RH124), o tener conocimientos equivalentes.

Orientación sobre el entorno del trabajo de laboratorio en el aula

En este curso, los estudiantes realizarán mayormente ejercicios prácticos y trabajo de laboratorio con dos sistemas informáticos, que se llamarán **`desktop`** y **`server`**. Los nombres de host de estas máquinas son desktop*X*.example.com y server*X*.example, donde *X* en los nombres de host de las computadoras será un número que variará de un estudiante a otro. Las dos máquinas tienen una cuenta de usuario estándar, *student*, con la contraseña *student*. La contraseña *raíz* de los dos sistemas es *redhat*.

En un aula de aprendizaje en línea de Red Hat, se asignarán a los estudiantes computadoras remotas a las que accederán mediante una aplicación web alojada en rol.redhat.com. Los estudiantes deberán iniciar sesión en esta máquina con las credenciales de usuario que se proporcionaron cuando se registraron en la clase.

Los sistemas que utilizan los estudiantes emplean diferentes subredes IPv4. En el caso de un estudiante específico, su red IPv4 es 172.25.*X*.0/24, donde el valor *X* coincide con el número en el nombre del host de sus sistemas **`desktop`** y **`server`**.

Máquinas del aula

Nombre de la máquina	Direcciones IP	Rol
desktop*X*.example.com	172.25.*X*.10	Computadora "cliente" del estudiante
server*X*.example.com	172.25.*X*.11	Computadora "servidor" del estudiante

Control de sus estaciones
En la parte superior de la consola se describe el estado de su máquina.

Estados de la máquina

Estado	Descripción
none (ninguno)	Todavía no se ha iniciado su máquina. Cuando se inicie, su máquina arrancará en un estado recientemente inicializado (el escritorio se habrá restablecido).
starting (en inicio)	Su máquina está por arrancar.
running (en ejecución)	Su máquina se está ejecutando y está disponible (o bien, cuando arranque, pronto lo estará).
stopping (en detención)	Su máquina está por apagarse.
stopped (detenida)	Su máquina se ha apagado completamente. Al iniciarse, su máquina arrancará en el mismo estado en el que estaba cuando se apagó (el disco se habrá preservado).
impaired (afectada)	No se puede realizar una conexión de red en su máquina. En general, este estado se logra cuando un estudiante ha corrompido las reglas de conexión de la red o del cortafuegos. Si se reinicia la máquina y el estado permanece, o si es intermitente, deberá abrir un caso de soporte.

Según el estado de su máquina, tendrá disponibles una selección de las siguientes acciones.

Acciones de la máquina

Acción	Descripción
Start Station (Iniciar estación)	Iniciar (“encender”) la máquina.
Stop Station (Detener estación)	Detener (“apagar”) la máquina y preservar el contenido del disco.
Reset Station (Restablecer estación)	Detener (“apagar”) la máquina y restablecer el disco de modo que vuelva a su estado original. **Precaución: Se perderá cualquier trabajo generado en el disco.**
Actualización	Si se actualiza la página, se volverá a realizar un sondeo del estado de la máquina.
Increase Timer (Aumentar temporizador)	Agrega 15 minutos al temporizador para cada clic.

Temporizador de la estación

Su inscripción al aprendizaje en línea de Red Hat le da derecho a una cierta cantidad de tiempo de uso del equipo. Para ayudarlo a conservar su tiempo, las máquinas tienen un temporizador asociado, que se inicializa en 60 minutos cuando se inicia su máquina.

El temporizador funciona como un "interruptor de seguridad", que disminuye mientras funciona su máquina. Si el temporizador se reduce por debajo de 0, puede optar por incrementar el temporizador.

Internacionalización

Compatibilidad de idioma

Red Hat Enterprise Linux 7 admite oficialmente 22 idiomas: inglés, asamés, bengalí, chino (simplificado), chino (tradicional), francés, alemán, guyaratí, hindi, italiano, japonés, canarés, coreano, malayalam, maratí, oriya, portugués (brasileño), panyabí, ruso, español, tamil y telugú.

Selección de idioma por usuario

Es posible que los usuarios prefieran usar un idioma diferente para su entorno de escritorio distinto al predeterminado del sistema. Quizás también quieran definir su cuenta para usar una distribución del teclado o un método de entrada distinto.

Configuración de idioma

En el entorno de escritorio GNOME, posiblemente el usuario deba definir el idioma de su preferencia y el método de entrada la primera vez que inicie sesión. Si no es así, la manera más simple para un usuario individual de definir el idioma de su preferencia y el método de entrada es usando la aplicación **Region & Language** (Región e idioma). Ejecute el comando **`gnome-control-center region`** o en la barra superior, seleccione **(User) (Usuario)** > **Settings (Parámetros)**. En la ventana que se abre, seleccione **Region & Language** (Región e idioma). El usuario puede hacer clic en la casilla **Language** (Idioma) y seleccionar el idioma de su preferencia de la lista que aparece. Esto también actualizará la configuración **Formats** (Formatos) mediante la adopción del valor predeterminado para ese idioma. La próxima vez que el usuario inicie sesión, se efectuarán los cambios.

Estas configuraciones afectan al entorno de escritorio GNOME y todas las aplicaciones, incluida **`gnome-terminal`**, que se inician dentro de este. Sin embargo, no se aplican a la cuenta si el acceso a ella es mediante un inicio de sesión **`ssh`** desde un sistema remoto o desde una consola de texto local (como **`tty2`**).

nota

Un usuario puede hacer que su entorno de shell use la misma configuración de **`LANG`** que su entorno gráfico, incluso cuando inician sesión mediante una consola de texto o mediante **`ssh`**. Una manera de hacer esto es colocar un código similar al siguiente en el archivo **`~/.bashrc`** del usuario. Este código de ejemplo definirá el idioma empleado en un inicio de sesión en interfaz de texto, de modo que coincida con el idioma actualmente definido en el entorno de escritorio GNOME del usuario.

```
i=$(grep 'Language=' /var/lib/AccountService/users/${USER} \
  | sed 's/Language=//')
if [ "$i" != "" ]; then
    export LANG=$i
fi
```

Es posible que algunos idiomas, como el japonés, coreano, chino y otros con un conjunto de caracteres no latinos, no se vean correctamente en consolas de texto locales.

Se pueden crear comandos individuales para utilizar otro idioma mediante la configuración de la variable **LANG** en la línea de comandos:

```
[user@host ~]$ LANG=fr_FR.utf8 date
jeu. avril 24 17:55:01 CDT 2014
```

Los comandos subsiguientes se revertirán y utilizarán el idioma de salida predeterminado del sistema. El comando **locale** se puede usar para comprobar el valor actual de **LANG** y otras variables de entorno relacionadas.

Valores del método de entrada
GNOME 3 en Red Hat Enterprise Linux 7 emplea de manera automática el sistema de selección de método de entrada **IBus**, que permite cambiar las distribuciones del teclado y los métodos de entrada de manera rápida y sencilla.

La aplicación **Region & Language** (Región e idioma) también se puede usar para habilitar métodos de entrada alternativos. En la ventana de la aplicación **Region & Language** (Región e idioma), la casilla **Input Sources** (Fuentes de entrada) muestra los métodos de entrada disponibles en este momento. De forma predeterminada, es posible que **English (US)** (Inglés [EE. UU.]) sea el único método disponible. Resalte **English (US)** (Inglés [EE. UU.]) y haga clic en el ícono de **keyboard** (teclado) para ver la distribución actual del teclado.

Para agregar otro método de entrada, haga clic en el botón **+**, en la parte inferior izquierda de la ventana **Input Sources** (Fuentes de entrada). Se abrirá la ventana **Add an Input Source** (Añadir una fuente de entrada). Seleccione su idioma y, luego, el método de entrada o la distribución del teclado de su preferencia.

Una vez que haya más de un método de entrada configurado, el usuario puede alternar entre ellos rápidamente escribiendo **Super**+**Space** (en ocasiones denominado **Windows**+**Space**). También *indicador de estado* en la barra superior de GNOME con dos funciones: por un lado, indica el método de entrada activo; por el otro lado, funciona como un menú que puede usarse para cambiar de un método de entrada a otro o para seleccionar funciones avanzadas de métodos de entrada más complejos.

Algunos de los métodos están marcados con engranajes, que indican que tienen opciones de configuración y capacidades avanzadas. Por ejemplo, el método de entrada japonés **Japanese (Kana Kanji)** (japonés [Kana Kanji]) le permite al usuario editar previamente texto en latín y usar las teclas de **Down Arrow** (flecha hacia abajo) y **Up Arrow** (flecha hacia arriba) para seleccionar los caracteres correctos que se usarán.

El indicador también puede ser de utilidad para los hablantes de inglés de Estados Unidos. Por ejemplo, dentro de **English (United States)** (Inglés [Estados Unidos]) está la configuración del teclado **English (international AltGr dead keys)**, que trata **AltGr** (o la tecla **Alt** derecha) en un teclado de 104/105 teclas de una PC como una tecla m"Bloq Mayús secundaria" y tecla de activación de teclas muertas para escribir caracteres adicionales. Hay otras distribuciones alternativas disponibles, como Dvorak.

nota

Cualquier carácter Unicode puede ingresarse en el entorno de escritorio GNOME, si el usuario conoce el código Unicode del carácter, escribiendo **Ctrl**+**Shift**+**U**, seguido por el código. Después de ingresar **Ctrl**+**Shift**+**U**, aparecerá una **u** subrayada que indicará que el sistema espera la entrada del código Unicode.

Por ejemplo, la letra del alfabeto griego en minúscula lambda tiene el código U +03BB y puede ingresarse escribiendo **Ctrl**+**Shift**+**U**, luego **03bb** y, por último, **Enter**.

Valores de idioma predeterminado en todo el sistema

El idioma predeterminado del sistema está definido en US English, que utiliza la codificación UTF-8 de Unicode como su conjunto de caracteres (**en_US.utf8**), pero puede cambiarse durante o después de la instalación.

Desde la línea de comandos, *root* puede cambiar la configuración local de todo el sistema con el comando **localectl** . Si **localectl** se ejecuta sin argumentos, mostrará la configuración local de todo el sistema actual.

Para configurar el idioma de todo el sistema, ejecute el comando **localectl set-locale LANG=*locale***, donde *locale* es el **$LANG** adecuado de la tabla “Referencia de códigos de idioma” en este capítulo. El cambio tendrá efecto para usuarios en su próximo inicio de sesión y se almacena en **/etc/locale.conf**.

```
[root@host ~]# localectl set-locale LANG=fr_FR.utf8
```

En GNOME, un usuario administrativo puede cambiar esta configuración en **Region & Language** (Región e idioma) y al hacer clic en el botón **Login Screen** (Pantalla de inicio de sesión) ubicado en la esquina superior derecha de la ventana. Al cambiar la opción de **Language** (Idioma) de la pantalla de inicio de sesión, también ajustará el valor de idioma predeterminado de todo el sistema en el archivo de configuración **/etc/locale.conf**.

Importante

Las consolas de texto locales como **tty2** están más limitadas en las fuentes que pueden mostrar que las sesiones **gnome-terminal** y **ssh**. Por ejemplo, los caracteres del japonés, coreano y chino posiblemente no se visualicen como se espera en una consola de texto local. Por este motivo, es posible que tenga sentido usar el inglés u otro idioma con un conjunto de caracteres latinos para la consola de texto del sistema.

De manera similar, las consolas de texto locales admiten una cantidad de métodos de entrada también más limitada y esto se administra de manera separada desde el entorno de escritorio gráfico. La configuración de entrada global disponible se puede configurar mediante **localectl** tanto para consolas virtuales de texto locales como para el entorno gráfico X11. Para obtener más información, consulte las páginas del manual **localectl**(1), **kbd**(4) y **vconsole.conf**(5).

Paquetes de idiomas

Si utiliza un idioma diferente al inglés, posiblemente desee instalar “paquetes de idiomas” adicionales para disponer de traducciones adicionales, diccionarios, etcétera. Para ver la lista de paquetes de idiomas disponibles, ejecute **yum langavailable**. Para ver la lista de paquetes de idiomas actualmente instalados en el sistema, ejecute **yum langlist**. Para agregar un paquete de idioma adicional al sistema, ejecute **yum langinstall *code***, donde *code* (código) es el código en corchetes después del nombre del idioma en el resultado de **yum langavailable**.

Referencias

Páginas del manual: **locale**(7), **localectl**(1), **kbd**(4), **locale.conf**(5), **vconsole.conf**(5), **unicode**(7), **utf-8**(7) y **yum-langpacks**(8).

Las conversiones entre los nombres de las configuraciones X11 del entorno de escritorio gráfico y sus nombres en **localectl** se pueden encontrar en el archivo **/usr/share/X11/xkb/rules/base.lst**.

Referencia de códigos de idioma

Códigos de idioma

Idioma	Valor $LANG
Inglés (EE. UU.)	en_US.utf8
Asamés	as_IN.utf8
Bengalí	bn_IN.utf8
Chino (simplificado)	zh_CN.utf8
Chino (tradicional)	zh_TW.utf8
Francés	fr_FR.utf8
Alemán	de_DE.utf8
Guyaratí	gu_IN.utf8
Hindi	hi_IN.utf8
Italiano	it_IT.utf8
Japonés	ja_JP.utf8
Canarés	kn_IN.utf8
Coreano	ko_KR.utf8
Malayalam	ml_IN.utf8
Maratí	mr_IN.utf8
Odia	or_IN.utf8
Portugués (brasileño)	pt_BR.utf8
Panyabí	pa_IN.utf8
Ruso	ru_RU.utf8
Español	es_ES.utf8
Tamil	ta_IN.utf8
Telugú	te_IN.utf8

redhat. TRAINING

CAPÍTULO 1

AUTOMATIZACIÓN DE LA INSTALACIÓN CON KICKSTART

Descripción general	
Meta	Automatizar la instalación de sistemas Red Hat Enterprise Linux con Kickstart.
Objetivos	• Explicar los conceptos y la arquitectura de Kickstart. • Crear un archivo de configuración kickstart.
Secciones	• Definición del sistema Anaconda Kickstart (y práctica) • Implementación de un nuevo sistema virtual con Kickstart (y práctica)
Prueba del capítulo	• Automatización de la instalación con Kickstart

Definición del sistema Anaconda Kickstart

Objetivos

Luego de completar esta sección, los estudiantes deberían poder identificar elementos de configuración clave que se encuentran dentro de un archivo de configuración Kickstart.

Introducción a instalaciones Kickstart

Un administrador de sistemas puede automatizar la instalación de Red Hat Enterprise Linux usando una función denominada *Kickstart*. Anaconda, el instalador de Red Hat, necesita recibir instrucciones de cómo instalar un sistema: particionar discos, configurar interfaces de redes, seleccionar qué paquetes instalar, etc. Este es un proceso interactivo de forma predeterminada. Una instalación Kickstart usa un archivo de texto para proporcionar todas las respuestas a estas preguntas, de modo que no se requiere interacción.

nota

En Red Hat Enterprise Linux, Kickstart es similar a Jumpstart de Oracle Solaris o a la instalación desatendida de Microsoft Windows.

Los archivos de configuración Kickstart comienzan con una lista de comandos que definen cómo se instalará la máquina de destino. Las líneas que comienzan con caracteres **#** son comentarios que son ignorados por el instalador. Las secciones adicionales comienzan con una línea que comienza con un carácter **%** y termina con una línea con la directiva **%end**.

La sección **%packages** especifica el software que se instalará en el sistema de destino. Los paquetes individuales se especifican por nombre (sin versiones). Los grupos de paquetes se pueden especificar por nombre o id. y comienzan con el carácter **@**. Los grupos del entorno (grupos de grupos de paquetes) se pueden especificar con **@^** seguido inmediatamente por el nombre o id. del grupo de entorno. Los grupos tienen componentes obligatorios, predeterminados y opcionales. Normalmente, los componentes obligatorios y predeterminados serán instalados por Kickstart. Los nombres de paquetes o grupos precedidos por un carácter **-** quedan excluidos de la instalación a menos que sean obligatorios o se instalen debido a dependencias de RPM de otros paquetes.

Dos secciones adicionales son los scripts **%pre** y **%post**. Los scripts **%post** son más comunes. Configuran el sistema después de que todo el software ha sido instalado. El script **%pre** se ejecuta antes de que haga alguna partición del disco.

Los comandos de configuración deben especificarse primero. Los **%pre**, **%post** y **%packages** pueden ocurrir en cualquier orden luego de los comandos de configuración.

Comandos de archivo de configuración Kickstart

Comandos de instalación

- **url**: Especifica la ubicación de los medios de instalación.

  Ejemplo:

```
url --url="ftp://installserver.example.com/pub/RHEL7/dvd"
```

- **repo**: Esta opción indica a Anaconda dónde encontrar los paquetes para la instalación. Esta opción debe apuntar a un repositorio **yum** válido.

  Ejemplo:

```
repo --name="Custom Packages" --baseurl="ftp://repo.example.com/custom"
```

- **text**: Fuerza la instalación del modo de texto.
- **vnc**: Permite la visualización de forma remota de la instalación gráfica vía VNC.

  Ejemplo:

```
vnc --password=redhat
```

- **askmethod**: No usa automáticamente el CD-ROM como fuente de paquetes cuando los medios de instalación se detectan en la unidad de CD-ROM.

Comandos de partición

- **clearpart**: Borra las particiones especificadas antes de la instalación.

  Ejemplo:

```
clearpart --all --drives=sda,sdb --initlabel
```

- **part**: Especifica el tamaño, el formato y el nombre de una partición.

  Ejemplo:

```
part /home --fstype=ext4 --label=homes --size=4096 --maxsize=8192 --grow
```

- **ignoredisk**: Ignora los discos especificados durante la instalación.

  Ejemplo:

```
ignoredisk --drives=sdc
```

- **bootloader**: Define dónde instalar el cargador de arranque.

  Ejemplo:

```
bootloader --location=mbr --boot-drive=sda
```

- **volgroup**, **logvol**: Crea grupos de volúmenes LVM y volúmenes lógicos.

  Ejemplo:

```
part pv.01 --size=8192
volgroup myvg pv.01
logvol / --vgname=myvg --fstype=xfs --size=2048 --name=rootvol --grow
```

```
logvol /var --vgname=myvg --fstype=xfs --size=4096 --name=varvol
```

- **zerombr**: Se inicializan los discos cuyo formato no se reconoce.

Comandos de red

- **network**: Configura la información de red para el sistema de destino y activa dispositivos de red en el entorno del instalador.

  Ejemplo:

```
network --device=eth0 --bootproto=dhcp
```

- **firewall**: Esta opción define cómo se configurará el firewall en el sistema de destino.

  Ejemplo:

```
firewall --enabled --service=ssh,cups
```

Comandos de configuración

- **lang**: Este comando obligatorio establece el idioma para usar durante la instalación y el idioma predeterminado del sistema instalado.

  Ejemplo:

```
lang en_US.UTF-8
```

- **keyboard**: Este comando obligatorio establece el tipo de teclado del sistema.

  Ejemplo:

```
keyboard --vckeymap=us --xlayouts='us','us'
```

- **timezone**: Define la zona horaria, los servidores NTP y si el reloj del hardware usa UTC.

  Ejemplo:

```
timezone --utc --ntpservers=time.example.com Europe/Amsterdam
```

- **auth**: Este comando obligatorio establece opciones de autenticación para el sistema.

  Ejemplo:

```
auth --useshadow --enablemd5 --passalgo=sha512
```

- **rootpw**: Define la contraseña **raíz** inicial.

  Ejemplo:

```
rootpw --plaintext redhat
```

o

```
rootpw --iscrypted $6$KUnFfrTzO8jv.PiH$YlBbOtXBkWzoMuRfb0.SpbQ....XDR1UuchoMG1
```

- **`selinux`**: Establece el estado de SELinux en el sistema instalado.

  Ejemplo:

  ```
  selinux --enforcing
  ```

- **`services`**: Modifica el conjunto de servicios predeterminados que se ejecutarán en el destino **`systemd`** predeterminado.

  Ejemplo:

  ```
  services --disabled=network,iptables,ip6tables --enabled=NetworkManager,firewalld
  ```

- **`group`**, **`user`**: Crea un grupo o usuario locales en el sistema.

  Ejemplo:

  ```
  group --name=admins --gid=10001
  user --name=jdoe --gecos="John Doe" --groups=admins --password=changeme --plaintext
  ```

Comandos varios

- **`logging`**: Este comando define cómo Anaconda se registrará durante la instalación.

  Ejemplo:

  ```
  logging --host=loghost.example.com --level=info
  ```

- **`firstboot`**: Determina si el primer arranque se inicia la primera vez que se inicia el sistema.

  Ejemplo:

  ```
  firstboot --disabled
  ```

- **`reboot`**, **`poweroff`**, **`halt`**: Especifica qué debe suceder luego de finalizada la instalación.

nota

La utilidad **`ksverdiff`** del paquete *pykickstart* sirve para identificar cambios en la sintaxis del archivo Kickstart entre dos versiones de Red Hat Enterprise Linux o Fedora.

Por ejemplo, **`ksverdiff -f RHEL6 -t RHEL7`** identificará cambios en la sintaxis de RHEL 6 a RHEL 7. Las versiones disponibles se enumeran en la parte superior del archivo **`/usr/lib/python2.7/site-packages/pykickstart/version.py`**.

Ejemplo de un archivo kickstart:

La primera parte del archivo consta de los comandos de instalación, como la partición del disco y la fuente de instalación.

```
#version=RHEL7
# System authorization information
auth --useshadow --enablemd5
# Use network installation
url --url="http://classroom.example.com/content/rhel7.0/x86_64/dvd/"
# Firewall configuration
firewall --enabled --service=ssh
firstboot --disable
ignoredisk --only-use=vda
# Keyboard layouts
keyboard --vckeymap=us --xlayouts='us','us'
# System language
lang en_US.UTF-8
# Installation logging level
logging --level=info
# Network information
network  --bootproto=dhcp
# Root password
rootpw --iscrypted $6$/h/Mumvarr2dKrv1$Krv7h9.QoV0s....foMXsGXP1KllaiJ/w7EWiL1
# SELinux configuration
selinux --enforcing
# System services
services --disabled="kdump,rhsmcertd" --enabled="network,sshd,rsyslog,chronyd"
# System timezone
timezone --utc America/Los_Angeles
# System bootloader configuration
bootloader --location=mbr --boot-drive=vda
# Clear the Master Boot Record
zerombr
# Partition clearing information
clearpart --all --initlabel
# Disk partitioning information
part / --fstype="xfs" --ondisk=vda --size=10000
```

La segunda parte contiene la sección **`%packages`**, que detalla qué paquetes y grupo de paquetes deben instalarse, y qué paquetes no deben instalarse.

```
%packages
@core
chrony
cloud-init
```

```
dracut-config-generic
dracut-norescue
firewalld
grub2
kernel
rsync
tar
-NetworkManager
-plymouth

%end
```

La última parte contiene todos los scripts de instalación **%pre** y **%post**.

```
%post --erroronfail

# For cloud images, 'eth0' _is_ the predictable device name, since
# we don't want to be tied to specific virtual (!) hardware
rm -f /etc/udev/rules.d/70*
ln -s /dev/null /etc/udev/rules.d/80-net-name-slot.rules

# simple eth0 config, again not hard-coded to the build hardware
cat > /etc/sysconfig/network-scripts/ifcfg-eth0 << EOF
DEVICE="eth0"
BOOTPROTO="dhcp"
ONBOOT="yes"
TYPE="Ethernet"
USERCTL="yes"
PEERDNS="yes"
IPV6INIT="no"
EOF

%end
```

nota

En un archivo Kickstart, si no se determinan los valores obligatorios, el instalador solicitará una repuesta interactivamente o abortará la instalación por completo.

Referencias

Página del manual (1)**ksverdiff**

El archivo **/usr/share/doc/pykickstart-*/kickstart-docs.txt**cproporcionado por el paquete *pykickstart* contiene información útil y detallada sobre la sintaxis de archivos Kickstart.

Es posible que haya información adicional disponible en la *Guía de instalación de Red Hat Enterprise Linux* para RHEL 7 ubicada en:

> https://access.redhat.com/documentation/

Práctica: Sintaxis y modificación del archivo Kickstart

Relacione los comandos Kickstart con sus descripciones en la tabla.

`%packages`	`%post`	`auth`	`clearpart`	`network`
`part`	`rootpw`	`services`	`timezone`	`url`

Descripción	Comando
Sección del archivo de configuración Kickstart que especifica qué software está instalado en el nuevo sistema.	
Comando de Kickstart obligatorio que configura cómo los usuarios acceden al sistema.	
Ubicación del software usado por Kickstart para instalar un sistema.	
Script en un archivo de configuración Kickstart que se ejecuta luego de que el software está instalado en un sistema.	
Comando Kickstart que especifica qué particiones deben borrarse antes de la instalación.	
Modifica qué servicios iniciarán de forma predeterminada en el arranque del sistema.	

Descripción	Comando
Define las credenciales de autenticación predeterminadas para el superusuario.	
Comando Kickstart que especifica el tamaño, el formato y el nombre de una partición de disco.	
Comando Kickstart usado para especificar servidores NTP.	
Determina la configuración de red para la instalación y el sistema de destino.	

Solución

Relacione los comandos Kickstart con sus descripciones en la tabla.

Descripción	Comando
Sección del archivo de configuración Kickstart que especifica qué software está instalado en el nuevo sistema.	**%packages**
Comando de Kickstart obligatorio que configura cómo los usuarios acceden al sistema.	**auth**
Ubicación del software usado por Kickstart para instalar un sistema.	**url**
Script en un archivo de configuración Kickstart que se ejecuta luego de que el software está instalado en un sistema.	**%post**
Comando Kickstart que especifica qué particiones deben borrarse antes de la instalación.	**clearpart**
Modifica qué servicios iniciarán de forma predeterminada en el arranque del sistema.	**services**
Define las credenciales de autenticación predeterminadas para el superusuario.	**rootpw**
Comando Kickstart que especifica el tamaño, el formato y el nombre de una partición de disco.	**part**
Comando Kickstart usado para especificar servidores NTP.	**timezone**

Descripción	Comando
Determina la configuración de red para la instalación y el sistema de destino.	**network**

Implementación de un nuevo sistema virtual con Kickstart

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Crear un archivo de configuración Kickstart con la utilidad **`system-config-kickstart`**.
- Modificar un archivo de configuración Kickstart existente con un editor de textos y revisar su sintaxis con **`ksvalidator`**.
- Publicar un archivo de configuración Kickstart para el instalador.
- Realizar una instalación Kickstart de red.

Pasos de instalación Kickstart

Se requiere un proceso ordenado para automatizar la instalación exitosa de Red Hat Enterprise Linux.

Se deben llevar a cabo tres pasos para la instalación de Kickstart:

1. Crear un archivo de configuración kickstart.
2. Publicar el archivo de configuración Kickstart para el instalador.
3. Arrancar Anaconda y apuntarlo al archivo de configuración Kickstart.

Creación de un archivo de configuración Kickstart

Hay dos maneras de crear un archivo de configuración Kickstart:

- Use la utilidad **`system-config-kickstart`**.
- Use un editor de textos.

La utilidad **`system-config-kickstart`** presenta una cantidad de cuadros de diálogo gráficos, toma entradas del usuario, y luego crea un archivo de texto con directivas Kickstart que corresponden a las elecciones del usuario. Cada cuadro de diálogo corresponde a la categoría de preguntas formuladas por el instalador de Red Hat, Anaconda. De forma opcional, un archivo de configuración existente se puede pasar como un argumento y **`system-config-kickstart`** lo usará para completar los valores de las opciones de configuración. El paquete *system-config-kickstart* provee **`system-config-kickstart`**.

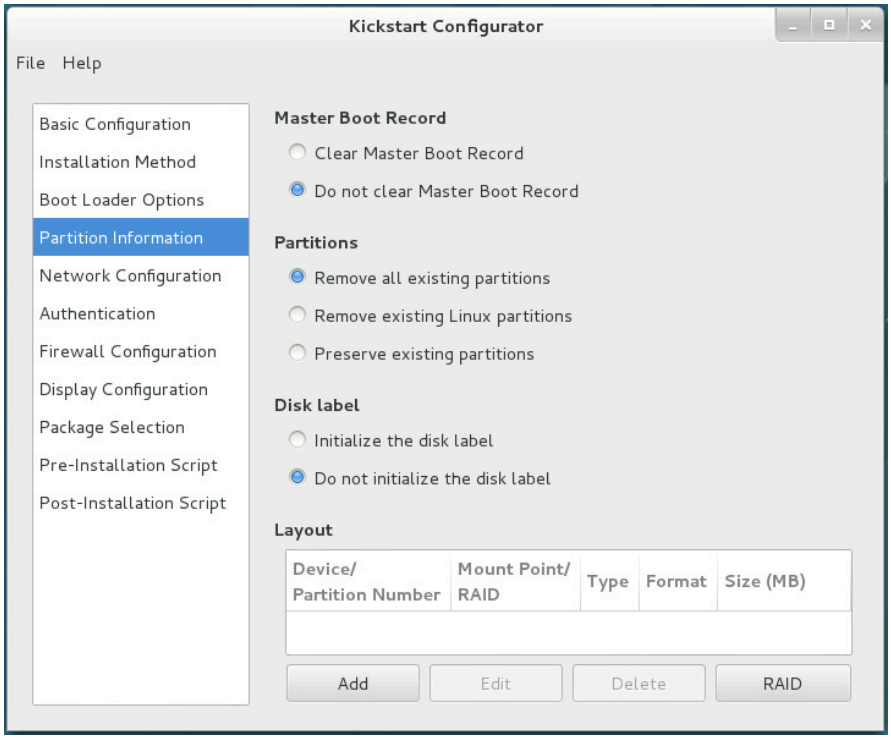

Figura 1.1: Configuración del almacenamiento con system-config-kickstart

La creación de un archivo de configuración Kickstart desde el arranque con un editor de texto es poco común. El instalador de Anaconda crea un archivo denominado **`/root/anaconda-ks.cfg`** que contiene las directivas Kickstart que se pueden usar para generar el sistema instalado recientemente. Este archivo crea un buen punto de inicio al crear un archivo de configuración Kickstart con un editor de textos.

A continuación, se detallan algunos motivos de la creación manual de un archivo Kickstart en lugar de usar **`system-config-kickstart`**:

1. La GUI o **`system-config-kickstart`** no está disponible.
2. Se necesitan instrucciones de configuración de partición de disco avanzadas. **`system-config-kickstart`** no admite LVM.
3. Se deben incluir u omitir paquetes individuales (no sólo grupos).
4. Se necesitan scripts más avanzados en las secciones **`%pre`** y **`%post`**.

`ksvalidator` es una utilidad que revisa errores de sintaxis en un archivo de configuración Kickstart. Asegurará que las palabras clave y las opciones se usen adecuadamente, pero no validará las rutas URL, los paquetes ni grupos individuales, ni ninguna parte de los scripts **`%post`** o **`%pre`**. Por ejemplo, si la directiva **`firewall --disabled`** está mal escrita, **`ksvalidator`** podría producir uno de los siguientes errores:

```
[student@desktopX]$ ksvalidator /tmp/anaconda-ks.cfg
The following problem occurred on line 10 of the kickstart file:

Unknown command: frewall
```

```
[student@desktopX]$ ksvalidator /tmp/anaconda-ks.cfg
The following problem occurred on line 10 of the kickstart file:

no such option: --dsabled
```

El RPM *pykickstart* proporciona **ksvalidator**.

Publicar el archivo de configuración Kickstart para Anaconda

Ponga el archivo de configuración Kickstart a disposición del instalador:

- Servidores de red: FTP, HTTP, NFS
- Servidor DHCP/TFTP
- Disco USB o CD-ROM
- Disco duro local

El instalador debe poder acceder al archivo Kickstart para iniciar una instalación automatizada. Si bien existen varios métodos para hacer que el archivo de configuración Kickstart esté disponible; el más común es a través de un servidor de red como un servidor FTP, un servidor web o un servidor NFS. Los servidores de red facilitan el mantenimiento del archivo Kickstart porque solo es necesario hacer cambios una vez y estos entran en efecto inmediatamente.

Proporcionar archivos Kickstart en USB o CD-ROM es otra manera conveniente de publicar archivos de configuración. El archivo de configuración Kickstart está incluido en los medios de arranque usados para iniciar la instalación. Cuando se realizan cambios, se deben generar nuevos medios de instalación.

Es posible proporcionar el archivo Kickstart en un disco local. Esto permite una manera rápida de volver a crear un servidor de implementación.

Arrancar Anaconda y apuntarlo al archivo de configuración Kickstart

Una vez elegido un método de Kickstart, se le debe indicar al instalador dónde está ubicado el archivo Kickstart. Esto se hace al pasar un argumento **ks=*LOCATION*** al kernel de instalación. Las siguientes son algunas especificaciones de muestra:

- ks=http://*server*/*dir*/*file*
- ks=ftp://*server*/*dir*/*file*
- ks=nfs:*server*:/*dir*/*file*
- ks=hd:*device*:/*dir*/*file*
- ks=cdrom:/*dir*/*file*

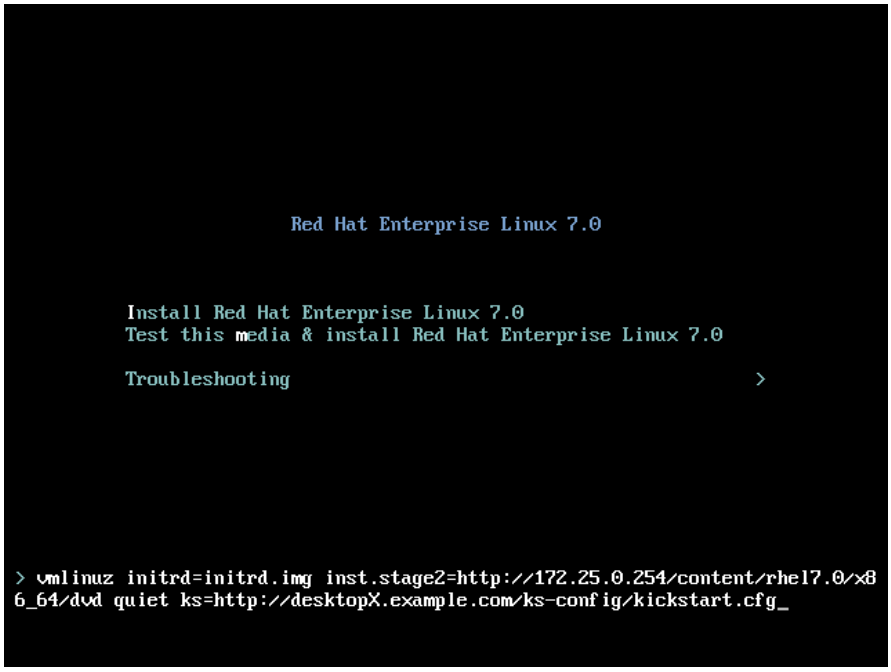

Figura 1.2: Especificación de la ubicación del archivo Kickstart durante el arranque PXE

En el caso de instalaciones en máquinas virtuales mediante el uso de **Virtual Machine Manager** o **`virt-manager`**, la URL Kickstart se puede especificar en un cuadro debajo de **URL Options** (Opciones de URL). Cuando realice una instalación en máquinas físicas, realice el arranque usando medios de instalación y presione la tecla de **`tabulación`** para interrumpir el proceso de arranque. Ingrese una de las entradas **`ks=`** de arriba como un parámetro para el kernel de instalación.

Nota

La función de selección de paquetes de la utilidad system-config-kickstart está actualmente deshabilitada debido al siguiente error (https://bugzilla.redhat.com/show_bug.cgi?id=1272068).

Referencias

Páginas del manual: **`ksvalidator`**(1), **`system-config-kickstart`**(8)

Práctica: Instalación de un sistema usando Kickstart

En este trabajo de laboratorio, creará un archivo de configuración Kickstart, confirmará que su sintaxis sea correcta y lo publicará para su uso.

Recursos	
Archivos:	/root/anaconda-ks.cfg
Máquinas:	**desktopX**

Resultados
Tendrá un archivo de configuración Kickstart basado en el archivo **anaconda-ks.cfg** en **desktopX**. Instalará paquetes desde **classroom.example.com**, usará DHCP para establecimiento de redes, particionará el almacenamiento e instalará paquetes según las especificaciones, y realizará una breve personalización del sistema recientemente instalado.

Andes de comenzar
- Restablezca su sistema **desktopX**.
- Inicie sesión en su sistema **desktopX** y configúrelo.

```
[student@desktopX ~]$ lab kickstart setup
```

1. Copie **/root/anaconda-ks.cfg** en **desktopX**, en un archivo denominado **kickstart.cfg** que **student** pueda editar.

```
[student@desktopX ~]$ sudo cat /root/anaconda-ks.cfg > kickstart.cfg
```

2. Haga los siguientes cambios en **kickstart.cfg**.

2.1. Cambie el comando **url** para especificar los medios de fuentes de instalación HTTP usados en el aula:

```
url --url="http://classroom.example.com/content/rhel7.0/x86_64/dvd/"
```

2.2. Configure la red para usar DHCP. Solo debe haber una única directiva de **red** que sea similar a la siguiente:

```
network --bootproto=dhcp
```

2.3. Modifique la configuración del disco para solo tener las siguientes tres directivas:

```
# Clear the Master Boot Record
zerombr
# Partition clearing information
clearpart --all --initlabel
# Disk partitioning information
```

```
part / --fstype="xfs" --ondisk=vda --size=5120
```

Asegúrese de que el tamaño se ajuste a 5120.

2.4. Comente la directiva **reiniciar**:

```
#reboot
```

2.5. Cambie los paquetes que están instalados para incluir **httpd**, pero no **cloud-init**. Simplifique la especificación del paquete para que se vea de la siguiente manera:

```
@core
chrony
dracut-config-generic
dracut-norescue
firewalld
grub2
kernel
rsync
tar
httpd
-plymouth
```

2.6. Elimine todo el contenido de la sección **%post**, excepto las siguientes líneas:

```
%post --erroronfail
# make sure firstboot doesn't start
echo "RUN_FIRSTBOOT=NO" > /etc/sysconfig/firstboot
# append /etc/issue with a custom message
echo "Kickstarted for class on $(date)" >> /etc/issue
%end
```

2.7. Establezca la contraseña **raíz** en **redhat**. Cambie la línea que comienza con **rootpw** por:

```
rootpw --plaintext redhat
```

3. Use el comando **ksvalidator** para comprobar si hay errores de sintaxis en el archivo Kickstart.

```
[student@desktopX ~]$ ksvalidator kickstart.cfg
```

4. Copie **kickstart.cfg** en el directorio **/var/www/html/ks-config**.

```
[student@desktopX ~]$ sudo cp ~student/kickstart.cfg /var/www/html/ks-config
```

5. Ejecute el script de clasificación **lab kickstart** en **desktopX** para confirmar que los cambios especificados se hayan hecho y que el archivo Kickstart esté disponible vía HTTP.

```
[root@desktopX ~]# lab kickstart grade
Kickstart file available via HTTP ..... PASS
Confirming installation media ......... PASS
```

```
Checking installed disk size .......... PASS
Confirming network configuration ...... PASS
Checking software package selection ... PASS
```

Evaluación del capítulo: Automatización de la instalación con Kickstart

A continuación, se indican los pasos para instalar un servidor Red Hat Enterprise Linux usando Kickstart. Indique el orden en que deben efectuarse los pasos.

__ a. Verifique el archivo de configuración para ver si hay errores de sintaxis con **`ksvalidator`**.

__ b. Arranque Anaconda desde un medio de instalación.

__ c. Use un editor de textos para agregar comandos de administración de volúmenes lógicos al archivo de configuración de Kickstart.

__ d. Especifique la opción **`ks=`** para apuntar el instalador al archivo de configuración de Kickstart.

__ e. Use **`system-config-kickstart`** para crear un archivo de configuración de Kickstart.

__ f. Publique el archivo de configuración de Kickstart vía HTTP, FTP o NFS.

Solución

A continuación, se indican los pasos para instalar un servidor Red Hat Enterprise Linux usando Kickstart. Indique el orden en que deben efectuarse los pasos.

3 a. Verifique el archivo de configuración para ver si hay errores de sintaxis con **`ksvalidator`**.

5 b. Arranque Anaconda desde un medio de instalación.

2 c. Use un editor de textos para agregar comandos de administración de volúmenes lógicos al archivo de configuración de Kickstart.

6 d. Especifique la opción **`ks=`** para apuntar el instalador al archivo de configuración de Kickstart.

1 e. Use **`system-config-kickstart`** para crear un archivo de configuración de Kickstart.

4 f. Publique el archivo de configuración de Kickstart vía HTTP, FTP o NFS.

Resumen

Definición del sistema Anaconda Kickstart

- Kickstart automatiza la instalación de Red Hat Enterprise Linux usando un archivo de texto.
- Los archivos de configuración Kickstart se inician con comandos, seguidos de la sección **`%packages`**.
- Las secciones **`%post`** y **`%pre`** opcionales pueden contener scripts que personalizan las instalaciones.

Implementación de un nuevo sistema virtual con Kickstart

- La utilidad **`system-config-kickstart`** se puede usar para crear un archivo de configuración Kickstart.
- Otra forma de crear un archivo de configuración Kickstart es usar un editor de textos y el comando **`ksvalidator`** para verificar errores de sintaxis.
- La opción **`ks=`*`ksfile-location`*** para el kernel de Anaconda especifica dónde encontrar el archivo de configuración Kickstart.

redhat. TRAINING

CAPÍTULO 2

USO DE EXPRESIONES REGULARES CON GREP

Descripción general	
Meta	Escribir expresiones regulares mediante el uso de **grep** para aislar o localizar contenido en archivos de texto.
Objetivos	• Crear expresiones regulares que coincidan con patrones de texto. • Usar **grep** para localizar contenido en archivos.
Secciones	• Aspectos básicos de expresiones regulares (y práctica) • Búsqueda de texto con grep (y práctica) • Uso de **grep** con registros (y práctica)
Trabajo de laboratorio	• Uso de expresiones regulares con **grep**

Aspectos básicos de expresiones regulares

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Crear expresiones regulares que correspondan a los datos deseados.
- Usar **grep** para aplicar expresiones regulares a archivos de texto.

Escritura de expresiones regulares

Las expresiones regulares son un lenguaje que se corresponde con patrones, usado para habilitar las aplicaciones para que examinen datos en busca de contenido específico. Además de **vim**, **grep** y **less** que usan expresiones regulares, los lenguajes de programación, como Perl, Python y C usan expresiones regulares cuando usan criterios que corresponden a patrones.

Las expresiones regulares son un lenguaje en sí mismas, lo que significa que tienen su propia sintaxis y reglas. En esta sección, se dará un vistazo a la sintaxis usada en la creación de expresiones regulares y se mostrarán algunos ejemplos del uso de expresiones regulares.

Una expresión regular simple

La expresión regular más simple es una correspondencia exacta. Una correspondencia exacta es cuando los caracteres de la expresión regular coinciden con el tipo y el orden de los datos que se están buscando.

Supongamos que un usuario estaba explorando el siguiente archivo de datos en busca de todas las veces que aparece el patrón **cat**:

```
cat
dog
concatenate
dogma
category
educated
boondoggle
vindication
chilidog
```

cat es una correspondencia exacta de una **c**, seguida de una **a**, seguida de una **t**. El uso de **cat** como expresión regular mientras busca el archivo anterior, arroja las siguientes coincidencias:

```
cat
con cat enate
cat egory
edu cat ed
vindi cat ion
```

Uso de delimitadores de línea

En la sección anterior, se usó una expresión regular de correspondencia exacta en un archivo de datos. Observe que la expresión regular coincidiría con los datos sin importar en qué

parte de la línea se encuentren: al principio, al final o en el medio de la palabra o línea. Una de las maneras para controlar la ubicación donde la expresión regular busca una coincidencia es un *delimitador de línea*.

Use un **^**, un inicio de un delimitador de línea, o **$**, un final de un delimitador de línea. Uso del archivo anterior:

```
cat
dog
concatenate
dogma
category
educated
boondoggle
vindication
chilidog
```

Para que la expresión regular coincida con **cat**, pero solo si ocurre al inicio de la línea en el archivo, use **^cat**. Si se aplica la expresión regular **^cat** para los datos, se arrojarán las siguientes correspondencias:

```
cat
category
```

Si los usuarios solo deseaban localizar las líneas del archivo que terminaban con dog, use esa expresión exacta y un delimitador de final de línea para crear la expresión regular **dog$**. Si se aplica **dog$** al archivo, se arrojarán dos coincidencias:

```
dog
chilidog
```

Si los usuarios deseaban asegurarse de que el patrón fuera lo único en una línea, use ambos delimitadores, de inicio y de final de la línea. **^cat$** localizaría solo una línea en el archivo, una con un inicio de línea, una **c**, seguida de una **a**, seguida de una **t**, y con un final del línea.

Otro tipo de delimitador de línea es la *delimitación de palabras*. **\<** y **\>** se pueden usar para hacer coincidir respectivamente el principio y el final de una palabra.

Comodines y multiplicadores

Las expresiones regulares usan un **.** como carácter comodín sin restricciones. Una expresión regular de **c.t** buscará datos que contengan una **c**, seguida de cualquier carácter, seguido de una **t**. Los ejemplos de datos que coincidirían con este patrón de expresión regular son cat, cot y cut, pero también c5t y cQt.

Otro tipo de comodín usado en expresiones regulares es un conjunto de caracteres aceptables en una posición de carácter específica. Al usar un comodín sin restricciones, los usuarios no podrían predecir el carácter que coincidiría con el comodín; sin embargo, si los usuarios desearan solo buscar las palabras cat, cot y cut, pero no elementos como c5t o cQt, se debe reemplazar el comodín sin restricciones con uno donde se especifiquen caracteres aceptables. Si la expresión regular se modificó a **c[aou]t**, especificaría que la expresión regular debe coincidir con patrones que comiencen con una **c**, seguidas de una **a** o una **o** o una **u**, seguidas de una **t**.

Los multiplicadores son un mecanismo usado a menudo con comodines. Los multiplicadores se aplican al carácter anterior en la expresión regular. Uno de los multiplicadores más comunes usados es **`*`**. Un **`*`**, cuando se usa en una expresión regular, modifica el carácter anterior para que signifique cero hasta infinitamente muchos caracteres de esos. Si se usó una expresión regular de **`c.*t`**, coincidiría con ct, cat, coat, culvert, etc. todos los datos que comiencen con una **c**, luego desde cero hasta infinitamente muchos caracteres, y que finalicen con una **`t`**.

Otro tipo de multiplicador indicaría la cantidad de caracteres anteriores deseados en el patrón. Un ejemplo del uso de un multiplicador explícito sería **`c.\\{2\\}t`**. Al usar esta expresión regular, los usuarios buscan datos que comiencen con una **c**, seguida de exactamente dos caracteres cualesquiera, y que finalice con una **`t`**.

nota

En el ejemplo anterior, se usó la sintaxis Bash regex. Hay algunas pequeñas diferencias en la sintaxis usada para expresiones regulares entre diferentes implementaciones (Bash, Python, Perl, etc.)

Referencias

Página del manual **`regex`**(7).

Práctica: Relacionar la expresión regular

Relacione las siguientes palabras con la expresión regular a la que cada una corresponde de forma única en la tabla.

Error	Instalado	^Au.*U	^i	error	s$

Palabra o frase	Expresión regular
Aug 19 13:45:41 Updated: lvm2-libs-2.02.95-10.el6_3.3.x86_64	
Aug 19 17:33:15 Installed: wireshark-gnome-1.2.15-2.el6_2.1.x86_64	
io scheduler deadline registered	
Jan 27 10:38:47 serverX NetworkManager[2179]: ifcfg-wlan: error: Missing SSID	
Jan 25 16:02:46 serverX pulseaudio[30014]: main.c: Unable to contact D-Bus: org.freedesktop.DBus.Error.NoServer: Connection refused	
Jan 27 10:39:57 serverX ntpd[2464]: time reset -0.252602 s	

Solución

Relacione las siguientes palabras con la expresión regular a la que cada una corresponde de forma única en la tabla.

Palabra o frase	Expresión regular
Aug 19 13:45:41 Updated: lvm2-libs-2.02.95-10.el6_3.3.x86_64	^Au.*U
Aug 19 17:33:15 Installed: wireshark-gnome-1.2.15-2.el6_2.1.x86_64	Instalado
io scheduler deadline registered	^i
Jan 27 10:38:47 serverX NetworkManager[2179]: ifcfg-wlan: error: Missing SSID	error
Jan 25 16:02:46 serverX pulseaudio[30014]: main.c: Unable to contact D-Bus: org.freedesktop.DBus.Error.NoServer: Connection refused	Error
Jan 27 10:39:57 serverX ntpd[2464]: time reset -0.252602 s	s$

Búsqueda de texto con grep

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Usar el comando **grep** con opciones comunes.
- Usar **grep** para buscar archivos y datos de comandos canalizados.

Uso de grep

grep es un comando proporcionado como parte de la distribución que utiliza expresiones regulares para aislar los datos correspondientes.

Uso de grep

El uso básico de grep es proporcionar una expresión regular y un archivo con el cual la expresión regular debe coincidir.

```
[student@serverX ~]$ grep 'cat$' /usr/share/dict/words
```

nota

Debido a que las expresiones regulares a menudo contienen metacaracteres de shell (como $, * y otros), se recomienda usar comillas simples (**'**) para encapsular la expresión regular en la línea de comandos.

grep se puede usar junto con otros comandos mediante el uso de **|**.

```
[root@serverX ~]# ps aux | grep '^student'
```

grep opciones

grep tiene muchas opciones útiles para ajustar cómo usa la expresión regular con datos.

Opción	Función
-i	Usa la expresión regular proporcionada; sin embargo, no detecta diferencias entre mayúsculas y minúsculas.
-v	Solo muestra líneas que NO contienen coincidencias con la expresión regular.
-r	Aplica la búsqueda de datos que coincidan con la expresión regular de forma recursiva para un grupo de archivos o directorios.
-A <NUMBER>	Muestra <NUMBER> (número) de líneas luego de la coincidencia de la expresión regular.
-B <NUMBER>	Muestra <NUMBER> (número) de líneas antes de la coincidencia de la expresión regular.

Opción	Función
-e	Si se usan varias opciones -e, se pueden suministrar varias expresiones regulares y se usarán con un "or" lógico.

Hay muchas más opciones para **grep** también, pero estas son algunas de las que se usan frecuentemente.

Ejemplos de grep

Para los siguientes ejemplos, use el siguiente contenido de archivos, almacenado en un archivo denominado **dogs-n-cats**.

```
[student@serverX ~]$ cat dogs-n-cats
# This file contains words with cats and dogs
Cat
dog
concatenate
dogma
category
educated
boondoggle
vindication
Chilidog
```

Las expresiones regulares distinguen entre mayúsculas y minúsculas de forma predeterminada; el uso de la opción **-i** con grep hará que la expresión regular no distinga entre mayúsculas y minúsculas.

```
[student@serverX ~]$ grep -i 'cat' dogs-n-cats
# This file contains words with cats and dogs
Cat
concatenate
category
educated
vindication
```

A veces, los usuarios saben lo que no están buscando en vez de lo que están buscando. En esos casos, el uso de **-v** es bastante útil. En el siguiente ejemplo, se muestran todas las líneas, sin distinguir entre mayúsculas y minúsculas, que no contienen la expresión regular "cat".

```
[student@serverX ~]$ grep -i -v 'cat' dogs-n-cats
dog
dogma
boondoggle
Chilidog
```

Otro ejemplo práctico del uso de **-v** es necesitar ver un archivo, pero no desear distraerse con contenido de comentarios. En el siguiente ejemplo, la expresión regular buscará todas las líneas que comiencen con un # o ; (caracteres típicos que indican que la línea será interpretada como un comentario).

```
[student@serverX ~]$ grep -v '^[#;]' <FILENAME>
```

Hay veces en que los usuarios deben buscar líneas que contienen información tan diferente que los usuarios no pueden crear simplemente una expresión regular para hallar todos los datos. **grep** proporciona la opción **-e** para estas situaciones. En el siguiente ejemplo, los usuarios localizarán todas las apariciones de "cat" o "dog".

```
[student@serverX ~]$ grep -e 'cat' -e 'dog' dogs-n-cats
# This file contains words with cats and dogs
dog
concatenate
dogma
category
educated
boondoggle
vindication
Chilidog
```

Referencias

Página del manual (1)**grep**

Práctica: Uso de grep con registros

En este trabajo de laboratorio, usará expresiones regulares y **grep** para localizar entradas de registros específicos en archivos de registros.

Recursos:	
Archivos:	/var/log/messages
Máquinas:	serverX

Resultados:
Mediante el uso de expresiones regulares y el comando **grep**, puede aislar mensajes o grupos de mensajes específicos en función de los criterios de búsqueda proporcionados.

Andes de comenzar
- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo.

```
[student@serverX ~]$ lab grep setup
```

1. Eleve sus privilegios para obtener un inicio de sesión de raíz usando **su -**.

   1.1.
   ```
   [student@serverX ~]$ su -
   ```

2. Elabore una expresión regular y use **grep** para mostrar todos los registros en **/var/log/messages** desde la **Hora de inicio** informada por **lab grep setup**.

   2.1. Los siguientes comandos asumen una hora de inicio proporcionada por el script **lab grep** del 1 de abril a las 15:53.

   Compruebe la hora actual de modo que sepamos no solo la hora de inicio, sino también la hora de finalización de los mensajes que estamos buscando.

   ```
   [root@serverX ~]# date
   Tue Apr  1 15:54:55 EDT 2014
   ```

   2.2.
   ```
   [root@serverX ~]# grep '^Apr 1 15:5[34]' /var/log/messages
   Apr  1 15:53:25 serverX ima_daemon[14847]: logging ACCESS:
    927265f3c0e95f4ae6294451060d0717
   Apr  1 15:53:25 serverX ima_daemon[14848]: logging ACCESS:
    b4866e8f2ec0058abe1dc0a142e0b737
   Apr  1 15:53:25 serverX ima_daemon[14849]: logging ACCESS:
    7afa51b31aabca065dd358cc475d8863
   ... Output Truncated ...
   ```

3. Modifique su expresión regular para localizar el primer mensaje de **ERROR**.

   3.1.
   ```
   [root@serverX ~]# grep '^Apr 1 15:5[34].*ERROR' /var/log/messages | head -n 1
   ```

```
Apr  1 15:53:30 serverX database[14877]: bad entry ERROR:
 2e28564860d5c6e5151a31fd923c7b61 invalid
```

4. Los mensajes de registros son generados por aplicaciones. No hay un estándar adoptado sobre qué palabras clave o información deben proporcionarse como parte de un mensaje de registro.

   Mediante el uso de una opción para **grep**, busque todos los registros luego de la hora de inicio que contengan la palabra **ERROR**, y que ignoren la diferencia entre mayúsculas y minúsculas de la expresión regular.

   4.1.
   ```
   [root@serverX ~]# grep -i '^Apr 1 15:5[34].*ERROR' /var/log/messages
   ```

5. Use la opción **-v** con **grep**, así como una expresión regular, para localizar el mensaje de **ERROR** que no contenga una suma de verificación en el cuerpo del mensaje.

   5.1. En esta situación, puede resultar útil usar un grep y una expresión regular para cumplir con algunos de los criterios, y otro para filtrar aún más los resultados para obtener el contenido deseado.

   ```
   [root@serverX ~]# grep '^Apr 1 15:5[34].*ERROR' /var/log/messages | grep -v '[a-
   z0-9]\{32\}'
   ```

Trabajo de laboratorio: Uso de expresiones regulares con grep

En este trabajo de laboratorio, usará expresiones regulares y **grep** con archivos de texto para localizar los datos solicitados.

Recursos:	
Archivos:	`http://classroom.example.com/pub/materials/awesome_logs`
Máquinas:	serverX

Resultados:
Siga las pistas y ayude al Dr. Zingruber a recuperar la "obra de arte" perdida.

Dr. Zingruber: "¡Hola! Me dijeron que usted es la persona con la que debo hablar sobre la ayuda para la administración de sistemas de Red Hat Enterprise Linux."

Sí, soy yo.

Dr. Zingruber: "Entonces, tal vez pueda ayudarme; es mi última esperanza. Ha ocurrido algo terrible. Ha habido un robo en el Museo de Awesome."

¿Qué robaron?

Dr. Zingruber: "Una obra de Wander van Gogh".

¿Wander van Gogh? Nunca oí hablar de él.

Dr. Zingruber: "No me sorprende. Es un descendiente de Vincent van Gogh, pero es mucho, MUCHO, más demente. Esta es una de las piezas más importantes; por eso la tenemos en el Museo de Awesome."

Veo. ¿Cuándo fue robada la pieza?

Dr. Zingruber: "Fue el **`8 de agosto, en algún momento entre la 1:00 p. m. y las 3:00 p. m`**."

Espere, ¿cómo? ¿Fue robada el 8 de agosto y recién ahora está investigando el caso?

Dr. Zingruber: "Sí, bueno, para ser honesto, nadie había notado que faltaba hasta ahora. Verá, mientras la pieza estaba en el Museo de Awesome, estaba en el Hall of Mildly Awesome. Si visita el Museo de Awesome, ¿se dirige al Hall of Mildly Awesome o a la Cavern of Supreme Awesome? Debido a su ubicación, nadie la mira y, entre nosotros, me da miedo."

Um... Okay. Entonces, ¿qué más puede decirme sobre el robo?

Dr. Zingruber: "Bueno, tenemos una variedad de registros de diferentes cosas. Puede descargarlos desde **`http://classroom.example.com/pub/materials/awesome_logs`**. Creo que debería empezar la investigación **`door.log`** cerca de la hora del hecho."

Andes de comenzar
- Restablezca su sistema **`serverX`**.

1. Descargue los registros en su máquina, y cambie el directorio al directorio de registros.

2. Use **`grep`** para buscar en **`door.log`**. Siga las demás instrucciones que pueda hallar en los registros.

Solución

En este trabajo de laboratorio, usará expresiones regulares y **grep** con archivos de texto para localizar los datos solicitados.

Recursos:	
Archivos:	**http://classroom.example.com/pub/materials/awesome_logs**
Máquinas:	serverX

Resultados:
Siga las pistas y ayude al Dr. Zingruber a recuperar la "obra de arte" perdida.

Dr. Zingruber: "¡Hola! Me dijeron que usted es la persona con la que debo hablar sobre la ayuda para la administración de sistemas de Red Hat Enterprise Linux."

Sí, soy yo.

Dr. Zingruber: "Entonces, tal vez pueda ayudarme; es mi última esperanza. Ha ocurrido algo terrible. Ha habido un robo en el Museo de Awesome."

¿Qué robaron?

Dr. Zingruber: "Una obra de Wander van Gogh".

¿Wander van Gogh? Nunca oí hablar de él.

Dr. Zingruber: "No me sorprende. Es un descendiente de Vincent van Gogh, pero es mucho, MUCHO, más demente. Esta es una de las piezas más importantes; por eso la tenemos en el Museo de Awesome."

Veo. ¿Cuándo fue robada la pieza?

Dr. Zingruber: "Fue el **8 de agosto, en algún momento entre la 1:00 p. m. y las 3:00 p. m**."

Espere, ¿cómo? ¿Fue robada el 8 de agosto y recién ahora está investigando el caso?

Dr. Zingruber: "Sí, bueno, para ser honesto, nadie había notado que faltaba hasta ahora. Verá, mientras la pieza estaba en el Museo de Awesome, estaba en el Hall of Mildly Awesome. Si visita el Museo de Awesome, ¿se dirige al Hall of Mildly Awesome o a la Cavern of Supreme Awesome? Debido a su ubicación, nadie la mira y, entre nosotros, me da miedo."

Um... Okay. Entonces, ¿qué más puede decirme sobre el robo?

Dr. Zingruber: "Bueno, tenemos una variedad de registros de diferentes cosas. Puede descargarlos desde **http://classroom.example.com/pub/materials/awesome_logs**. Creo que debería empezar la investigación **door.log** cerca de la hora del hecho."

Andes de comenzar
- Restablezca su sistema **serverX**.

1. Descargue los registros en su máquina, y cambie el directorio al directorio de registros.

```
[root@serverX ~]# wget -r -l 1 -np http://classroom.example.com/pub/materials/
awesome_logs
[root@serverX ~]# cd classroom.example.com/pub/materials/awesome_logs
```

2. Use **grep** para buscar en **door.log**. Siga las demás instrucciones que pueda hallar en los registros.

   El Dr. Zingruber observó que el robo ocurrió entre la 1:00 p. m. y las 3:00 p. m., o bien, en el formato de 24 horas (usado en los registros), entre las 13:00 y las 15:00. Nuestra expresión regular debe usar el campo de la fecha y hora del momento para obtener entradas relevantes.

```
[root@serverX awesome_logs]# grep '^Aug *8 1[345]' door.log
```

   Observe que hay DOS caracteres de espacio entre **Aug** (agosto) y **8** en el formato de fecha del archivo de registro. Para abordar esto, puede usar dos espacios en su expresión regular o un multiplicador en el carácter de espacio. Es posible que deba buscar entre los datos encontrados para hallar lo que está buscando. Si no puede, intente lo siguiente:

```
[root@serverX awesome_logs]# grep '^Aug *8 14.*OPEN' door.log
... Output Truncated ...
Aug  8 14:37:03 alarm_monitor activity: back door: OPEN Dr Zingruber: "Oh yes...
Aug  8 14:40:01 alarm_monitor activity: back door: OPEN look here, you can see
Aug  8 14:41:26 alarm_monitor activity: back door: OPEN the door stayed open.
Aug  8 14:43:55 alarm_monitor activity: back door: OPEN Now that we know a more
Aug  8 14:46:20 alarm_monitor activity: back door: OPEN exact time, we should
Aug  8 14:48:31 alarm_monitor activity: back door: OPEN check wall.log for the
Aug  8 14:51:30 alarm_monitor activity: back door: OPEN same period.
... Output Truncated ...
```

   En las entradas de **door.log**, nos derivaron al archivo **wall.log**, pero ahora tenemos un tiempo más acotado. Use **grep** para mirar entre los códigos de tiempo 14:37 y 14:51.

```
[root@serverX awesome_logs]# grep '^Aug *8 14:[345]' wall.log
```

   Observe que, una vez más, hay DOS caracteres de espacio entre **Aug** (agosto) y **8** en el formato de fecha del archivo de registro. Para abordar esto, puede usar dos espacios en su expresión regular o un multiplicador en el carácter de espacio. Es posible que deba buscar entre los datos encontrados para hallar lo que está buscando. Si no puede, intente lo siguiente:

```
[root@serverX awesome_logs]# grep '^Aug *8 14.*ALERT' wall.log
Aug  8 14:37:03 alarm_monitor ALERT: Mildly Awesome: Dr. Zingruber: Ah, yes here
Aug  8 14:40:01 alarm_monitor ALERT: Mildly Awesome: it is, looks like they
Aug  8 14:41:26 alarm_monitor ALERT: Mildly Awesome: digitized the image. We
Aug  8 14:43:55 alarm_monitor ALERT: Mildly Awesome: should check proxy.log at
Aug  8 14:46:20 alarm_monitor ALERT: Mildly Awesome: 14:40.  The digitalized
Aug  8 14:48:31 alarm_monitor ALERT: Mildly Awesome: image will be on the 24
Aug  8 14:51:30 alarm_monitor ALERT: Mildly Awesome: lines following the log.
```

   En las entradas de **wall.log**, nos derivaron al archivo **proxy.log**, pero ahora tenemos un tiempo exacto. Use **grep** para mirar entre el código de tiempo 14:40. Además, no solo deseamos la línea del código de tiempo 14:40, sino además las 24 líneas que siguen a esta entrada de registro.

```
[root@serverX awesome_logs]# grep -A 24 '14:40' proxy.log
```

Ahora debe haber recuperado la "obra de arte".

```
Aug  8 14:40:03 Outbound data Captured...Dr. Zingruber: You found it, thank you!
.............................MMMMMMMMMMMMMN~.............................
...........................:MMMMMMMMMMMMMMMMMM?...........................
.........................DMMMMMMN88MMMMNZZZZMMMMMMMN.....................
.......................+MMMMMMMZZZZZZZZZZZMM8ZMMMMMMM?...................
.....................MMMMMMMMZZZZZZZZZZZZZZZZZMMMMMMMM..................
.................. MMMMMMMMMZOMMMMMMZZZZZZZZZZMMMMMMMM ................
................. MMMMMMMMMOZZZNZZZZZZZZZZZZZZMMMMMMMMM ...............
.................MMMMMMDDDNMZZZZZZZZZZZZZZZZZZZMMMMMMMM...............
.................+MMM$ZZZZZ8MMMZZZZZZZZZZZZZZZZZZMMMMMMMM~.............
.................MMMMZZZZZZZDMMMMMMMNZZZZZZZZZZZNZ8MMMMMMM.............
.................MMMMOZZZZZZZZZMMMMMMMZZZZZZZZZZZZZZZZDMMMM.............
.................,MMMMMMZZZZZZZZZZZZMMMMZZZZZZZZZZZZZZZZZMMMZ............
.................DMMMMMMMMZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZMMMD............
.................ZMMMMMMMMMMDZZZZZZZZZZZZZZZZZZZZZZZZZZZZMMMMN............
.................,MMMMMMMMN..:MNZZZZZZZZZZZZZZZZZZZZZZZZMMMMM7............
.................. MMMMMMMM?... M,MMMZZZZZZZZZZZZZZZZZMMMMMMM ............
.................MMMMMN7MMI..... MMMMMMMMNNNNNMMMMMMMMMMM.................
...................    ....7MM ..... IDZ=..$, =I MMMMMMMMM.................
.....................................................MMMMMMMMM.................
.....................................IMMM,...NMMMMMMMM Z88.................
.................................................MMN......... ...............
.............................................IMD.............................
.......................................... $M.............................
................................................................................
```

Resumen

Aspectos básicos de expresiones regulares
Escriba expresiones regulares que correspondan a los datos.

Búsqueda de texto con `grep`
Uso de **`grep`** con expresiones regulares para aislar datos de texto.

redhat. TRAINING

CAPÍTULO 3

CREACIÓN Y EDICIÓN DE ARCHIVOS DE TEXTO CON VIM

Descripción general	
Meta	Presentar el editor de textos `vim`.
Objetivos	• Explicar los tres modos principales de `vim`. • Abrir, editar y guardar archivos de texto. • Usar atajos del editor.
Secciones	• Editor de textos vim (y práctica) • Flujo de trabajo básico de vim (y práctica) • Edición con vim (y práctica)
Trabajo de laboratorio	• Edición de un archivo de sistema con vim

El editor de textos de vim

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Explicar los tres modos principales de **vim**.

Introducción a vim

La edición de archivos de texto es una de las tareas más comunes que un administrador de sistemas realizará en un sistema Linux. Debido a esto, hay una amplia variedad de editores de texto disponible. Uno de los editores más antiguos, pero más usado es **vi**. **vi** significa *Visual Interface (interfaz visual),* dado que fue uno de los primeros editores de texto en mostrar realmente el documento en el que se trabajaba mientras se estaba editando. Antes de eso, la mayoría de los editores se basaba en líneas (como **ed**, y el todavía muy usado **ex**). En el uso regular, **vi** y **vim** se denominan normalmente *v.i.* (dos letras) y *vim*.

VI mejorado

La versión de **vi** que se incluye con Red Hat Enterprise Linux 7 se denomina **vim**. **vim** significa *VI IMproved (VI mejorado),*dado que **vim** incluye muchas funciones que no se encuentran en **vi** original, mientras aún sigue siendo (mayormente) compatible con las versiones anteriores. Entre las nuevas funciones, se encuentran opciones populares como resaltado de la sintaxis, modos de finalización y revisión de la ortografía.

vim tiene una gran capacidad de ampliación. Admite script en varios idiomas, complementos (plug-ins) de tipos de archivos, diferentes modos de finalización de texto y muchas otras opciones. Se puede adaptar a casi cualquier rol; y se lo ha adaptado. Hay extensiones y macros disponibles en Internet para casi cualquier propósito, desde ayudar a editar un determinado tipo de archivo (como DocBook), finalización más introspección para casi todos los idiomas de programación existentes, hasta tareas más mundanas como administrar listas de tareas pendientes.

Importante

Cuando un usuario sin privilegios invoca el comando **vi** en una máquina Red Hat Enterprise Linux 7, el comando que se ejecuta será **vim**. Esto se realiza con un alias que se configura desde **/etc/profile.d/vim.sh** cuando se inicia la shell.

Este alias *no* se establece para usuarios con un UID menor o igual a **200**. Estos usuarios ejecutarán **vi**, que es **vim** en modo compatible de **vi**. Esto significa que todas las funciones no halladas en el **vi** clásico se deshabilitarán.

Se recomienda siempre ejecutar el comando **vim** cada vez que se deseen las funciones más nuevas, y no contar con un alias que podría no estar disponible. Esto se recomienda especialmente cuando los usuarios también tienen que trabajar como **raíz**.

¿Por qué aprender **vim**?

Cada administrador de sistemas tendrá una preferencia por un editor de textos. Algunos preferirán **gedit**, otros, **nano**, e incluso hay personas que prefieren **emacs**. Incluso si la persona ya tiene un editor preferido, es importante estar familiarizado con los conceptos básicos de **vim** o **vi** por un simple motivo: es el editor con el que se puede contar para instalar en cualquier sistema en el que se esté trabajando.

Diferentes versiones de **vim**

Se pueden instalar tres variaciones distintas de **vim** en un sistema Red Hat Enterprise Linux. Cada versión tiene su propio caso de uso y las variaciones se pueden instalar en forma paralela. Las variaciones vienen en estos tres paquetes:

- *vim-minimal*: Este paquete solo proporciona **vi** y comandos relacionados (como **rvi**, la versión restringida que no puede iniciar comandos ni una shell). Esta es la versión incluida en una instalación mínima de Red Hat Enterprise Linux 7.
- *vim-enhanced*: Este paquete proporciona el comando **vim** (y amigos), que proporciona funciones como resaltado de sintaxis, complementos (plug-ins) de tipos de archivo y revisión de la ortografía.
- *vim-X11*: Este paquete proporciona **gvim**, una versión de **vim** que se ejecuta en su propia ventana gráfica en lugar de hacerlo en una terminal. Una de las principales funciones de **gvim** es la barra de menú, útil cuando el usuario está aprendiendo **vim** o no recuerda un comando específico. (Nota: Según el tipo de terminal y la configuración por usuario de **vim**, puede que también sea posible usar un mouse dentro de una sesión de **vim** regular).

Un editor modal

vim no es el editor más fácil de aprender. Esto se debe, en parte, a que todos los comandos de **vim** están adaptados para mejorar la velocidad y la eficiencia, y no es fácil recordarlos; y, en parte, a que **vim** es un *editor* editor. *Un editor modal* significa que la función de determinados comandos y secuencia de teclas cambia en función del modo que esté activo.

vim tiene tres modos principales:

Función	Modo
Command modo	Este modo se usa para la exploración de archivos, copiar y pegar, y ejecutar comandos simples. Con este modo, también se realizan funciones como deshacer, rehacer y otras.
Modo **insertar**	Este modo se usa para la edición de texto normal. El modo **reemplazar** es una variación del modo **insertar** que reemplaza texto en lugar de insertarlo.
Modo **ex**	Este modo se usa para guardar, cerrar y abrir archivos, así como también para buscar y reemplazar, y otras operaciones más complejas. Desde este modo, es posible insertar el resultado de programas en el archivo actual, configurar **vim** y mucho más. Todo lo que es posible usando **ex** se puede hacer desde este modo.

Referencias

Página del manual (1)**`vim`**

`vim` ayuda incluida

Práctica: Modos vim

Relacione los siguientes elementos con sus partes correspondientes en la tabla.

Modo **`comando`**	Modo **`ex`**	Modo **`insertar`**

Función	**Modo**
Este modo se usa para la exploración de archivos, copiar y pegar, y ejecutar comandos simples.	
Este modo se usa para la edición de texto normal.	
Este modo se usa para guardar, cerrar y abrir archivos, así como también para buscar y reemplazar, y otras operaciones más complejas.	

Solución

Relacione los siguientes elementos con sus partes correspondientes en la tabla.

Función	Modo
Este modo se usa para la exploración de archivos, copiar y pegar, y ejecutar comandos simples.	Modo **`comando`**
Este modo se usa para la edición de texto normal.	Modo **`insertar`**
Este modo se usa para guardar, cerrar y abrir archivos, así como también para buscar y reemplazar, y otras operaciones más complejas.	Modo **`ex`**

Flujo de trabajo básico de **vim**

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Abrir archivos de texto.
- Mover el cursor.
- Insertar y reemplazar texto.
- Guardar archivos.
- Obtener ayuda.

Conceptos básicos del editor

No importa qué editor use, siempre debe poder realizar las siguientes tres tareas:

- Abrir un archivo nuevo o existente.
- Hacer cambios o insertar texto nuevo.
- Guardar el archivo y salir del editor.

Apertura de archivos

La manera más fácil de abrir un archivo en **vim** es especificarlo como un argumento en la línea de comandos. Por ejemplo, para abrir el archivo denominado **/etc/hosts**, debe poder ejecutar el siguiente comando:

```
[root@serverX ~]# vim /etc/hosts
```

nota

Si intenta abrir un archivo que no existe, pero el directorio que especifica está disponible, **vim** le informará que está editando un **[archivo nuevo]**, y creará el archivo cuando lo guarde por primera vez.

Luego de abrir un archivo, **vim** se iniciará en modo *comando*. En la parte inferior izquierda de la pantalla, verá información sobre el archivo abierto (nombre del archivo, cantidad de líneas, cantidad de caracteres). En la parte inferior derecha, observará la posición del cursor actual (línea, carácter) y qué parte de este archivo se está mostrando (**All** ([Todo] para todo, **Top** [Superior] para las primeras líneas de un archivo, **Bot** [Inferior] para la parte inferior de un archivo o un porcentaje para indicar en qué parte del archivo está). La línea inferior se denomina *regla* en términos de **vim**.

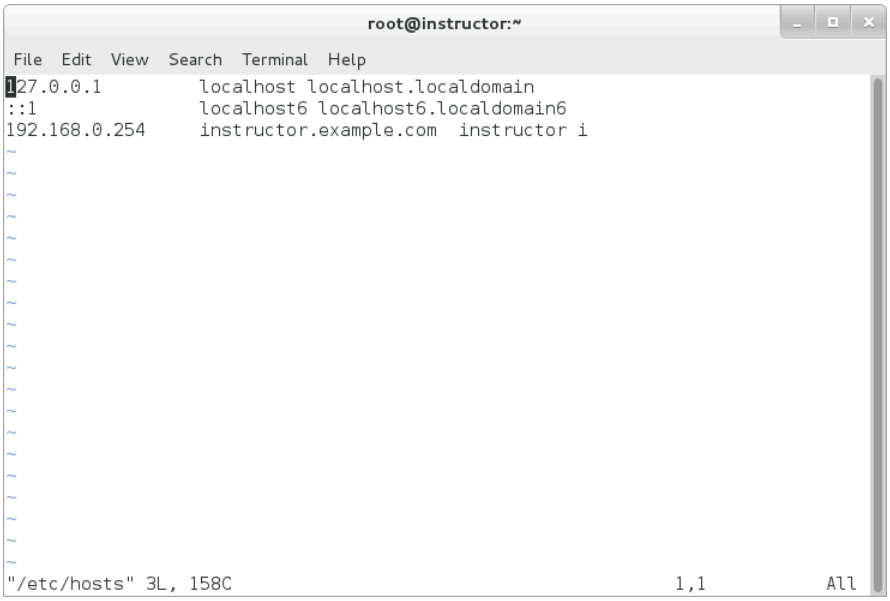

Figura 3.1:
***vim** que muestra un archivo recién abierto*

Edición de texto
Si ha usado alguna vez **vi** o **vim** antes, es posible que haya observado que en el modo *comando*, la mayoría de las teclas no hace exactamente lo que se espera. Esto se debe a que en modo *comando*, las teclas no están asignadas para insertar los caracteres que presiona, sino que realizan comandos como movimientos del cursor, acciones de copiar y pegar y más.

Para cambiar al modo *insertar*, hay comandos disponibles, cada uno asignado a una tecla diferente del teclado:

Tecla	Resultado
i	Cambia al modo *insertar* y comienza a insertar *antes* de la posición actual del cursor (insertar).
a	Cambia al modo *insertar* y comienza a insertar *luego* de la posición actual del cursor (anexar).
I	Mueve el cursor hasta el *inicio* de la línea actual y cambia al modo *insertar*.
A	Mueve el cursor hasta el *final* de la línea actual y cambia al modo *insertar*.
R	Cambia al modo *replace*, y comienza en el carácter bajo el cursor. En el modo *replace*, no se inserta texto, sino que cada carácter que ingresa reemplaza a un carácter del documento actual. (**vim** y **vi** también vienen con comandos de reemplazo más potentes; estos se analizan en otra sección.)
o	Abra una nueva línea *debajo* de la actual y cambie inmediatamente al modo *insertar*.
O	Abra una nueva línea *arriba* de la actual y cambie al modo *insertar*.

Siempre que se encuentre en el modo *insertar* o *replace*, la regla mostrará **--INSERT--** o **--REPLACE--**. Para volver al modo *comando*, puede presionar **Esc**.

La versión de **vi** y **vim** que viene con Red Hat Enterprise Linux se configura para que reconozca y use las teclas de dirección normales, así como teclas, tales como **PgUp** y **End**, mientras se encuentra en los modos *insertar* y *comando*. Este no es el comportamiento predeterminado en todas las instalaciones de **vi**. De hecho, las versiones anteriores de **vi** no reconocían las teclas de dirección en absoluto, y solo permitían mover el cursor si estaba en el modo *comando* usando teclas como **hjkl**.

En la siguiente tabla, encontrará algunas de las teclas que puede usar desde el modo *comando* para mover el cursor:

Tecla	Resultado
h	Cursor una posición a la izquierda
l	Cursor una posición a la derecha
j	Cursor una línea abajo
k	Cursor una línea arriba
^	Mueve el cursor hacia el inicio de la linea actual.
$	Mueve el cursor hacia el final de la linea actual.
gg	Mueve el cursor hacia la primera línea del documento.
G	Mueve el cursor hacia la última línea del documento.

nota

Si presiona **Esc** siempre se cancelará el comando actual o volverá al modo *comando*. Es una práctica común presionar **Esc** dos veces (o más) para garantizar que el sistema vuelva al modo *comando*.

Almacenamiento de archivos

El guardado de archivos en **vim** se hace desde el modo *ex*. Puede entrar al modo *ex* presionando **:** (dos puntos) desde el modo *comando*. Luego de ingresar al modo *ex*, la regla mostrará dos puntos (**:**) y esperará que se ingrese un comando. Los comandos se completan al presionar **Enter**

A continuación, se muestra una lista breve de comandos para guardar y cerrar el archivo que está usando actualmente desde el modo *ex*. De ningún modo es una lista completa de los comandos que se pueden usar.

Comando	Resultado
:wq	Guarda y cierra el archivo actual.
:x	Guarda el archivo actual si hay cambios sin guardar, y luego lo cierra.
:w	Guarda el archivo actual y permanece en el editor.
:w *<filename>*	Guarda el archivo actual bajo un nombre de archivo diferente.
:q	Cierra el archivo actual (solo si no hay cambios sin guardar).
:q!	Cierra el archivo actual, e ignora los cambios no guardados.

Un breve resumen de la tabla anterior es que **w** guarda (escribe), **q** cierra y **!** fuerza una acción (haz lo que digo, no lo que quiero).

Obtener ayuda

vim viene con una amplia ayuda en línea, disponible en el editor. Al escribir **:help** desde el modo *comando*, se iniciará la primera pantalla, que incluye la ayuda necesaria para navegar en la ayuda.

Se puede obtener ayuda para un tema específico al escribir **:help *subject*** desde el modo *comando*.

Las pantallas de ayuda se abren en una *nueva ventana dividida,* y se pueden cerrar con **:q**. Para obtener más información sobre ventanas divididas, use **:help windows**.

Además, hay un tutor seminteractivo disponible. Al iniciar el comando **vimtutor** desde la línea de comandos, se iniciará un recorrido guiado de **vim** que lleva a un nuevo usuario a conocer los conceptos básicos en aproximadamente una hora.

Referencias

Página del manual (1)**vim**

vim ayuda incluida

Práctica: Flujo de trabajo básico de vim

En este trabajo de laboratorio, editará un archivo de texto usando **vim**.

Recursos	
Máquinas:	**desktopX**

Resultados
Un archivo de texto editado correctamente.

Andes de comenzar
Una cuenta de **student** en funcionamiento en **desktopX**.

1. Inicie sesión en su sistema **desktopX** como **student** y abra una terminal.
2. Abra el (nuevo) archivo **/home/&stu;/vim-practice.txt** en **vim**. No tiene que crear este archivo primero.

   2.1.
   ```
   [student@desktopX ~]$ vim vim-practice.txt
   ```
3. Inserte el siguiente texto:

   ```
   This is my vim practice file.
   There are many like it, but this one is mine.
   ```

   3.1. Presione **i** o **a** para ingresar en el modo *insertar*.

   3.2. Escriba el texto que se mostró anteriormente.

   3.3. Presione **Esc** para volver al modo *comando*.
4. Inserte una nueva línea en la parte inferior con el siguiente contenido:

   ```
   More lines, I want more lines!
   ```

   4.1. Presione **o** para abrir una nueva línea debajo de la actual y cambiar inmediatamente al modo *insertar*.

   4.2. Escriba la línea que se agregará.

   4.3. Presione **Esc** para volver al modo *comando*.
5. Guarde y cierre el archivo.

   5.1. Desde el modo *comando*, ingrese **:wq**, y luego presione **Enter**.

Edición con vim

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Usar atajos de movimiento.
- Copiar y pegar texto.
- Usar herramientas para buscar y reemplazar.
- Deshacer (y rehacer) acciones.

Movimiento

Además de los antiguos y aburridos movimientos del cursor por caracteres/líneas simples que se pueden realizar en el modo *comando*, también hay varios comandos de movimientos avanzados para ayudar a los usuarios a navegar por los documentos de forma más eficiente. Estos atajos permiten el movimiento del cursor por palabra, oración o párrafo. Tenga en cuenta que, a diferencia de los movimientos regulares del cursor, estos comandos solo funcionan en el modo *comando*, y no en modo *insertar*.

Tecla	Resultado
w	Mueve el cursor hasta el principio de la siguiente palabra (**W** incluye puntuación).
b	Mueve el cursor hasta el principio de la palabra anterior (**B** incluye puntuación).
(	Mueve el cursor hasta el inicio de la oración actual o anterior.
)	Mueve el cursor hasta el inicio de la siguiente oración.
{	Mueve el cursor hasta el inicio del párrafo actual o anterior.
}	Mueve el cursor hasta el inicio del siguiente párrafo.

Se puede incluir un número delante de todos los comandos de movimiento, p. ej., **5w** para mover el cursor cinco palabras o **12j** para mover el cursor 12 líneas hacia abajo. De hecho, cada comando simple (incluido el cambio al modo *insertar*) se puede repetir una cantidad fija de veces al escribir el número de repeticiones antes del comando real. En la terminología **vim**, esto se denomina *conteo*.

Reemplazo de texto

vim permite a los usuarios reemplazar fácilmente grandes (y pequeñas) cantidades de texto usando el comando "change" (cambiar). El comando "change" (cambiar) funciona al presionar la tecla **c**, seguida de un movimiento del cursor; por ejemplo, **cw** para cambiar la posición actual del cursor hasta el final de la palabra actual. El texto que será reemplazado se elimina (y se coloca en el registro no nombrado) y **vim** cambia al modo *insertar*.

Hay varios atajos disponibles para hacer la edición más eficiente:

- Si presiona dos veces **c** (**cc**), se iniciará el reemplazo en la *línea,* y reemplazará la línea entera (o varias líneas cuando se le agrega un número delante). El mismo truco también se aplica a varios comandos (como el comando para eliminar).
- Se puede incluir una **i** y una **a** delante de la mayoría de los comandos de movimiento para seleccionar *la versión interna* o *a* del movimiento. Por ejemplo, **ciw** reemplazará toda la palabra actual, no solo desde la posición actual del cursor, y **caw** hará lo mismo, pero incluidos los espacios que la rodean.
- Para reemplazar hasta el final de la línea, se puede usar **c$**, pero **C** hace lo mismo. (Este truco también se aplica a varios otros comandos, como el comando para eliminar).
- Para simplemente reemplazar el carácter debajo del cursor, presione **r** seguido del nuevo carácter.
- Para cambiar entre mayúscula y minúscula el carácter debajo del cursor, presione **~**.

Eliminación de texto

La eliminación de texto funciona igual que el reemplazo de texto. El comando para eliminar texto es **d**, y todos los mismos movimientos que son válidos para cambiar texto también se aplican para eliminar texto, incluida la **D** para eliminar desde el cursor hasta el final de la línea.

Para eliminar solo el carácter debajo del cursor, use **x**.

Copiar y pegar

vim usa terminología levemente diferente para describir las operaciones de copiar y pegar a la que la mayoría de las personas están acostumbradas actualmente. Una operación de copiar se denomina *yank*, y la de pegar, *put*. Esto se refleja en los comandos del teclado asignados a estas operaciones: *yank* es **y** seguida de un movimiento, y las operaciones *put* se realizan con **p** y **P**.

Las operaciones yank siguen el mismo esquema general que las operaciones para reemplazar y eliminar texto: opcionalmente, un usuario escribe la cantidad de veces que desea repetir una operación seguida de **y**, seguida de un movimiento. Por ejemplo, **5yaw** copiará la palabra actual y las siguientes cuatro (para lograr un total de cinco). Si se presiona **yy**, se realizará la acción yank en toda la línea, etc.

La acción put (pegar) se realiza con los comandos **p** y **P**; la **p** minúscula pegará *después* de la posición actual del cursor (o debajo de la línea actual cuando se copien los datos de la línea), mientras que la **P** mayúscula pega *antes* de la posición actual del cursor, o arriba de la línea actual. Al igual que con los demás comandos, se puede colocar un número delante para establecer la cantidad de veces que se desea pegar el registro.

Varios registros

En lugar de solo un portapapeles para copiar y pegar, **vim** tiene 26 registros *nombrados,* además de una cantidad de registros para fines especiales. Tener varios registros disponibles permite a los usuarios cortar y pegar de forma más eficaz, sin tener que preocuparse por perder datos o mover demasiado el cursor. Si un registro que desea usar no está especificado, se usará el registro "no nombrado". Los registros normales se denominan **a** a **z**, y se seleccionan al poner ***"nombre del registro*** entre *el conteo* de un comando y el comando real; por ejemplo, para copiar la línea actual y las dos siguientes en el registro **t**, se puede usar el comando **3"tyy**.

Para pegar fuera de un registro nombrado, simplemente coloque **"*nombre del registro*** delante del comando put; por ejemplo, **"sp** pegará luego del cursor fuera del registro **s**.

Importante

Siempre que se utilice un registro nombrado, el registro no nombrado también se actualizará.

Hay una selección de registros que se pueden colocar delante de las operaciones para eliminar y cambiar texto. Cuando no se especifica ningún registro, solo se usará el registro no nombrado. Cuando se usa la versión en mayúscula de un registro, el texto que se corta, o para el cual se usa yank, se agrega al registro en lugar de sobrescribirlo.

Registros especiales
Hay 10 *registros* numerados, de **"0** a **"9**. El registro **"0** siempre tendrá una copia del texto más reciente para el cual se usó yank, mientras que el registro **"1** tendrá una copia del texto eliminado más reciente. Cuando se cambia o se elimina texto nuevo, el contenido de **"1** cambiará a **"2**, **"2** a **"3**, etc.

Importante

A diferencia de los registros nombrados, el contenido de los registros numerados **no** se guarda entre sesiones.

Modo visual

Para evitar tener que contar constantemente la cantidad de líneas, palabras o caracteres que especificar para los comandos, **vim** también incluye *el modo (de selección)* visual. Luego de ingresar al modo *visual* (indicado por **--VISUAL--** en la regla), todos los movimientos del cursor comenzarán a seleccionar texto. Cualquier comando de cambio, eliminación o yank emitido en el modo *visual* no necesita una parte de movimiento del cursor, sino que funcionará en el texto seleccionado.

El modo *visual* incluye tres clases (flavors): basado en caracteres (que comienza con **v**), basado en líneas (que comienza con **V**) y basado en bloques (que comienza con **Ctrl**+**V**). Al usar **gvim**, también se puede usar el mouse para seleccionar texto.

Todos los comandos **ex** emitidos en el modo *visual* también funcionarán, de forma predeterminada, sobre el texto seleccionado.

Búsqueda

La búsqueda en el documento actual puede iniciarse de dos maneras: al presionar **/** para buscar hacia delante desde la posición del curso, o al presionar **?** para buscar hacia atrás desde la posición actual del cursor. Luego de ingresar al modo de búsqueda, se puede escribir una expresión regular para buscar, y al presionar **Enter**, saltará a la primera coincidencia (si es que hay alguna).

Para buscar la coincidencia siguiente o la anterior, use **n** y **N**, respectivamente.

Atajo adicional: ***** buscará instantáneamente hacia adelante la palabra debajo del cursor.

Buscar y reemplazar

La función de buscar y reemplazar en **vim** se implementa en modo *ex*, y usa la misma sintaxis que se usaría con **sed** para buscar y reemplazar, incluida la capacidad de buscar usando expresiones regulares:

range*s/*pattern*/*string*/*flags

range (intervalo) puede ser un número de línea (**42**), un intervalo de números de línea (**1,7** para las líneas 1-7), un término de búsqueda (**/README\.txt/**), **%** para todas las líneas del documento actual (buscar y reemplazar normalmente solo funciona en la línea actual), o **'<,'>** para la selección actual del modo *visual*.

Dos de los ***flags*** (indicadores) más comunes son **g**, para habilitar el reemplazo de más de una aparición de ***pattern*** (patrón) por línea, e **i**, para hacer que la búsqueda actual distinga entre mayúsculas y minúsculas.

Ejemplo de buscar y reemplazar
Por ejemplo, para buscar cada aparición de la palabra “cat” y reemplazarla con “dog” en todas las líneas, independientemente de si está en mayúscula o minúscula, pero solo si es una palabra completa, y no algo como “catalog”, se podría usar el siguiente comando:

```
:%s/\<cat\>/dog/gi
```

Deshacer y rehacer

Para permitir la imperfección humana, **vim** cuenta con un mecanismo para deshacer y rehacer. Simplemente al presionar **u** en el modo *comando*, se deshará la última acción. Si se ha usado la acción de deshacer en exceso, al presionar **Ctrl**+**r**, se rehará la última acción para la que usó la función de deshacer.

Genialidad adicional: al presionar **.** (punto) desde el modo *comando*, se rehará la última acción de edición, pero en la línea actual. Esto se puede usar para realizar fácilmente la misma acción de edición varias veces.

Referencias

Página del manual (1)**vim**

vim ayuda incluida

Práctica: Editar un archivo con vim

En este trabajo de laboratorio, editará un archivo usando **vim**.

Recursos	
Máquinas:	**desktopX**
Archivos:	**/usr/share/doc/vim-common-*/README.txt**

Resultados
Una copia de **vim README.txt** que ha sido editada según las instrucciones de este ejercicio de práctica.

Andes de comenzar
N/D

1. Inicie sesión en su sistema **desktopX** como **student** y abra una terminal.
2. Cree una copia del archivo **/usr/share/doc/vim-common-*/README.txt** en su directorio principal.

   2.1.
   ```
   [student@desktopX ~]$ cp /usr/share/doc/vim-common-*/README.txt .
   ```
3. Abra **/home/student/README.txt** en **vim**.

   3.1.
   ```
   [student@desktopX ~]$ vim README.txt
   ```
4. Salte a la sección titulada **MAIN AUTHOR** (AUTOR PRINCIPAL), y luego ponga el cursor en la **A** de **AUTHOR** (AUTOR).

   4.1. Desde el modo *comando*, escriba lo que se detalla a continuación, y luego presione **Enter**. Esto lo llevará a la primera aparición del texto:

   ```
   /MAIN AUTHOR
   ```

   4.2. Presione **w** para mover el cursor una palabra hacia la derecha; esto lo llevará a la **A** de **AUTHOR**.
5. Cambie esta aparición de la palabra **AUTHOR** a **ROCKSTAR** (ESTRELLA DE ROCK).

   5.1. Desde el modo *comando*, escriba **cw** para cambiar la palabra que está debajo del cursor.

   5.2. Escriba **ROCKSTAR**.

   5.3. Presione **Esc** para volver al modo *comando*.
6. Deshaga su edición anterior.

   6.1. Presione **u** para deshacer su última edición.

7. Rehaga (es decir, deshaga lo que deshizo) su última edición.

   7.1. Presione **Ctrl**+**r** para rehacer lo último que deshizo.

8. Mediante el uso del modo *visual*, haga una copia del párrafo **INSTALLATION** (INSTALACIÓN) (incluido el encabezado) y colóquela al final del archivo.

   8.1. Mueva el cursor hasta el inicio de la sección **INSTALLATION** mediante la búsqueda de **^INSTALLATION**. Desde el modo *comando*, escriba:

   ```
   /^INSTALLATION
   ```

   8.2. Ingrese al modo *línea visual* presionando **V**.

   8.3. Escriba **3}** para mover el cursor hasta el final de la sección. Esto moverá el cursor tres párrafos hacia abajo y seleccionará toda la sección. (El encabezado se cuenta como un párrafo).

   8.4. Presione **y** para usar *yank* (copiar) con las líneas seleccionadas en el búfer no nombrado.

   8.5. Presione **G** para mover el cursor hasta el final del documento.

   8.6. Presione **p** para usar *put* (pegar) para pegar el búfer no nombrado debajo de la línea actual.

9. En todo el documento, reemplace cada ocurrencia de **README** (LÉAME) con **PLEASE_READ_ME** (POR FAVOR, LÉAME).

   9.1. Desde el modo *comando*, escriba lo siguiente:

   ```
   :%s/README/PLEASE_READ_ME/g
   ```

   - Los **:** ingresan al modo *Ex*.
   - **%** indica que deseamos trabajar en cada línea del documento.
   - **s/README/PLEASE_READ_ME/** es el comando de buscar y reemplazar.
   - La **g** final indica que esta operación de reemplazo se puede realizar más de una vez por línea.

10. Salga sin guardar los cambios.

    10.1 Desde el modo *comando* escriba **:q!**.

    Los **:** ingresan al modo *ex*, la **q** indica que deseamos cerrar, y el signo **!** indica a **vim** que se debe forzar el cierre porque no se guardaron los cambios.

11. Eliminar su **README.txt** para limpiar.

11.1
```
[student@desktopX ~]$ rm README.txt
```

Trabajo de laboratorio: Editar un archivo de sistema con vim

En este trabajo de laboratorio, creará y editará un nuevo archivo del sistema usando **vim**.

Recursos	
Archivos:	**/etc/motd**
Máquinas:	**desktopX**

Resultados
Un archivo **/etc/motd** actualizado en **desktopX**.

Andes de comenzar
N/D

Se le solicitó que actualice el archivo *Message-Of-The-Day* (MOTD) (Mensaje del día) en **desktopX**. Este archivo se denomina **/etc/motd**, y su contenido se muestra a los usuarios luego de un inicio de sesión correcto en la línea de comandos.

1. Actualice el archivo **/etc/motd** en **desktopX** para que lea exactamente lo mismo que en el siguiente bloque de texto sin reemplazar el valor de "X" en este paso:

```
desktopX.example.com

Please be careful.
```

2. Evalúe sus cambios con **ssh** para conectarse con la cuenta **student** en **localhost**. Si todo sale bien, debería ver su nuevo mensaje luego de la autenticación. Cierre la conexión de **ssh** cuando haya finalizado la prueba.

3. Edite **/etc/motd** nuevamente. Esta vez, reemplace la **X** en **desktopX.example.com** con el número de su estación real, usando la función buscar y reemplazar. También se le solicita que repita la línea "**Please be careful.**" (Por favor, tenga cuidado) dos veces más.

4. Evalúe sus cambios con **ssh** para conectarse con **student@localhost** nuevamente.

Solución

En este trabajo de laboratorio, creará y editará un nuevo archivo del sistema usando **vim**.

Recursos	
Archivos:	**/etc/motd**
Máquinas:	**desktopX**

Resultados
Un archivo **/etc/motd** actualizado en **desktopX**.

Andes de comenzar
N/D

Se le solicitó que actualice el archivo *Message-Of-The-Day* (MOTD) (Mensaje del día) en **desktopX**. Este archivo se denomina **/etc/motd**, y su contenido se muestra a los usuarios luego de un inicio de sesión correcto en la línea de comandos.

1. Actualice el archivo **/etc/motd** en **desktopX** para que lea exactamente lo mismo que en el siguiente bloque de texto sin reemplazar el valor de "X" en este paso:

```
desktopX.example.com

Please be careful.
```

   1.1. Inicie sesión en su sistema **desktopX** como **student** y abra una terminal.

   1.2. Dado que **/etc/motd** es un archivo del sistema, deberá elevar sus privilegios.

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

   1.3. Abra **/etc/motd** en **vim**.

```
[root@desktopX ~]# vim /etc/motd
```

   1.4. Presione **i** o **a** para ingresar en el modo *insertar*, luego ingrese el siguiente texto:

```
desktopX.example.com

Please be careful.
```

   1.5. Presione **Esc** para salir del modo *insertar* y volver al modo *comando*; luego escriba **:wq** para entrar al modo *ex* para guardar y cerrar.

2. Evalúe sus cambios con **ssh** para conectarse con la cuenta **student** en **localhost**. Si todo sale bien, debería ver su nuevo mensaje luego de la autenticación. Cierre la conexión de **ssh** cuando haya finalizado la prueba.

   2.1.

```
[root@desktopX ~]# ssh student@localhost
The authenticity of host 'localhost (::1) can't be established.
```

```
RSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
student@localhost's password: student
desktopX.example.com

Please be careful.
[student@desktopX ~]$ exit
```

3. Edite **/etc/motd** nuevamente. Esta vez, reemplace la **X** en **desktopX.example.com** con el número de su estación real, usando la función buscar y reemplazar. También se le solicita que repita la línea "**Please be careful.**" (Por favor, tenga cuidado) dos veces más.

   3.1. Abra **/etc/motd** en **vim**. Asegúrese de que aún esté trabajando como **raíz**.

   ```
   [root@desktopX ~]# vim /etc/motd
   ```

   3.2. Use la función buscar y reemplazar para reemplazar la **X** con el número de su estación real. En el siguiente ejemplo, se supone que usted está en la estación número **99**.

   Desde el modo *comando*, ingrese al modo *ex* y escriba lo siguiente para reemplazar todas las apariciones de **X** con **99**:

   ```
   :%s/X/99/g
   ```

   3.3. Escriba lo siguiente para mover el cursor al número de línea tres en el modo *comando*:

   ```
   :3
   ```

   3.4. Escriba **yy2p** para usar yank para copiar la línea actual, luego put para pegarla dos veces.

   La parte **yy** pega la línea actual y **2p** la pega dos veces.

   3.5. Escriba **:wq** para guardar y salir.

4. Evalúe sus cambios con **ssh** para conectarse con **student@localhost** nuevamente.

   4.1.
   ```
   [root@desktopX ~]# ssh student@localhost
   student@localhost's password: student
   desktop99.example.com

   Please be careful.
   Please be careful.
   Please be careful.
   [student@desktopX ~]$ exit
   ```

Resumen

El editor de textos de vim

- **`vim`** tiene tres modos principales.
  - *El modo comando* para la navegación de archivos y comandos simples.
  - *El modo insertar* para la edición de texto normal.
  - *El modo ex* para guardar, cerrar y realizar comandos más complejos.

Flujo de trabajo básico de `vim`

- Se pueden usar tanto las teclas de dirección como **`hjkl`** para mover el cursor.
- **`Escape`** sale del comando o modo actual, presione dos veces siempre para finalizar en modo comando.
- **`:w`** guarda, **`:q`** cierra, **`:wq`** guarda y cierra.

Edición con vim

- Comandos rápidos del cursor: **`wb(){}`**.
- **`c`** ingresa en el modo de cambio.
- **`d`** y **`y`** para cortar y copiar, **`p`** para pegar.

redhat. TRAINING

CAPÍTULO 4

PROGRAMACIÓN DE TAREAS FUTURAS DE LINUX

Descripción general	
Meta	Programar tareas para que se ejecuten automáticamente en el futuro.
Objetivos	• Programar tareas únicas con at. • Programar trabajos recurrentes con cron. • Programar trabajos de sistemas recurrentes. • Administrar archivos temporales.
Secciones	• Programación de tareas únicas con at (y práctica) • Programación de trabajos recurrentes con cron (y práctica) • Programación de trabajos cron del sistema (y práctica) • Administración de archivos temporales (y práctica)
Prueba del capítulo	• Programación de tareas futuras de Linux

Programación de tareas únicas con at

Objetivo

Luego de completar esta sección, los estudiantes deberían poder programar tareas únicas con **at**.

Programación de tareas futuras

De vez en cuando, un administrador (o usuario final) desea ejecutar un comando, o conjunto de comandos, en un punto establecido en el futuro. Entre los ejemplos, se incluyen el trabajador de oficina que desea programar un correo electrónico para su jefe, así como el administrador de sistemas que está trabajando en una configuración de firewall que pone un trabajo de "seguridad" en vigencia para restablecer la configuración de firewall en un tiempo de diez minutos, a menos que desactive el trabajo antes.

Estos comandos programados a menudo se denominan *tareas* o *trabajos*.

Programación de tareas únicas con at

Una de las soluciones disponibles para los usuarios de un sistema Red Hat Enterprise Linux para la programación de tareas futuras es **at**. Esa no es una herramienta independiente, sino un daemon del sistema (**atd**), con un conjunto de herramientas de línea de comandos para interactuar con el daemon (**at**, **atq**, y más). En una instalación de Red Hat Enterprise Linux predeterminada, el daemon **atd** se instalará y habilitará automáticamente. El daemon **atd** se puede hallar en el paquete *at*.

Los usuarios (incluido **raíz**) pueden poner en cola trabajos para el daemon **atd** usando la herramienta de línea de comandos **at**. El daemon **atd** proporciona 26 colas, de la **a** a la **z**, con trabajos en colas ordenadas alfabéticamente que obtienen menos prioridad en el sistema (niveles *buenos* más altos, analizados en un capítulo posterior).

Programación de trabajos

Se puede programar un nuevo trabajo con el comando **at <*TIMESPEC*>**. Luego, **at** leerá los comandos para ejecutarlos desde **stdin**. Para comandos más grandes, y comandos que distinguen errores de escritura, a menudo es más fácil usar la redirección de entrada desde un archivo de script, p. ej., **at now +5min < myscript**, que escribir todos los comandos a mano en una ventana de terminal. Al ingresar comandos a mano, puede terminar su entrada presionando **Ctrl**+**D**.

El **<*TIMESPEC*>** permite muchas combinaciones poderosas, lo que da a los usuarios una manera (casi) libre de describir exactamente cuándo un trabajo debe ejecutarse. Típicamente, comienzan con una hora, p. ej., **02:00 p. m.**, **15:59** o incluso la **teatime** (hora del té), seguida de una fecha opcional o una cantidad de días en el futuro.

Algunos ejemplos de combinaciones que se pueden usar se detallan en el siguiente texto. Para conocer una lista completa, consulte la definición de **timespec** en las referencias.

- **now + 5 min (ahora + 5 min)**
- **teatime tomorrow** (hora del té mañana) (la hora del té es **16:00**)
- **noon + 4 days (mediodía + 4 días)**

- **5 p.m. August 3 2016 (5 p. m., 3 de agosto, 2016)**

Inspección y administración de trabajos

Inspección de trabajos
Para obtener una descripción general de trabajos pendientes para su usuario, use el comando **atq** o, de forma alternativa, el alias **at -l**.

Ejecutar este comando da el siguiente resultado:

```
[student@desktopX ~]$ atq
28  Mon Feb  2 05:13:00 2015 a student
29  Mon Feb  3 16:00:00 2014 h student
27  Tue Feb  4 12:00:00 2014 a student
```

Este muestra cuatro columnas para cada trabajo programado para ejecutarse en el futuro:

- El número de trabajo, **28**, en la primera línea.
- La fecha y la hora programados para ese trabajo, **Mon Feb 2 05:13:00 2015** (lunes, 2 de febrero, 05:13:00, 2015), en la primera línea.
- La cola para el trabajo, **a**, en la primera línea, pero **h** en la segunda.
- El propietario del trabajo (y el usuario con el cual se ejecutará el trabajo), **student** en todas nuestras líneas.

Importante

Los usuarios normales sin privilegios solo pueden ver y controlar sus propios trabajos. El usuario **raíz** puede ver y administrar todos los trabajos.

Para inspeccionar los comandos reales que se ejecutarán cuando se ejecute un trabajo, use el comando **at -c <*JOBNUMBER*>**. Este resultado mostrará primero el *entorno* para el trabajo que se configura para reflejar el entorno del usuario que creó el trabajo en el momento en que se creó, seguido de los comandos reales que se ejecutarán.

Eliminar trabajos
El **atrm <*JOBNUMBER*>** eliminará un trabajo programado. Esto es útil cuando un trabajo ya no es necesario; por ejemplo, cuando una configuración de firewall remota dio un resultado satisfactorio, y no es necesario que se restablezca.

Referencias

Páginas del manual: **at**(1), **atd**(8)

/usr/share/doc/at-*/timespec

Práctica: Programación de tareas únicas con at

En este laboratorio, programará tareas únicas para el futuro.

Recursos	
Máquinas:	**desktopX**

Resultados
Tres trabajos programados para el futuro, con uno ejecutado y dos eliminados nuevamente.

1. Inicie sesión en su máquina **desktopX** como **student** y abra una ventana de terminal.
2. Programe una tarea para tres minutos en el futuro. La tarea debe escribir un sello de tiempo para **/home/&stu;/myjob**.

   2.1.
   ```
   [student@desktopX ~]$ echo "date > ~/myjob" | at now +3min
   ```
3. Inspeccione la lista de tareas programadas para la ejecución en el futuro para su usuario.

   3.1.
   ```
   [student@desktopX ~]$ atq
   1       Thu Jan 30 05:13:00 2014 a student
   ```
4. Espere a que su trabajo se ejecute, luego inspeccione el contenido de **/home/&stu;/myjob**.

   4.1. Repetidamente ejecute **atq** hasta que su trabajo desaparezca de la lista o (si solo tiene un trabajo pendiente y desea incluir scripts):

   ```
   [student@desktopX ~]$ while [ $(atq | wc -l) -gt 0 ]; do sleep 1s; done
   ```

   4.2.
   ```
   [student@desktopX ~]$ cat myjob
   ```
5. Programe un trabajo para ejecutar a las **16:00** mañana, usando la cola **g**. Este trabajo crea un nuevo archivo denominado **/home/&stu;/tea**.

   5.1.
   ```
   [student@desktopX ~]$ at -q g teatime tomorrow
   at> touch /home/student/tea
   at> Ctrl+D
   ```
6. Programe un trabajo, esta vez en la cola **b**, para que se ejecute a las 16:05 mañana. Este trabajo crea un nuevo archivo **/home/&stu;/cookies**.

   6.1.
   ```
   [student@desktopX ~]$ at -q b 16:05 tomorrow
   at> touch /home/student/cookies
   at> Ctrl+D
   ```

7. Inspeccione sus trabajos pendientes. Inspeccione los comandos reales que sus trabajos también ejecutarán.

   7.1.
   ```
   [student@desktopX ~]$ atq
   2       Fri Jan 31 16:00:00 2014 g student
   3       Fri Jan 31 16:05:00 2014 b student
   ```

   7.2.
   ```
   [student@desktopX ~]$ at -c 2
   [student@desktopX ~]$ at -c 3
   ```

8. Ha decidido que en realidad no le gusta tanto el té. Elimine el trabajo que escribe el archivo **/home/&stu;/tea**, pero mantenga el trabajo que escribe **/home/&stu;/cookies** (le gustan las galletas).

   8.1.
   ```
   [student@desktopX ~]$ atrm 2
   ```

   Importante: Si su trabajo para escribir **/home/&stu;/tea** tenía un número diferente de **2**, use ese número en el comando anterior.

Programación de trabajos recurrentes con cron

Objetivo

Luego de completar esta sección, los estudiantes deben poder programar trabajos recurrentes con **cron**.

Introducción a cron

Al usar **at**, se podría, en teoría, programar un trabajo recurrente al hacer que el trabajo vuelva a enviar un nuevo trabajo al final de su ejecución. En la práctica, esto resulta ser una mala idea. Los sistemas Red Hat Enterprise Linux incluyen el daemon **crond** habilitado e iniciado de forma predeterminada específicamente para trabajos recurrentes. Múltiples archivos de configuración, uno por usuario [editado con el comando **crontab**(1)], y archivos en todo el sistema controlan**crond** . Estos archivos de configuración les dan a los usuarios y administradores el control detallado exactamente cuando sus trabajos recurrentes deben ser ejecutados. El daemon **crond** se instala como parte del paquete *cronie*.

Si los comandos se ejecutan desde un trabajo **cron** producen cualquier resultado para **stdout** o **stderr** que no es redirigido, el daemon **crond** intentará enviar por correo electrónico ese resultado al usuario que es propietario de ese trabajo (a menos que se haya anulado) usando el servidor de correo configurado en el sistema. Según el entorno, es posible que sea necesaria una configuración adicional.

Programación de trabajos

Los usuarios normales pueden usar el comando **crontab** para administrar sus trabajos. Este comando se puede denominar de cuatro maneras diferentes:

Comando	Uso previsto
crontab -l	Detallar los trabajos para el usuario actual.
crontab -r	Eliminar **todos** los trabajos del usuario actual.
crontab -e	Editar trabajos para el usuario actual.
crontab <*filename*>	Eliminar todos los trabajos y reemplazar con los trabajos leídos de **<*nombre de archivo*>**. Si no se especifica ningún archivo, se usará **stdin**.

nota

raíz puede usar la opción **-u <*username*>** para administrar los trabajos para otro usuario. No se recomienda usar el comando **crontab** para administrar trabajos del sistema; en cambio, se deben usar los métodos descritos en la siguiente sección.

Formato de trabajos

Al editar trabajos con el **crontab -e**, se iniciará un editor (**vi** de forma predeterminada, a menos que la variable del entorno **EDITOR** haya sido establecida en algo diferente). El

archivo que se edita tendrá un trabajo por línea. Se permiten líneas vacías, y los comentarios inician su línea con un símbolo numeral (**#**). Las variables del entorno también se pueden declarar, usando el formato **`NAME=value`**, y afectará todas las líneas *debajo* de la línea donde se declararon. Las variables del entorno comunes en un **`crontab`** incluyen **`SHELL`** y **`MAILTO`**. La configuración de la variable **`SHELL`** cambiará qué shell se usa para ejecutar los comandos en las líneas debajo de esta, mientras que la configuración de la variable **`MAILTO`** cambiará el resultado de la dirección de correo electrónico (si existe alguno) al que se enviará el correo.

Importante

Enviar un correo electrónico puede requerir la configuración adicional del servidor de correo local o retransmisión SMTP en un sistema.

Los trabajos individuales constan de seis campos en los que se detallan cuándo y qué debe ejecutarse. Cuando los cinco primeros campos coinciden con la fecha y la hora actuales, el comando en el último campo se ejecutará. Estos campos son (en orden):

- Minutes (Minutos)
- Hours (Horas)
- Day-of-Month (Día del mes)
- Month (Mes)
- Day-of-Week (Día de la semana)
- Command (Comando)

Importante

Cuando los campos “Day-of-Month” (Día del mes) y “Day-of-Week” (Día de la semana) son distintos de **`*`**, el comando se ejecutará cuando **cualquiera** de estos campos coincidan. Esto se puede usar, por ejemplo, para ejecutar un comando el día 15 de cada mes, y cada viernes.

Los primeros cinco de estos campos usan las mismas reglas de sintaxis:

- **`*`** para “Don't Care”/always (no importa/siempre)
- Un número para especificar una cantidad de minutos u horas, una fecha o un día de la semana. (Para los días de semana, **`0`** equivale a domingo, **`1`** equivale a lunes, **`2`** equivale a martes, etc. **`7`** también equivale a domingo).
- **`x-y`** para un intervalo, **`x`** hasta **`y`** inclusive
- **`x,y`** para listas. Las listas pueden incluir intervalos también, por ejemplo, **`5,10-13,17`** en la columna “Minutes” (Minutos) para indicar que un trabajo debe ejecutarse a los 5 minutos de la hora, a los 10 minutos, a los 11 minutos, a los 12 minutos, a los 13 minutos y a los 17 minutos.
- **`*/x`** para indicar un intervalo de **`x`**, por ejemplo, **`*/7`** en la columna de minutos ejecutará un trabajo exactamente cada siete minutos.

Asimismo, se pueden usar abreviaturas en inglés de tres letras para los meses y los días de la semana, por ejemplo, Jan (enero), Feb (febrero) y Tue (martes), Wed (miércoles).

El último campo contiene el comando que se ejecutará. Este comando se ejecutará mediante **/bin/sh**, a menos que se haya declarado una variable del entorno **SHELL**. Si el comando contiene un símbolo de porcentaje no codificado (**%**), ese símbolo de porcentaje será tratado como una línea nueva, y todo lo que esté después de ese símbolo de porcentaje será enviado al comando en **stdin**.

Trabajos cron de ejemplo
Algunos trabajos **cron** de ejemplo:

- **0 9 2 2 * /usr/local/bin/yearly_backup**

  Ejecuta el comando **/usr/local/bin/yearly_backup** exactamente a las 9 a. m. del 2 de febrero, todos los años.

- ***/7 9-16 * Jul 5 echo "Chime"**

  Envía un correo electrónico que contiene la palabra **Chime** al propietario de este trabajo, cada siete minutos entre las 9 a. m. y las 5 p. m., todos los viernes de julio.

- **58 23 * * 1-5 /usr/local/bin/daily_report**

  Ejecuta el comando **/usr/local/bin/daily_report** todos los días de la semana dos minutos antes de la medianoche.

- **0 9 * * 1-5 mutt -s "Checking in" boss@example.com % Hi there boss, just checking in.**

  Todos los días laborables (de lunes a viernes), a las 9 a. m. en punto, envía un mensaje de correo a **boss@example.com** usando **mutt**.

Referencias

Páginas del manual: **crond**(8), **crontab**(1), **crontab**(5)

Práctica: Programación de trabajos recurrentes con cron

En este trabajo de laboratorio, programará un trabajo recurrente usando **cron**.

Recursos	
Máquinas:	**desktopX**

Resultados
Un trabajo recurrente se programa, y luego se elimina otra vez.

1. Inicie sesión en su máquina **desktopX** como **student**.
2. Programe un trabajo recurrente que...
   - ... se ejecute como su usuario **student**.
   - ...se ejecute cada dos minutos entre las **09:00** y las **16:59**, de lunes a viernes.
   - ...agregue la fecha y hora actuales al archivo **/home/student/my_first_cron_job**.

   2.1. Inicie el editor **crontab**.

   ```
   [student@desktopX ~]$ crontab -e
   ```

   2.2. Inserte la siguiente línea:

   ```
   */2 9-16 * * 1-5 date >> /home/student/my_first_cron_job
   ```

   2.3. Guarde los cambios y cierre el editor (**:wq**).
3. Inspeccione todos los trabajos **cron** programados.

   3.1.
   ```
   [student@desktopX ~]$ crontab -l
   ```
4. Espere a que su trabajo se ejecute, al menos, una vez o dos veces, y luego, inspeccione el contenido del archivo **/home/student/my_first_cron_job**.

   4.1.
   ```
   [student@desktopX ~]$ cat ~/my_first_cron_job
   ```
5. Elimine *todos* los trabajos **cron** para el estudiante.

   5.1.
   ```
   [student@desktopX ~]$ crontab -r
   ```

Programación de trabajos cron del sistema

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Programar tareas de sistemas recurrentes.

Trabajos cron del sistema

Además de trabajos del *usuario* **cron**, también hay trabajos del *sistema* **cron**.

Los trabajos cron del sistema no se identifican usando el comando **crontab**, sino que se configuran en un conjunto de archivos de configuración. La principal diferencia en estos archivos de configuración es un campo adicional, ubicado entre el campo **Day-of-Week** (Día de la semana) y el campo **Command** (Comando), donde se especifica bajo qué usuario debe ejecutarse un trabajo.

El **/etc/crontab** tiene un diagrama de sintaxis útil en los comentarios incluidos.

```
 # For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed
```

Los trabajos **cron** del sistema se definen en dos ubicaciones: **/etc/crontab** y **/etc/cron.d/***. Los paquetes que instalan trabajos **cron** deben hacerlo al colocar un archivo en **/etc/cron.d/**, pero los administradores también usan esta ubicación para agrupar con más facilidad trabajos relacionados en un único archivo, o enviar trabajos con un sistema de administración de configuración.

También hay trabajos predefinidos que se ejecutan cada hora, día, semana y mes.
Estos trabajos ejecutarán todos los scripts colocados en **/etc/cron.hourly/**, **/etc/cron.daily/**, **/etc/cron.weekly/** y **/etc/cron.monthly/**, respectivamente. Tenga en cuenta que estos directorios contienen *scripts ejecutables*, y no archivos de configuración **cron**.

Importante

Asegúrese de hacer que todos los scripts que coloca en estos directorios sean ejecutables. Si un script no se hace ejecutable (p. ej., con **chmod +x**), no se ejecutará.

Los scripts **/etc/cron.hourly/*** se ejecutan usando el comando **run-parts**, desde un trabajo definido en **/etc/cron.d/0hourly**. Los trabajos diarios, semanales y mensuales también se ejecutan usando el comando **run-parts**, pero desde un archivo de configuración diferente: **/etc/anacrontab**.

En el pasado, **/etc/anacrontab** se manejaba mediante un daemon por separado (**anacron**), pero en Red Hat Enterprise Linux 7, el archivo es analizado por el daemon **crond** regular. El propósito de este archivo es garantizar que los trabajos importantes siempre se ejecuten, y que no se omitan accidentalmente porque el sistema se apagó o quedó inactivo cuando el trabajo debería haberse ejecutado.

La sintaxis de **/etc/anacrontab** es diferente a la de los demás archivos de configuración de **cron**. Contiene exactamente cuatro campos por línea:

- **Period in days (Período en días)**

  Una vez cada cuántos días debe ejecutarse este trabajo.

- **Delay in minutes (Demora en minutos)**

  Cantidad de tiempo que el daemon **cron** debe esperar antes de iniciar este trabajo.

- **Job identifier (Identificador del trabajo)**

  Este es el nombre del archivo en **/var/spool/anacron/** que se usará para comprobar si este trabajo se ha ejecutado. Cuando **cron** inicie un trabajo desde **/etc/anacrontab**, actualizará el sello de tiempo en este archivo. El mismo sello de tiempo se utiliza para comprobar cuándo un trabajo se ha ejecutado por última vez.

- **Command (Comando)**

  El comando que se ejecutará.

/etc/anacrontab también contiene declaraciones variables del entorno usando la sintaxis **NAME=value**. De especial interés es **START_HOURS_RANGE**: los trabajos **no** se iniciarán fuera de este intervalo.

Referencias

Páginas del manual: **crond**(8), **crontab**(1), and **crontab**(5), **anacron**(8), and **anacrontab**(5)

Práctica: Programación de trabajos cron del sistema

En este trabajo de laboratorio, realizará tareas con trabajos de sistemas recurrentes.

Recursos	
Archivos:	• **/etc/crontab** • **/etc/cron.d/*** • **/etc/cron.{hourly,daily,weekly,monthly}/***
Máquinas:	**desktopX**

Resultados
Un trabajo diario para contar la cantidad de usuarios activos, y un trabajo **cron** actualizado para reunir datos de rendimiento del sistema.

1. Inicie sesión en su sistema **desktopX** como **student** y, luego, eleve sus privilegios a **raíz**.

   1.1.
   ```
   [student@desktopX ~]$ su -
   Password: redhat
   ```

2. Cree un nuevo trabajo **cron** diario que registre un mensaje para el registro del sistema con la cantidad de usuarios activos actualmente (**w -h | wc -l**). Puede usar el comando **logger** para enviar mensajes al registro del sistema.

   2.1. Abra un nuevo archivo en **/etc/cron.daily**, en un editor, p. ej., **/etc/cron.daily/usercount**.

   ```
   [root@desktopX ~]# vim /etc/cron.daily/usercount
   ```

   2.2. Escriba el script que registra la cantidad de usuarios activos en el registro del sistema.

   Inserte lo siguiente en su editor:

   ```
   #!/bin/bash
     USERCOUNT=$(w -h | wc -l)
     logger "There are currently ${USERCOUNT} active users"
   ```

   2.3. Haga el script ejecutable:

   ```
   [root@desktopX ~]# chmod +x /etc/cron.daily/usercount
   ```

3. El paquete *sysstat*, cuando se instala, tiene un trabajo cron que se ejecuta cada 10 minutos, y recopila datos usando un comando denominado **sa1**. Asegúrese de que

este paquete esté instalado, luego cambie este trabajo para que se ejecute cada cinco minutos.

3.1. Asegúrese de que esté instalado el paquete *sysstat*.

```
[root@desktopX ~]# yum -y install sysstat
```

3.2. Averigüe en qué archivo el paquete *sysstat* ha configurado los trabajos **cron**. Los trabajos cron generalmente están configurados en archivos marcados como un archivo de configuración para el administrador de paquetes.

```
[root@desktopX ~]# rpm -qc sysstat
```

/etc/cron.d/sysstat parece prometedor.

3.3. Abra **/etc/cron.d/sysstat** en un editor.

```
[root@desktopX ~]# vim /etc/cron.d/sysstat
```

3.4. Cambie ***/10** en la línea **sa1** a ***/5**.

3.5. Guarde sus cambios y salga.

3.6. Supervise los archivos en **/var/log/sa** para ver cuándo cambian sus tamaños y sellos de tiempo.

```
[root@desktopX ~]# watch ls -l /var/log/sa
```

Administración de archivos temporales

Objetivos

Luego de completar esta sección, los estudiantes deberían poder administrar archivos temporales usando **`systemd-tmpfiles`**.

Administración de archivos temporales con systemd-tmpfiles

Un sistema moderno requiere una gran cantidad de archivos y directorios temporales. No solo los más visibles por el usuario, como **`/tmp`** que son utilizados y abusados por usuarios regulares, sino también los de tareas más específicas, como el daemon y *los directorios volátiles* en **`/run`**. En este contexto, volátil significa que el sistema de archivos que almacena estos archivos solo existe en la memoria. Cuando el sistema vuelva a arrancar o pierda potencia, todo el contenido del almacenamiento volátil desaparecerá.

Para mantener un sistema ejecutándose de forma ordenada, es necesario que estos directorios y archivos se creen cuando no existen, dado que los deamons y scripts podrían contar con que estos estén allí, y que los archivos antiguos se purguen de modo que no puedan llenar espacio en el disco ni proporcionar información errónea.

En el pasado, los administradores de sistemas contaban con paquetes RPM y scripts de SystemV init para crear estos directorios y una herramienta denominada **`tmpwatch`** para eliminar archivos antiguos fuera de uso de los directorios configurados.

En Red Hat Enterprise Linux 7 **`systemd`** proporciona un método más estructurado y configurable para administrar directorios y archivos temporales: **`systemd-tmpfiles`**.

Cuando **`systemd`** inicia un sistema, una de las primeras unidades de servicio iniciadas es **`systemd-tmpfiles-setup`**. Este servicio ejecuta el comando **`systemd-tmpfiles --create --remove`**. Esta comando lee los archivos de configuración de **`/usr/lib/tmpfiles.d/*.conf`**, **`/run/tmpfiles.d/*.conf`** y **`/etc/tmpfiles.d/*.conf`**. Todos los archivos y directorios marcados para la eliminación en esos archivos de configuración se eliminarán, y todos los archivos y directorios marcados para la creación (o arreglos de permisos) se crearán con los permisos correctos si es necesario.

Limpieza regular

Para asegurarse de que los sistemas de ejecución extensa no llenen sus discos con datos viejos, hay también *una unidad de reloj de systemd* que invoca a **`systemd-tmpfiles --clean`** en un intervalo regular.

Las unidades de reloj de **`systemd`** constituyen un tipo especial de servicio de **`systemd`** que tienen un bloque **`[Timer]`** (Reloj) que indica la frecuencia con la que el servicio con el mismo nombre debe iniciarse.

En un sistema Red Hat Enterprise Linux 7, la configuración para la unidad **`systemd-tmpfiles-clean.timer`** se ve así:

```
[Timer]
OnBootSec=15min
```

```
OnUnitActiveSec=1d
```

Esto indica que el servicio con el mismo nombre (**systemd-tmpfiles-clean.service**) se iniciará 15 minutos después de que **systemd** se haya iniciado, y una vez cada 24 horas de allí en adelante.

El comando **systemd-tmpfiles --clean** analiza los mismos archivos de configuración que el **systemd-tmpfiles --create**, pero en lugar de crear archivos y directorios, purgará todos los archivos a los que no se haya accedido, y que no hayan sido modificados ni cambiados en una fecha anterior a la antigüedad máxima definida en el archivo de configuración.

Importante

La página del manual **tmpfiles.d**(5) declara que los archivos "más antiguos" que la antigüedad que figura en el campo de fecha se eliminan. Eso no es exactamente cierto.

Los archivos en un sistema de archivos Linux que cumplen el estándar POSIX tienen tres sellos de tiempo: **atime**, la última vez que se accedió al archivo; **mtime**, la última vez que se modificó el contenido del archivo; y **ctime**, la última vez que se modificó el estado del archivo (por **chown**, **chmod** y así sucesivamente). La mayoría de los sistemas de archivos Linux no tiene un sello de tiempo de creación. Esto es común en sistemas de archivos similares a Unix.

Los archivos se considerarán no utilizados si *los tres* sellos de tiempo son anteriores a la configuración de la antigüedad de **systemd-tmpfiles**. Si *cualquiera* de los tres sellos de tiempo es anterior a la configuración de antigüedad, el archivo no será eliminado debido a la antigüedad por **systemd-tmpfiles**.

El comando **stat** se puede ejecutar en un archivo para ver los valores de sus tres sellos de tiempo. El comando **ls -l** normalmente muestra **mtime**.

Archivos de configuración systemd-tmpfiles

El formato de los archivos de configuración para **systemd-tmpfiles** se detalla en la página del manual **tmpfiles.d**(5).

La sintaxis básica consta de siete columnas: Type (Tipo), Path (Ruta), Mode (Modo), UID, GID, Age (Antigüedad) y Argument (Argumento). Tipo se refiere a la acción que debe realizar **systemd-tmpfiles**; por ejemplo, **d** para crear un directorio si no existe aún, o **Z** para restaurar recursivamente contextos de SELinux y propiedad y permisos de archivos.

Algunos ejemplos con explicaciones:

```
d /run/systemd/seats 0755 root root -
```

Al crear archivos y directorios, cree el directorio **/run/systemd/seats** si aún no existe, propiedad del usuario **raíz** y el grupo **raíz**, con permisos establecidos para **rwxr-xr-x**. Este directorio no se purgará automáticamente.

```
D /home/student 0700 student student 1d
```

Cree el directorio **/home/student** si aún no existe. Si existe, vacíe todos los contenidos. Cuando **systemd-tmpfiles --clean** se ejecute, elimine todos los archivos a los que no se haya accedido, ni se hayan modificado ni cambiado en más de un día.

```
L /run/fstablink - root root - /etc/fstab
```

Cree el enlace simbólico **/run/fstablink** que apunte a **/etc/fstab**. Nunca purgue automáticamente esta línea.

Precedencia de archivos de configuración
Los archivos de configuración pueden estar en tres lugares:

- **/etc/tmpfiles.d/*.conf**
- **/run/tmpfiles.d/*.conf**
- **/usr/lib/tmpfiles.d/*.conf**

Los archivos en **/usr/lib/tmpfiles.d/** son proporcionados por los paquetes de RPM relevantes, y no deben ser editados por los administradores del sistema. Los archivos en **/run/tmpfiles.d/** son en sí mismos archivos volátiles, normalmente usados por daemons para administrar sus propios archivos temporales de tiempo de ejecución, y los archivos en **/etc/tmpfiles.d/** están diseñados para que los administradores configuren ubicaciones temporales personalizadas y para reemplazar los valores predeterminados proporcionados por el proveedor.

Si un archivo en **/run/tmpfiles.d/** tiene el mismo nombre de archivo que un archivo en **/usr/lib/tmpfiles.d/**, se usará el archivo en **/run/tmpfiles.d/**. Si un archivo en **/etc/tmpfiles.d/** tiene el mismo nombre de archivo que un archivo en **/run/tmpfiles.d/** o **/usr/lib/tmpfiles.d/**, se usará el archivo en **/etc/tmpfiles.d/**.

Dadas estas reglas de precedencia, un administrador puede reemplazar fácilmente la configuración proporcionada por el proveedor si *copia* el archivo relevante en **/etc/tmpfiles.d/**, y luego lo edita. Trabajar de esta manera garantiza que la configuración proporcionada por el administrador se puede administrar fácilmente desde un sistema de administración de configuración central, y que no se sobrescriba por una actualización de un paquete.

nota

Al evaluar configuraciones nuevas o modificadas, puede ser útil solo aplicar los comandos fuera de un archivo de configuración. Esto se puede lograr si se especifica el nombre del archivo de configuración en la línea de comandos.

Referencias

Páginas del manual: **systemd-tmpfiles**(8), **tmpfiles.d**(5), **stat**(1), **stat**(2) y **systemd.timer**(5).

Práctica: Administración de archivos temporales

En este trabajo de laboratorio, configurará su sistema para purgar archivos de una antigüedad superior a 5 días desde **/tmp**. También agregará un nuevo directorio temporal denominado **/run/gallifrey** para que se cree automáticamente, y los archivos que han estado en desuso durante más de 30 segundos se purgarán automáticamente.

Recursos	
Archivos:	• **/etc/tmpfiles.d/** • **/usr/lib/tmpfiles.d/tmp.conf**
Máquinas:	**serverX**

Resultados:
Un nuevo directorio temporal denominado **/run/gallifrey**, configurado para el purgado automático, y una configuración de purgado modificada para **/tmp**.

Andes de comenzar
Restablezca su sistema **serverX**.

En producción, se han presentado varios problemas:

- **/tmp** se queda sin espacio en disco. Parece que permitir que los archivos estén 10 días en desuso antes de eliminarlos no es adecuado para su sitio. Ha determinado que eliminar archivos luego de cinco días de desuso es aceptable.
- Su deamon de búsqueda de desplazamiento del tiempo **gallifrey** necesita un directorio temporal por separado denominado **/run/gallifrey**. Los archivos en este directorio deben purgarse automáticamente luego de haber estado en desuso durante más de 30 segundos. Solo **raíz** debe tener acceso de lectura y escritura a **/run/gallifrey**.

1. **/tmp** está bajo el control de **systemd-tmpfiles**. Para anular la configuración upstream, copie **/usr/lib/tmpfiles.d/tmp.conf** en **/etc/tmpfiles.d/**.

   1.1.
   ```
   [student@serverX ~]$ sudo cp /usr/lib/tmpfiles.d/tmp.conf /etc/tmpfiles.d/
   ```

2. Encuentre la línea en **/etc/tmpfiles.d/tmp.conf** que controla el intervalo de purgado para **/tmp**, y cambie el intervalo de **10d** a **5d**.

   2.1. Abra **/etc/tmpfiles.d/tmp.conf** en un editor y haga el cambio; o bien, haga lo siguiente:

   ```
   [student@serverX ~]$ sudo sed -i '/^d .tmp /s/10d/5d/' /etc/tmpfiles.d/tmp.conf
   ```

3. Evalúe si **systemd-tmpfiles --clean** acepta la nueva configuración.

   ```
   [student@serverX ~]$ sudo systemd-tmpfiles --clean tmp.conf
   ```

4. Cree un nuevo archivo de configuración **/etc/tmpfiles.d/gallifrey.conf** con el siguiente contenido:

```
# Set up /run/gallifrey, owned by root with 0700 permissions
# Files not used for 30 seconds will be automatically deleted
d /run/gallifrey 0700 root root 30s
```

5. Evalúe su nueva configuración para crear **/run/gallifrey**.

5.1.
```
[student@serverX ~]$ sudo systemd-tmpfiles --create gallifrey.conf
```

5.2.
```
[student@serverX ~]$ ls -ld /run/gallifrey
drwx------. 2 root root Feb 19  10:29 /run/gallifrey
```

6. Evalúe el purgado de su directorio **/run/gallifrey**.

6.1. Cree un archivo nuevo en **/run/gallifrey**.

```
[student@serverX ~]$ sudo touch /run/gallifrey/companion
```

6.2. Espere al menos 30 segundos.

```
[student@serverX ~]$ sleep 30s
```

6.3. Haga que **systemd-tmpfiles** limpie el directorio de **/run/gallifrey**.

```
[student@serverX ~]$ sudo systemd-tmpfiles --clean gallifrey.conf
```

6.4. Inspeccione el contenido de **/run/gallifrey**.

```
[student@serverX ~]$ sudo ls -l /run/gallifrey
```

Evaluación del capítulo: Programación de tareas futuras en Linux

Relacione las descripciones con los trabajos **`cron`** o **`at`** relevantes.

Cada miércoles a las 12:30 p. m.

El próximo jueves a las 5:00 p. m.

El próximo miércoles a las 12:30 p. m.

Luego de la medianoche todos los lunes y cada 1.° de mes.

Temprano en la mañana de Navidad

Todos los jueves a las 5:00 p. m.

Trabajo	Descripción del momento
`30 6 25 12 * /usr/local/bin/open_presents`	
`30 12 * * 3 reboot`	
`0 17 * * 4 rm -rf /home/student`	
`echo reboot | at 12:30 wednesday`	

Trabajo	Descripción del momento
`3 0 1 * 1 /sbin/dump 0uf / dev/st0 /home`	
`echo "userdel -r student" | at 17:00 thursday`	

Solución

Relacione las descripciones con los trabajos **cron** o **at** relevantes.

Trabajo	Descripción del momento
`30 6 25 12 * /usr/local/bin/open_presents`	Temprano en la mañana de Navidad
`30 12 * * 3 reboot`	Cada miércoles a las 12:30 p. m.
`0 17 * * 4 rm -rf /home/student`	Todos los jueves a las 5:00 p. m.
`echo reboot | at 12:30 wednesday`	El próximo miércoles a las 12:30 p. m.
`3 0 1 * 1 /sbin/dump 0uf /dev/st0 /home`	Luego de la medianoche todos los lunes y cada 1.° de mes.
`echo "userdel -r student" | at 17:00 thursday`	El próximo jueves a las 5:00 p. m.

Resumen

Programación de tareas únicas con at

- **`at`** programa trabajos futuros.
- **`atq`** detalla trabajos programados.
- **`at -c`** inspecciona trabajos programados.
- **`atrm`** elimina trabajos futuros programados.

Programación de trabajos recurrentes con cron

- **`crontab -e`** edita un usuario crontab.
- Seis columnas en un crontab: Minutes (Minutos), Hours (Horas), Day-of-Month (Día-del-mes), Month (Mes), Day-of-Week (Día-de-semana) y Command (Comando).

Programación de trabajos cron del sistema

- Los crontabs del sistema tienen una columna adicional: **`Username`** (Nombre de usuario).
- Los archivos de crontab del sistema en **`/etc/crontab`** y **`/etc/cron.d/*`**.
- Scripts controlados por **`/etc/anacrontab`** en **`/etc/cron.{hourly,daily,weekly,monthly}/`**.

Administración de archivos temporales

- **`systemd-tmpfiles`** se utiliza para administrar archivos temporales y almacenamiento volátil.
- Invocado durante el arranque desde **`systemd-tmpfiles-setup.service`**.
- Invocado a intervalos regulares desde **`systemd-tmpfiles-clean.timer`**.
- Configurado desde **`/usr/lib/tmpfiles.d/*.conf`** y **`/etc/tmpfiles.d/*conf`**.
- Los archivos en **`/etc/tmpfiles.d/`** tienen prioridad frente a archivos denominados de forma similar en **`/usr/lib/tmpfiles.d/`**.

redhat. TRAINING

CAPÍTULO 5

ADMINISTRACIÓN DE LA PRIORIDAD DE LOS PROCESOS DE LINUX

Descripción general	
Meta	Influir en las prioridades relativas según las cuales se ejecutan los procesos de Linux.
Objetivos	• Describir niveles de nice. • Establecer niveles de nice sobre procesos nuevos y existentes.
Secciones	• Conceptos de prioridades de procesos y de "nice" (y práctica) • Uso de nice y renice para influir en la prioridad de procesos (y práctica)
Trabajo de laboratorio	• Administración de la prioridad de los procesos de Linux

Conceptos de prioridad y "nice" de procesos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder describir *niveles* nice y sus efectos.

Programación y multitareas de procesos de Linux

Los sistemas de computación modernos tienen una variedad de procesadores que incluyen desde procesadores económicos, que solo pueden ejecutar una única instrucción a la vez, hasta supercomputadoras de alto rendimiento con cientos de CPU cada una y múltiples núcleos en cada CPU, que realizan cientos de instrucciones en paralelo. Pero todos estos sistemas tienden a tener una cosa en común: siempre deben ejecutar más procesos que la cantidad de núcleos que tienen realmente.

La manera en que Linux (y otros sistemas operativos) pueden realmente ejecutar más procesos (y subprocesos) que la cantidad de unidades de procesamiento reales disponibles es mediante el empleo de una técnica denominada *particionamiento de tiempo*. El programador de procesos *del sistema operativo* cambiará rápidamente entre procesos en un único núcleo, lo que le da al usuario la impresión de que hay más procesos ejecutándose al mismo tiempo.

La parte del kernel de Linux que realiza este intercambio se denomina *programador de procesos*.

Prioridades relativas

Dado que todos los procesos tienen distinta importancia, se le puede indicar al programador que use diferentes políticas de programación para diferentes procesos. La política de programación usada para la mayoría de los procesos que se ejecutan en un sistema regular se denomina **`SCHED_OTHER`** (también denominada **`SCHED_NORMAL`**), pero hay otras políticas disponibles según el propósito.

Debido a que no todos los procesos se crean de igual manera, a los procesos que se ejecutan con la política **`SCHED_NORMAL`** se les puede dar una prioridad relativa. Esta prioridad se denomina *nivel* nice de un proceso, y hay exactamente **`40`** niveles nice diferentes que un proceso puede tener.

Estos niveles nice varían desde **`-20`** hasta **`19`**. De forma predeterminada, los procesos heredarán su nivel nice de su proceso principal, que generalmente es **`0`**. Los niveles nice más altos indican menos prioridad (el proceso abandona fácilmente el uso de la CPU para otros), mientras que los niveles nice más bajos indican una mayor prioridad (el proceso tiene menos tendencia a abandonar el uso de la CPU). Si no hay disputa por recursos (por ejemplo, cuando hay menos procesos activos que núcleos de la CPU disponibles), incluso los procesos con un nivel nice alto usarán todos los recursos de la CPU disponibles que puedan. Pero cuando hay más procesos que solicitan tiempo de CPU que núcleos disponibles, los procesos con un nivel nice más alto recibirán menos tiempo de la CPU que aquellos con un nivel nice más bajo.

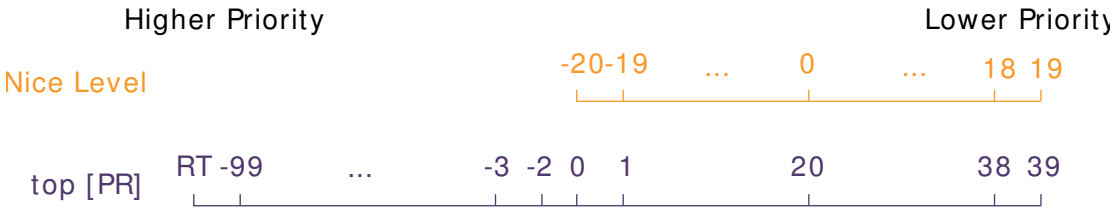

Figura 5.1: Niveles nice y cómo se informan por el comando top

Niveles nice y permisos

Dado que establecer un nivel nice bajo en un proceso que requiere mucha CPU podría afectar de forma negativa el rendimiento de otros procesos que se ejecutan en el mismo sistema, solo **`raíz`** (más detallado: usuarios con la capacidad **`CAP_SYS_NICE`**) tiene permitido establecer niveles nice negativos y disminuir el nivel nice en procesos existentes.

Los usuarios regulares sin privilegios solo tienen permitido establecer niveles nice positivos. Asimismo, solo tienen permitido *elevar* el nivel nice en sus procesos existentes, pero no pueden *disminuirlo*.

Importante

Además de los niveles nice, existen otras maneras de influir en la prioridad de los procesos y el uso de recursos. Hay configuraciones y políticas de programadores alternativas, *grupos de control* (**`cgroups`**), y más. Sin embargo, los niveles nice son los más fáciles de usar y pueden ser usados por usuarios regulares así como por administradores de sistemas.

Referencias

Páginas del manual: **`nice`**(1), **`sched_setscheduler`**(2)

Práctica: Conceptos de prioridad de procesos y de "nice"

Relacione los siguientes elementos con su descripción en la tabla.

Nivel nice alto	Nivel nice negativo	Usuarios regulares
`de -20 a +19`	`raíz`	

Descripción	Elemento
Estos tipos de procesos abandonan fácilmente sus recursos de la CPU para otros.	
Estos tipos de procesos intentan mantener el uso de la CPU para sí mismos.	
No pueden asignar niveles de nice negativos	
Pueden cambiar el nivel de nice de procesos que pertenecen a otros usuarios	
El intervalo completo de niveles nice	

Solución

Relacione los siguientes elementos con su descripción en la tabla.

Descripción	Elemento
Estos tipos de procesos abandonan fácilmente sus recursos de la CPU para otros.	Nivel nice alto
Estos tipos de procesos intentan mantener el uso de la CPU para sí mismos.	Nivel nice negativo
No pueden asignar niveles de nice negativos	Usuarios regulares
Pueden cambiar el nivel de nice de procesos que pertenecen a otros usuarios	**raíz**
El intervalo completo de niveles nice	**de -20 a +19**

Uso de nice y del cambio del valor de nice para influir en la prioridad de procesos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Iniciar procesos con un nivel nice establecido.
- Modificar el nivel nice en un proceso en ejecución.
- Informar niveles nice de procesos.

Informe de niveles nice

Los niveles nice para procesos existentes se pueden visualizar de varias maneras. La mayoría de las herramientas de administración de procesos (como **gnome-system-monitor**) ya muestra el nivel nice de forma predeterminada, o se puede configurar para mostrar el nivel nice.

Visualización de niveles nice con el comando top

El comando **`top`** se puede usar para visualizar (y administrar) procesos de forma interactiva. En una configuración predeterminada, **`top`** mostrará dos columnas de interés para el nivel nice: **`NI`**, con el nivel nice real, y **`PR`**, que muestra el nivel nice según se asignó a una cola de prioridades más grande, con un nivel nice de **`-20`** que se asigna a una prioridad de **`0`** y un nivel nice de **`+19`** que se asigna a una prioridad de **`39`**.

Visualización de niveles nice con el comando ps

El comando **`ps`** también puede mostrar niveles nice para procesos, aunque no lo hace en la mayoría de sus formatos de resultados predeterminados. Sin embargo, los usuarios pueden solicitar exactamente las columnas que desean a **`ps`**, y el nombre del campo de nice es **`nice`**.

En el siguiente ejemplo, se solicita una lista de todos los procesos, con su pid, nombre y nivel nice, ordenada de forma descendente por nivel nice:

```
[student@desktopX ~]$ ps axo pid,comm,nice --sort=-nice
  PID COMMAND          NI
   74 khugepaged       19
  688 alsactl          19
 1953 tracker-miner-f  19
   73 ksmd              5
  714 rtkit-daemon      1
```

Importante

Algunos procesos podrían informar un **-** como su nivel nice. Estos procesos se ejecutan con una política de programación diferente, y casi con certeza el programador los considerará con una prioridad más alta. Es posible mostrar la política del programador si se solicita el campo **cls** de **ps**. Un **TS** en este campo indica que el proceso se ejecuta bajo **SCHED_NORMAL** y puede usar niveles nice; todo lo demás significa que se está usando una política de programador diferente.

Inicio de procesos con un nivel nice diferente

Cada vez que se inicia un proceso, normalmente heredará el nivel nice de su proceso principal. Esto significa que cuando un proceso se inicia desde la línea de comandos, obtendrá el mismo nivel nice que el proceso del shell desde donde se inició. En la mayoría de los casos, esto generará en nuevos procesos que se ejecutarán con un nivel nice de **0**.

Para iniciar un proceso con un nivel diferente, tanto los usuarios como los administradores de sistemas pueden ejecutar sus comandos usando la herramienta **nice**. Sin ninguna otra opción, ejecutar **nice *<COMMAND>*** iniciará ***<COMMAND>*** con un nivel nice de **10**. Otros niveles se pueden seleccionar al usar la opción **-n *<NICELEVEL>*** para el comando **nice**. Por ejemplo, para iniciar el comando **dogecoinminer** con un nivel nice de **15** y enviarlo a segundo plano inmediatamente, se puede usar el siguiente comando:

```
[student@desktopX ~]$ nice -n 15 dogecoinminer &
```

Importante

Los usuarios sin privilegios solo tienen permitido establecer un nivel nice positivo (de **0** a **19**). Solo **raíz** puede establecer un nivel nice negativo (de **-20** a **-1**).

Cambio del nivel nice de un proceso existente

El nivel nice de un proceso existente se puede cambiar desde la línea de comandos con el comando **renice**. La sintaxis para el comando **renice** es la siguiente:

renice -n *<NICELEVEL>* *<PID>*...

Por ejemplo, para cambiar el nivel nice de todos los procesos de **origami@home** a **-7**, un administrador de sistemas podría usar el siguiente comando (observe que se puede especificar más de un PID a la vez):

```
[root@desktopX ~]# renice -n -7 $(pgrep origami@home)
```

Importante

Los usuarios regulares solo tienen permitido *elevar* el nivel nice en sus procesos. Solo **raíz** puede usar **renice** para disminuir el nivel nice.

El comando **top** también se puede usar para cambiar (interactivamente) el nivel nice de un proceso. En **top**, presione **r**, seguido del PID que se cambiará y el nuevo nivel nice.

Referencias

Páginas del manual: **nice**(1), **renice**(1), **top**(1)

Práctica: Detección de prioridades de procesos

En este ejercicio, experimentará la influencia que los niveles nice tienen en prioridades de procesos relativas.

Recursos	
Máquinas:	**desktopX**

Resultados:
Un recorrido interactivo de los efectos de niveles nice.

Andes de comenzar
Ninguno

1. Inicie sesión como **student** en su sistema **desktopX**.

2. Mediante el uso del archivo especial **/proc/cpuinfo**, determine la cantidad de núcleos de CPU de su sistema **desktopX**, y luego, inicie *dos* instancias del comando **sha1sum /dev/zero &** para cada núcleo.

   2.1. Para determinar la cantidad de núcleos que usan **/proc/cpuinfo**:

   ```
   [student@desktopX ~]$ NCORES=$( grep -c '^processor' /proc/cpuinfo )
   ```

   2.2. Ya sea manualmente o con un script, inicie dos comandos **sha1sum /dev/zero &** para cada núcleo en su sistema.

nota

El comando **seq** imprime una lista de números.

```
[student@desktopX ~]$ for I in $( seq $((NCORES*2)) )
> do
>  sha1sum /dev/zero &
> done
```

3. Verifique que tenga todos los trabajos en segundo plano en ejecución que esperaba (dos para cada núcleo de su sistema).

   3.1.

   ```
   [student@desktopX ~]$ jobs
   [1]-  Running                 sha1sum /dev/zero &
   [2]+  Running                 sha1sum /dev/zero &
   ...
   ```

4. Inspeccione el uso de la CPU (como porcentaje) de todos sus procesos **sha1sum**, usando los comandos **ps** y **pgrep**. ¿Qué observó?

4.1.
```
[student@desktopX ~]$ ps u $(pgrep sha1sum)
```

4.2. El porcentaje de la CPU para todos los procesos **sha1sum** es aproximadamente igual.

5. Use el comando **killall** para finalizar todos los procesos **sha1sum**.

5.1.
```
[student@desktopX ~]$ killall sha1sum
```

6. Inicie dos comandos **sha1sum /dev/zero &** para cada uno de sus núcleos, pero dé exactamente a uno de ellos un nivel nice de **10**.

6.1.
```
[student@desktopX ~]$ for I in $( seq $((NCORES*2-1)) )
> do
>  sha1sum /dev/zero &
> done
[student@desktopX ~]$ nice -n 10 sha1sum /dev/zero &
```

7. Mediante el uso del comando **ps**, inspeccione el uso de la CPU de sus comandos **sha1sum**. Asegúrese de incluir el nivel nice en su resultado, así como el PID y el uso de la CPU. ¿Qué observó?

7.1.
```
[student@desktopX ~]$ ps -o pid,pcpu,nice,comm $(pgrep sha1sum)
```

7.2. La instancia de **sha1sum** con el nivel nice de **10** obtiene significativamente menos CPU que otras instancias.

8. Use el comando **renice** para establecer el nivel nice de **sha1sum** con un nivel nice de **10** hasta **5**. El PID debería aún estar visible en el resultado del paso anterior.

¿Funcionó? ¿Por qué no?

8.1.
```
[student@desktopX ~]$ renice -n 5 <PID>
renice: failed to set priority for <PID> (process ID): Permission denied
```

8.2. Los usuarios sin privilegios no tienen permitido establecer valores nice negativos ni disminuir el valor nice de un proceso existente.

9. Mediante el uso de los comandos **sudo** y **renice**, establezca el nivel nice del proceso que identificó en el paso anterior en **-10**.

9.1.
```
[student@desktopX ~]$ sudo renice -n -10 <PID>
```

10. Inicie el comando **top** como **raíz**, luego use **top** para disminuir el nivel nice del proceso **sha1sum** que usa la mayoría de la CPU hasta **0**. ¿Qué observa luego de esto?

10.1
```
[student@desktopX ~]$ sudo top
```

10.2 Identifique el proceso **sha1sum** que usa la mayoría de la CPU. Está cerca de la parte superior de la pantalla.

10.3 Presione **r** para ingresar *en el modo renice* y, luego, ingrese el PID que identificó o presione **Enter** si el PID predeterminado ofrecido es el que desea.

10.4 Ingrese **0**, luego presione **Enter**.

10.5 Todos los comandos **sha1sum** están una vez más usando una cantidad (casi) igual de la CPU.

11. **Importante**: Limpie todo al salir de **top** y al eliminar todos sus procesos **sha1sum**.

11.1 Presione **q** para salir de **top**.

11.2
```
[student@desktopX ~]$ killall sha1sum
```

Trabajo de laboratorio: Administración de la prioridad de los procesos de Linux

En este trabajo de laboratorio, buscará procesos con alto consumo de la CPU y ajustará los niveles de nice.

Recursos	
Archivos:	`/usr/local/bin/lab nice`
Máquinas:	`desktopX`

Resultados:
El nivel nice de los principales consumidores de la CPU ajustado para que se desempeñen bien con otros.

Andes de comenzar

- Restablezca su sistema **`desktopX`**.
- Inicie sesión en su sistema **`desktopX`** y configúrelo.

```
[student@desktopX ~]$ lab nice setup
```

1. Mediante el uso de **`top`** o **`ps`**, identifique los dos principales consumidores de la CPU en su sistema **`desktopX`**. Si **`gnome-shell`** se encuentra entre los dos principales, ignórelo y tome el siguiente proceso más alto. Asegúrese de tomar nota de los id. de estos dos procesos.
2. Desde la línea de comandos, configure el nivel nice de los procesos que halló en el paso anterior en **`10`**.
3. Clasifique su trabajo mediante la ejecución del siguiente comando:

```
[student@desktopX ~]$ lab nice grade
```

4. **Limpieza importante**: Cuando haya clasificado satisfactoriamente su trabajo, ejecute el siguiente comando para limpiarlo:

```
[student@desktopX ~]$ lab nice clean
```

Solución

En este trabajo de laboratorio, buscará procesos con alto consumo de la CPU y ajustará los niveles de nice.

Recursos	
Archivos:	**/usr/local/bin/lab nice**
Máquinas:	**desktopX**

Resultados:
El nivel nice de los principales consumidores de la CPU ajustado para que se desempeñen bien con otros.

Andes de comenzar

- Restablezca su sistema **desktopX**.
- Inicie sesión en su sistema **desktopX** y configúrelo.

```
[student@desktopX ~]$ lab nice setup
```

1. Mediante el uso de **top** o **ps**, identifique los dos principales consumidores de la CPU en su sistema **desktopX**. Si **gnome-shell** se encuentra entre los dos principales, ignórelo y tome el siguiente proceso más alto. Asegúrese de tomar nota de los id. de estos dos procesos.

   1.1. Ejecute **top** y tome nota de los dos procesos principales, o bien ejecute lo siguiente:

   ```
   [student@desktopX ~]$ ps aux --sort=pcpu
   ```

   Al usar la versión **ps**, los principales consumidores de la CPU estarán en la parte inferior, con sus PID detallados en la segunda columna.

2. Desde la línea de comandos, configure el nivel nice de los procesos que halló en el paso anterior en **10**.

   2.1.
   ```
   [student@desktopX ~]$ sudo renice -n 10 <PROCESSPID1> <PROCESSPID2>
   ```

   Asegúrese de reemplazar ***<PROCESSPID1>*** y ***<PROCESSPID2>*** con el id. del proceso que identificó en el paso anterior.

3. Clasifique su trabajo mediante la ejecución del siguiente comando:

   ```
   [student@desktopX ~]$ lab nice grade
   ```

4. **Limpieza importante**: Cuando haya clasificado satisfactoriamente su trabajo, ejecute el siguiente comando para limpiarlo:

```
[student@desktopX ~]$ lab nice clean
```

Resumen

Conceptos de prioridad y "nice" de procesos

- Todos los procesos de un sistema Linux tienen prioridad relativa.
- El *nivel nice* de un proceso influye en su prioridad.

Uso de nice y del cambio del valor de nice para influir en la prioridad de procesos

- **`nice`** se usa para configurar el nivel nice para procesos nuevos.
- **`renice`** y **`top`** se pueden usar para modificar el nivel nice de un proceso existente.
- Tanto **`ps`** como **`top`** se pueden usar para informar niveles nice.

redhat. TRAINING

CAPÍTULO 6

CONTROL DE ACCESO A ARCHIVOS CON LISTAS DE CONTROL DE ACCESO (ACL)

Descripción general	
Meta	Administrar la seguridad de los archivos utilizando listas de control de acceso (ACL) POSIX.
Objetivos	• Describir listas de control de acceso POSIX. • Administrar listas de control de acceso POSIX.
Secciones	• Listas de control de acceso (ACL) POSIX (y práctica) • Protección de archivos con ACL (y práctica)
Trabajo de laboratorio	• Control de acceso a archivos con listas de control de acceso (ACL)

Listas de control de acceso (ACL) POSIX

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Describir opciones de montaje de ACL y sistemas de archivos.
- Ver e interpretar ACL con **`ls`** y **`getfacl`**, y describir la máscara de ACL y la precedencia de permisos de ACL.

Conceptos de listas de control de acceso

Los permisos de archivos Linux estándar son correctos para la mayoría de las situaciones, pero tienen limitaciones. Los permisos que restringen el acceso a un archivo se limitan al propietario del archivo, membresía de un único grupo o todos los demás. Es posible que no sea adecuado para el proceso (un programa en ejecución) ser un miembro del grupo propietario del archivo, y aún menos deseable otorgar permiso a todos.

Las ACL permiten la asignación de permisos detallados a un archivo. Se pueden otorgar permisos a los usuarios o a los grupos nombrados, así como a los usuarios y a los grupos identificados por un UID o GUID, además de los permisos estándares de *propietario del archivo*, *propietario de grupo*, y *otros* permisos de archivo. Se aplican las mismas marcas de permiso: **`r`**, leer; **`w`**, escribir; y **`x`**, ejecutar (en los archivos, buscar directorios).

El propietario del archivo puede establecer ACL en archivos o directorios individuales. Los nuevos archivos y subdirectorios pueden heredar automáticamente la configuración de ACL de las ACL *predeterminadas* del directorio principal, si están configuradas. Al igual que las reglas de acceso a archivos normales, la jerarquía del directorio principal necesitará al menos el *otro* conjunto de permisos de ejecución para habilitar el acceso de usuarios y grupos nombrados.

Opción de montaje de sistema de archivos
El sistema de archivos debe montarse con el soporte para ACL habilitado. Los sistemas de archivos XFS tienen soporte para ACL incorporado. Los sistemas de archivos Ext4 creados en Red Hat Enterprise Linux 7 tienen la opción **`acl`** habilitada de forma predeterminada, pero es posible que los sistemas de archivos ext4 creados en versiones anteriores de Red Hat Enterprise Linux necesiten que se incluya la opción **`acl`** con la solicitud de montaje, o configurada en el superbloqueo.

Visualización e interpretación de permisos de ACL

El comando **`ls -l`** solo produce detalles de configuración de ACL mínimos:

```
[student@serverX steamies]$ ls -l roster.txt
-rwxrw----+ 1 student controller 130 Mar 19 23:56 roster.txt
```

El "**+**" al final de la secuencia de permiso de 10 caracteres indica que hay configuraciones de ACL asociadas con este archivo. Las marcas "**rwx**" de *usuario*, *grupo* y *otras* se deben interpretar del siguiente modo:

- **usuario:** muestra la configuración de ACL del *usuario*, que es la misma que la configuración de archivos del *usuario* estándar; **`rwx`**.

- **grupo:** muestra la configuración de la *máscara* de ACL, no la configuración del *propietario del grupo*; **rw**.
- **otro:** muestra la configuración de ACL de *otro*, que es la misma que la configuración de archivos de *otro* estándar; sin acceso.

Importante

Si se modifican los permisos del grupo en un archivo con ACL mediante el uso de **chmod**, no se modifican los permisos del propietario del grupo, pero sí se modifica la máscara de ACL. Use **setfacl -m g::*perms file*** si lo que intenta es actualizar los permisos del propietario del grupo de archivos.

Ver ACL de archivos

Para visualizar la configuración de ACL en un archivo, use **getfacl *file***:

```
[student@serverX steamies]$ getfacl roster.txt
# file: roster.txt
# owner: student
# group: controller
user::rwx
user:james:---
user:1005:rwx       #effective:rw-
group::rwx          #effective:rw-
group:sodor:r--
group:2210:rwx      #effective:rw-
mask::rw-
other::---
```

Dé un vistazo a cada sección del ejemplo anterior:

Abrir entradas de comentarios:

```
# file: roster.txt
# owner: student
# group: controller
```

Las primeras tres líneas son comentarios que identifican el nombre del archivo, el propietario (**student**) y el propietario del grupo (**controller**). Si hay marcas de archivos adicionales (por ejemplo, **setuid** o **setgid**), aparecerá una cuarta línea de comentarios que muestra las marcas establecidas.

Entradas de usuarios:

```
user::rwx                          (1)
user:james:---                     (2)
user:1005:rwx       #effective:rw- (3)
```

(1) Permisos del propietario de archivos. **student** tiene **rwx**.

(2) Permisos de usuarios nombrados. Una entrada para cada usuario nombrado asociado con este archivo. **james** NO tiene permisos.

3. Permisos de usuarios nombrados. El UID **1005** tiene **rwx**, pero la máscara limita los permisos efectivos a **rw** solamente.

Entradas de grupos:

```
group::rwx          #effective:rw-  (1)
group:sodor:r--                     (2)
group:2210:rwx      #effective:rw-  (3)
```

1. Permisos de propietario de grupo. **controller** tiene **rwx**, pero la máscara limita los permisos efectivos a **rw** solamente.
2. Permisos de grupos nombrados. Una entrada para cada grupo nombrado asociado con este archivo. **sodor** tiene **r** solamente.
3. Permisos de grupos nombrados. El GID **2210** tiene **rwx**, pero la máscara limita los permisos efectivos a **rw** solamente.

Entrada de la máscara:

```
mask::rw-
```

La configuración de la máscara muestra los máximos permisos posibles para todos los usuarios nombrados, el propietario del grupo y los grupos nombrados. El UID **1005**, **controller** y el GID **2210** no pueden ejecutar este archivo, aunque cada entrada tenga establecido el permiso de ejecución.

Otra entrada:

```
other::---
```

Otro permiso o permisos "mundiales". Todos los demás UID y GID NO tienen permisos.

Ver ACL de directorios

Para visualizar la configuración de ACL en un directorio, use **getfacl *~/directory***:

```
[student@serverX steamies]$ getfacl .
# file: .
# owner: student
# group: controller
# flags: -s-
user::rwx
user:james:---
user:1005:rwx
group::rwx
group:sodor:r-x
group:2210:rwx
mask::rwx
other::---
default:user::rwx
default:user:james:---
default:group::rwx
default:group:sodor:r-x
default:mask::rwx
default:other::---
```

Dé un vistazo a cada sección del ejemplo anterior:

Abrir entradas de comentarios:

```
# file: .
# owner: student
# group: controller
# flags: -s-
```

Las primeras tres líneas son comentarios que identifican el nombre del directorio, el propietario (**student**) y el propietario del grupo (**controller**). Si hay marcas de directorio adicionales (**setuid**, **setgid**, **sticky**), aparecerá una cuarta línea de comentario mostrando las marcas establecidas (en este caso, **setgid**).

Entradas de ACL estándares:

```
user::rwx
user:james:---
user:1005:rwx
group::rwx
group:sodor:r-x
group:2210:rwx
mask::rwx
other::---
```

Los permisos de ACL en este directorio son los mismos que los del archivo del ejemplo anterior, pero se aplican al directorio. La diferencia clave es la inclusión del permiso de ejecución en estas entradas (cuando corresponda) para habilitar el permiso de búsqueda del directorio.

Entradas del usuario predeterminadas:

```
default:user::rwx                    (1)
default:user:james:---               (2)
```

1. Permisos de ACL del propietario del archivos predeterminados. El propietario del archivo obtendrá **rwx**, lectura/escritura en archivos nuevos y ejecución en subdirectorios nuevos.
2. Permisos de ACL de usuarios nombrados predeterminados. Una entrada para cada usuario nombrado que obtendrá automáticamente ACL predeterminadas aplicadas a archivos o subdirectorios nuevos. **james**, de forma predeterminada, NO tendrá permisos.

Entradas del grupo predeterminadas:

```
default:group::rwx                   (1)
default:group:sodor:r-x              (2)
```

1. Permisos de ACL del propietario del grupo predeterminados. El propietario del grupo de archivos obtendrá **rwx**, lectura/escritura en archivos nuevos y ejecución en subdirectorios nuevos.
2. Permisos de ACL del grupo nombrado predeterminados. Una entrada para cada grupo nombrado que obtendrá automáticamente ACL predeterminadas. **sodor** obtendrá **rx**, lectura/escritura en archivos nuevos y ejecución en subdirectorios nuevos.

Entrada de la máscara ACL predeterminada:

```
default:mask::rwx
```

La configuración de la máscara predeterminada muestra los permisos máximos iniciales posibles para todos los archivos y directorios nuevos creados que tienen ACL de usuarios nombrados, ACL del propietario del grupo o ACL de grupos nombrados: lectura y escritura para archivos nuevos y permiso de ejecución en subdirectorios nuevos; los archivos nuevos nunca obtienen permiso de ejecución.

Entrada de otro predeterminada:

```
default:other::---
```

Permisos "mundiales" o de *otro* predeterminados. Todos los demás UID y GID NO tienen permisos para archivos nuevos o subdirectorios nuevos.

Las entradas *predeterminadas* del ejemplo anterior no incluyen el usuario nombrado (UID **1005**) ni el grupo nombrado (GID **2210**); consecuentemente, no obtendrán entradas de ACL iniciales automáticamente agregadas para estas a ningún archivo nuevo o subdirectorio nuevo. Esto las limita de manera efectiva a archivos y subdirectorios que ya tienen ACL, o si el propietario del archivo relevante agrega la ACL más tarde utilizando **setfacl**, Aún pueden crear sus propios archivos y subdirectorios.

nota

La salida de **getfacl** se puede usar como entrada para **setfacl** para restaurar la ACL o para copiar la ACL desde el origen. Por ejemplo, para restaurar las ACL desde una copia de seguridad, use **getfacl -R dir1 > file1** para generar un archivo de volcado de salida de ACL recursiva para el directorio y su contenido. Luego, esta salida se puede usar para la recuperación de ACL originales al pasar la salida guardada y una entrada al comando **setfacl**. Por ejemplo: **setfacl --set-file=file1** para hacer una actualización masiva al mismo directorio en la ruta actual.

La máscara de ACL
La máscara de ACL define los permisos máximos que se pueden otorgar a *usuarios nombrados*, el *propietario del grupo* y los *grupos nombrados*. No restringe los permisos del usuario *propietario del archivo* ni *otro*. Todos los archivos y directorios que implementan ACL tendrán una máscara de ACL.

La máscara se puede visualizar con **getfacl** y establecer explícitamente con **setfacl**.
Se calculará y se agregará automáticamente si no se la establece de forma explícita, pero también podría heredarse de una configuración de máscara predeterminada de un directorio principal. De forma predeterminada, la máscara se calcula nuevamente siempre que se agregue, se modifique o se elimine cualquiera de las ACL afectadas.

Precedencia de permisos de ACL
Al determinar si un proceso (un programa en ejecución) puede acceder a un archivo, los permisos del archivo y las ACL se aplican de la siguiente manera:

- Si el proceso se ejecuta como el usuario que es propietario del archivo, se aplican los permisos de ACL del usuario del archivo.

- Si el proceso se ejecuta como un usuario que está detallado en una entrada de ACL del usuario, se aplican los permisos de ACL de usuario nombrado (siempre que esté permitido por la máscara).
- Si el proceso se ejecuta como grupo que coincide con el propietario del grupo del archivo, o como un grupo con una entrada de ACL de grupos nombrados explicita, se aplican los permisos de ACL que coinciden (siempre que esté permitido por la máscara).
- De lo contrario, se aplican los *otros* permisos de ACL del archivo.

Referencias

Páginas del manual: **`acl`**(5), **`getfacl`**(1), **`ls`**(1)

Práctica: interpretar ACL

Establezca una coincidencia entre los siguientes elementos y sus equivalentes de la tabla.

`default:m::rx /directory`

`default:user:mary:rx /directory`

`g::rw /directory`

`g::rw file`

`getfacl /directory`

`group:hug:rwx /directory`

`user::rx file`

`user:mary:rx file`

Descripción	Operación de ACL
Muestra ACL en un directorio.	
Usuario nombrado con permisos de lectura y ejecución para un archivo.	
Propietario del archivo con permisos de lectura y ejecución para un archivo.	
Permisos de lectura y escritura para un directorio otorgados al propietario del grupo del directorio.	
Permisos de lectura y escritura para un archivo otorgados al propietario del grupo del archivo.	

Descripción	Operación de ACL
Permisos de lectura, escritura y ejecución para un directorio otorgados a un grupo nombrado.	
Permisos de lectura y ejecución establecidos como la máscara predeterminada.	
Permiso de lectura inicial otorgado a usuario nombrado para archivos nuevos y permiso de lectura y ejecución para subdirectorios nuevos.	

Solución

Establezca una coincidencia entre los siguientes elementos y sus equivalentes de la tabla.

Descripción	Operación de ACL
Muestra ACL en un directorio.	**`getfacl /directory`**
Usuario nombrado con permisos de lectura y ejecución para un archivo.	**`user:mary:rx file`**
Propietario del archivo con permisos de lectura y ejecución para un archivo.	**`user::rx file`**
Permisos de lectura y escritura para un directorio otorgados al propietario del grupo del directorio.	**`g::rw /directory`**
Permisos de lectura y escritura para un archivo otorgados al propietario del grupo del archivo.	**`g::rw file`**
Permisos de lectura, escritura y ejecución para un directorio otorgados a un grupo nombrado.	**`group:hug:rwx /directory`**
Permisos de lectura y ejecución establecidos como la máscara predeterminada.	**`default:m::rx /directory`**
Permiso de lectura inicial otorgado a usuario nombrado para archivos nuevos y permiso de lectura y ejecución para subdirectorios nuevos.	**`default:user:mary:rx /directory`**

Protección de archivos con ACL

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Cambiar permisos de archivos de ACL regulares usando **setfacl**.
- Controlar permisos de archivos de ACL predeterminados para archivos y directorios nuevos.

Cambio de permisos de archivos de ACL

Use **setfacl** para agregar, modificar o eliminar ACL en archivos y directorios.

Las ACL usan la representación de permisos de sistema de archivos normal, "**r**" para permiso de lectura, "**w**" para permiso de escritura y "**x**" para permiso de ejecución. Un "**-**" (guión) indica que el permiso relevante está ausente. Cuando (recursivamente) se configuran ACL, se puede usar una "**X**" mayúscula para indicar que el permiso de ejecución solo se debe establecer en directorios y no en archivos regulares, a menos que el archivo ya tenga el permiso de ejecución relevante. Este es el mismo comportamiento de **chmod**.

Adición o modificación de una ACL

Las ACL se pueden establecer a través de la línea de comandos utilizando **-m**, o se pueden especificar a través de un archivo usando **-M** (use un "**-**" [guión]) en lugar de un nombre de archivo para *stdin*). Estas dos opciones son las opciones "modificar"; agregan entradas de ACL nuevas o reemplazan entradas de ACL existentes específicas en un archivo o directorio. Las demás entradas de ACL existentes en el archivo o el directorio permanecen intactas.

nota

Use las opciones **--set** o **--set-file** para reemplazar completamente la configuración de ACL en un archivo.

Cuando se define por primera vez una ACL en un archivo, si la operación de adición no incluye configuración para permisos del *propietario del archivo*, el *propietario del grupo* u *otros*, se establecerán en función de los permisos de archivos estándar actuales (estas también son conocidas como ACL *base* y no se pueden eliminar), y, asimismo, se calculará y se agregará un nuevo valor de *máscara*.

Para agregar o modificar una ACL de *usuario* o *usuario nombrado*:

```
[student@serverX ~]$ setfacl -m u:name:rX file
```

Si *name* se deja en blanco, se aplica al *propietario del archivo*; de lo contrario, *name* puede ser un nombre de usuario o un valor de UID. En este ejemplo, los permisos otorgados serían de solo lectura y, si ya están establecidos, de ejecución (a menos que *file* fuera un directorio, en cuyo caso el directorio obtendría el permiso de ejecución establecido para permitir la búsqueda en el directorio).

Los permisos del *propietario del archivo* de ACL y el *propietario del archivo* estándar son equivalentes; por consiguiente, el uso de **chmod** en los permisos del *propietario del archivo* es

equivalente a usar **setfacl** en los permisos del *propietario del archivo*. **chmod** no tiene efecto sobre los usuarios nombrados.

Para agregar o modificar una ACL de *grupo* o *grupo nombrado*:

```
[student@serverX ~]$ setfacl -m g:name:rw file
```

Esto sigue el mismo patrón para agregar o modificar una ACL de usuario. Si *name* se deja en blanco, se aplica al *propietario del grupo*. De lo contrario, especifique un nombre de grupo o un valor de GID para un *grupo nombrado*. Los permisos serían de lectura y escritura en este ejemplo.

chmod no tiene efecto en permisos de ningún grupo para archivos con configuraciones de ACL, pero actualiza la máscara de ACL.

Para agregar o modificar la ACL de *otro*:

```
[student@serverX ~]$ setfacl -m o::- file
```

otro solo acepta configuración de permisos. Es común que el permiso se establezca en "**-**" (guión), que especifica que los usuarios *otro* NO tienen permiso, pero se puede especificar cualquiera de los permisos estándares.

Los permisos de *otro* de ACL y *otro* estándar son equivalentes; por consiguiente, el uso de **chmod** en los permisos de *otro* es equivalente a usar **setfacl** en los permisos de *otro*.

Agregue varias entradas a través del mismo comando y separe con coma cada una de las entradas:

```
[student@serverX ~]$ setfacl -m u::rwx,g:sodor:rX,o::- file
```

Esto establecerá al *propietario del archivo* a leer, escribir y ejecutar, establecerá al grupo nombrado **sodor** en solo lectura y ejecución condicional y restringirá a todos los usuarios *otro* a NINGÚN permiso. El *propietario del grupo* mantendrá sus permisos de ACL o de archivo existentes y las otras entradas "nombradas" permanecerán iguales.

Uso de getfacl como entrada

El resultado de **getfacl** se puede usar como entrada para **setfacl**:

```
[student@serverX ~]$ getfacl file-A | setfacl --set-file=- file-B
```

--set-file acepta entrada de un archivo o *stdin*, y el "**-**" (guión) especifica el uso de *stdin*. En este caso, *file-B* tendrá la misma configuración de ACL que *file-A*.

Configuración de una máscara de ACL explícita

Una máscara de ACL se puede establecer de forma explícita en un archivo o directorio para limitar los permisos efectivos máximos para usuarios nombrados, el propietario del grupo y los grupos nombrados. Esto restringe los permisos existentes que superen la máscara, pero no afecta los permisos que son menos permisivos que la máscara.

```
[student@serverX ~]$ setfacl -m m::r file
```

Esto agregaría un valor de la máscara que restringiría a cualquiera de los *usuarios nombrados*, el *propietario del grupo* y cualquiera de los *grupos nombrados* a permiso de solo lectura, independientemente de su configuración existente. Los usuarios *propietario del archivo* y *otro* no se ven afectados por la configuración de la máscara.

`getfacl` mostrará un comentario "*efectivo*" además de entradas que son restringidas por una configuración de máscara.

Importante

De forma predeterminada, la máscara de ACL se vuelve a calcular cada vez que una de las configuraciones de ACL afectadas (usuarios nombrados, propietario del grupo o grupos nombrados) se modifica o elimina, y potencialmente se restablece una configuración de la máscara explícita.

Para evitar calcular nuevamente la máscara, use **`-n`** o incluya una configuración de la máscara (**`-m m::`*`perms`***) con cualquier operación **`setfacl`** que modifique la configuración de ACL afectada de la máscara.

Modificaciones de ACL recursivas

Cuando se configura una ACL en un directorio, es común querer aplicar la ACL de forma recursiva a la estructura del directorio y los archivos. Use la opción **`-R`** para hacer esto. El permiso "**X**" (x mayúscula) se usa a menudo con recursión, de modo que los archivos con permiso de ejecución establecido retienen la configuración y los directorios obtienen el permiso de ejecución establecido para permitir la búsqueda de directorios. También se considera práctica recomendada usar la X mayúscula cuando se configuran ACL de manera no recursiva, dado que esto evita que un administrador agregue de forma accidental permisos de ejecución a un archivo regular.

```
[student@serverX ~]$ setfacl -R -m u:name:rX directory
```

Esto agregaría al usuario *name* al *directorio* y todos los archivos y subdirectorios existentes, y otorgaría permiso de solo lectura y ejecución condicional.

Eliminación de una ACL

La eliminación de entradas de ACL específicas sigue el mismo formato básico que la operación de modificar, excepto que "*:perms*" no debe especificarse.

```
[student@serverX ~]$ setfacl -x u:name,g:name file
```

Esto solo eliminaría al usuario nombrado y al grupo nombrado de la lista de ACL de archivos o directorios. El resto de las ACL existentes permanecen activas.

Es posible usar las operaciones de eliminación (**`-x`**) y modificación (**`-m`**) en la misma operación **`setfacl`**.

La máscara solo puede eliminarse si no hay otras ACL establecidas (excluidas las ACL *base* que no se pueden eliminar), de modo que debe eliminarse última. El archivo no tendrá ACL y **`ls -l`** no mostrará el símbolo "**+**" junto a la cadena de permisos. De forma alternativa, para eliminar TODAS las ACL de un archivo o un directorio (incluidas las ACL *predeterminadas* en los directorios), use:

```
[student@serverX ~]$ setfacl -b file
```

Control de permisos de archivos de ACL predeterminadas

Un directorio puede tener ACL *predeterminadas* establecidas que se heredan automáticamente mediante todos los archivos nuevos y subdirectorios nuevos. Puede haber permisos de ACL *predeterminadas* establecidos para cada una de las configuraciones de ACL estándares, incluida una máscara predeterminada.

Un directorio aún requiere ACL estándares para el control de acceso porque las ACL *predeterminadas* no implementan control de acceso para el directorio; solo proporcionan soporte de herencia para permisos de ACL.

Un ejemplo:

```
[student@serverX ~]$ setfacl -m d:u:name:rx directory
```

Esto agrega un usuario nombrado predeterminados (**d:u:*name***) con permiso de solo lectura y ejecución en subdirectorios.

El comando **setfacl** para agregar una ACL *predeterminada* para cada uno de los tipos de ACL es exactamente el mismo que para las ACL estándares, pero incluye **d:** delante. De forma alternativa, use la opción **-d** en la línea de comandos.

Importante

Al configurar las ACL *predeterminadas* en un directorio, asegúrese de que los usuarios podrán acceder al contenido de los subdirectorios nuevos creados en este, al incluir el permiso de ejecución en la ACL *predeterminada*.

Los usuarios no recibirán automáticamente el permiso de ejecución establecido en los archivos regulares creados recientemente, ya que, a diferencia de los directorios nuevos, la *máscara* de ACL de un archivo regular nuevo es **rw-**.

nota

Los archivos y subdirectorios nuevos continúan obteniendo los valores de UID de su propietario y de GID del grupo primario establecidos a partir del usuario creador, excepto cuando la marca **setgid** del directorio principal está habilitada, en cuyo caso el GID del grupo primario será el mismo que el GID del directorio principal.

Eliminación de ACL predeterminadas

Eliminar una ACL *predeterminada* es también igual que eliminar una ACL estándar; nuevamente, se agrega **d:** adelante o se usa la opción **-d**.

```
[student@serverX ~]$ setfacl -x d:u:name directory
```

Esto elimina la ACL *predeterminada* que se agregó en el ejemplo anterior.

Para eliminar todas las ACL *predeterminadas* en un directorio, use **`setfacl -k /directory`**.
Para eliminar TODAS las ACL en un directorio, use **`setfacl -b /directory`**.

Referencias

Páginas del manual: **`acl`**(5), **`setfacl`**(1)

Práctica: Uso de ACL para otorgar y limitar el acceso

En este laboratorio, agregará una lista de control de acceso (ACL) de grupo nombrado y una ACL de usuario nombrado a una carpeta compartida existente y su contenido. Configurará ACL *predeterminadas* para asegurar que los archivos y directorios futuros obtengan los permisos correctos.

Recursos:	
Archivos:	**/shares/steamies/***, **/shares/steamies/display_engines.sh**
Máquinas:	serverX

Resultados:

- Los miembros del grupo **sodor** tendrán los mismos permisos de acceso que el grupo **controller** en el directorio **steamies**, excepto **james**, quien no tiene acceso.
- Los archivos y directorios existentes se actualizarán para reflejar los nuevos permisos de ACL de **sodor** y **james**.
- Los archivos y directorios nuevos obtendrán automáticamente los permisos de ACL y de archivos correctos.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en su sistema de servidor y configúrelo.

```
[student@serverX ~]$ lab acl setup
```

- Abra una terminal.
- Cambie a **root** usando **sudo -i**.

El estudiante es un controlador para la red Sodor Island Rail. Hay un directorio compartido configurado adecuadamente y ubicado en **/shares/steamies** que aloja archivos que detallan alineación, motores a vapor, etc.

Actualmente, solo los miembros del grupo **controller** tienen acceso a este directorio, pero se ha decidido que se otorgará a los miembros del grupo **sodor** el beneficio de acceso completo a este directorio.

James, un miembro del grupo **sodor**, ha ocasionado *caos y confusión* en muchas ocasiones, de modo que se le negará el acceso al directorio, al menos hasta que muestre que es un *motor realmente útil*.

Su tarea es agregar ACL adecuadas al directorio y su contenido, de modo que los miembros del grupo **sodor** tengan acceso completo, pero negar todo tipo de acceso al usuario **james**.

Asegúrese de que a los archivos y directorios futuros almacenados en **/shares/steamies** se le apliquen las ACL adecuadas.

Información importante:

- Grupo **controller**: **student**
- Grupo **sodor**: **thomas**, **james**
- Hay un subdirectorio denominado **engines** y varios archivos para evaluar las ACL. Además, hay un script ejecutable que puede evaluar.
- Thomas y James tienen sus contraseñas establecidas como **redhat**.
- Todos los cambios deben ocurrir en el directorio **steamies** y sus archivos; no ajuste el directorio **shares**.

1. Agregue las ACL nombradas al directorio **steamies** y todo su contenido.

   1.1. Use **setfacl** para actualizar recursivamente el directorio **steamies**, y otorgue permisos de lectura, escritura y ejecución condicional al grupo **sodor**.

   ```
   [root@serverX ~]# setfacl -Rm g:sodor:rwX /shares/steamies
   ```

   -R recursivo, **-m** modificar/agregar, **:rwX** leer/escribir/ejecutar (pero solo en directorios y ejecutables existentes)

   1.2. Use **setfacl** para actualizar recursivamente el directorio **steamies**, denegar al usuario **james** del grupo **sodor** todo tipo de acceso.

   ```
   [root@serverX ~]# setfacl -Rm u:james:- /shares/steamies
   ```

   -R recursivo, **-m** modificar/agregar, **:-** sin permisos

2. Agregue las ACL nombradas como ACL *predeterminadas* para admitir futuras adiciones de archivos y directorios.

   2.1. Use **setfacl** para agregar una regla de acceso predeterminada para el grupo **sodor**. Otorgue permisos de lectura, escritura y ejecución en el directorio **steamies**.

   ```
   [root@serverX ~]# setfacl -m d:g:sodor:rwx /shares/steamies
   ```

   -m modificar/agregar, **d:g** grupo predeterminado, **:rwx** leer/escribir/ejecutar (necesario para creación y acceso adecuados a subdirectorio)

   2.2. Use **setfacl** para agregar una regla de acceso predeterminada para el usuario **james**. Niegue todo acceso al directorio **steamies**.

   ```
   [root@serverX ~]# setfacl -m d:u:james:- /shares/steamies
   ```

   -m modificar/agregar, **d:u** usuario predeterminado, **:-** sin permisos

3. Verifique sus cambios en ACL.

Thomas debe poder leer cualquier archivo, crear un directorio nuevo con un nuevo archivo en este y ejecutar el script **display_engines.sh**.

James no debe poder leer, escribir ni ejecutar ningún archivo; esto incluye no poder listar los contenidos del directorio.

Use **sudo -i -u *user*** para cambiar a usuarios de prueba. Use **exit** o **Ctrl**+**D** para salir de la shell de usuarios de prueba.

```
[root@serverX ~]# exit
[student@serverX ~]$ sudo -i -u thomas
[thomas@serverX ~]$ cd /shares/steamies/
```

3.1. Use **cat** para comprobar que Thomas pueda leer un archivo.

```
[thomas@serverX steamies]$ cat roster.txt
James - Shunting at Brendam docks
Percy - Overnight mail run
Henry - Flying Kipper run
Thomas - Annie and Clarabel, Knapford line
```

3.2. Use **display_engines.sh** para comprobar que Thomas pueda ejecutar un script.

```
[thomas@serverX steamies]$ ./display_engines.sh
They're two, they're four, they're six, they're eight ...
Edward wants to help and share
...
Toby, well let's say, he's square
```

3.3. Use **mkdir** para crear un directorio como Thomas.

Use **echo** para crear un archivo en el directorio nuevo como Thomas.

Cambie nuevamente a **student** cuando haya finalizado.

```
[thomas@serverX steamies]$ mkdir tidmouth
[thomas@serverX steamies]$ echo "toot toot" > tidmouth/whistle.txt
[thomas@serverX steamies]$ exit
```

3.4. Use **cd** para probar y cambiar dentro del directorio como James, y también pruebe **ls** para listar el directorio. Ambos comandos deben fallar con **permiso denegado**.

Puede intentar uno o más de los comandos emitidos por Thomas, excepto como James, para verificar mejor su falta de acceso. Pruebe agregar prefijos a cada archivo con la ruta completa, **/shares/steamies**, debido a que no puede usar **cd** en el directorio.

Cambie nuevamente a **student** cuando haya terminado de evaluar a **james**.

```
[student@serverX ~]$ sudo -i -u james
[james@serverX ~]$ cd /shares/steamies/
-bash: cd: /shares/steamies/: Permission denied
[james@serverX ~]$ ls /shares/steamies/
```

```
ls: cannot open directory /shares/steamies: Permission denied
[james@serverX ~]$ cat /shares/steamies/roster.txt
cat: /shares/steamies/roster.txt: Permission denied
[james@serverX ~]$ exit
```

3.5. Use **getfacl** para ver todas las ACL en **/shares/steamies** y las ACL en **/shares/steamies/tidmouth**.

nota

Use **newgrp controller** para cambiar *student* al grupo *controller*.

El script **lab acl setup** agrega a *controller* como grupo suplementario a *student*; sin embargo, a menos que haya reiniciado la shell antes de este paso, la shell actual no reconoce aún la nueva membresía y **getfacl** en **tidmouth** tendrá el **permiso denegado**.

```
[student@serverX ~]$ newgrp controller
[student@serverX ~]$ getfacl /shares/steamies
getfacl: Removing leading '/' from absolute path names
# file: shares/steamies/
# owner: root
# group: controller
# flags: -s-
user::rwx
user:james:---
group::rwx
group:sodor:rwx
mask::rwx
other::---
default:user::rwx
default:user:james:---
default:group::rwx
default:group:sodor:rwx
default:mask::rwx
default:other::---

[student@serverX ~]$ getfacl /shares/steamies/tidmouth
getfacl: Removing leading '/' from absolute path names
# file: shares/steamies/tidmouth
# owner: thomas
# group: controller
# flags: -s-
user::rwx
user:james:---
group::rwx
group:sodor:rwx
mask::rwx
other::---
default:user::rwx
default:user:james:---
default:group::rwx
default:group:sodor:rwx
default:mask::rwx
default:other::---
```

Trabajo de laboratorio: Control de acceso a archivos con listas de control de acceso (ACL)

En este trabajo de laboratorio, actualizará un directorio de colaboración para tener la propiedad y los permisos del grupo correctos. Agregará ACL para permitir que otro grupo tenga permisos adecuados y, a su vez, limitará el permiso para un usuario específico.

Recursos:	
Archivos:	**/shares/cases/***
Máquinas:	serverX

Resultados:

- Los miembros del grupo de **bakerstreet** tendrán permisos de acceso correctos para el directorio **cases**.
- Los miembros del grupo de **scotlandyard** tendrán acceso de lectura/escritura para el directorio **cases**, excepto el usuario **jones**, que solo tiene acceso de lectura. Todos los miembros del grupo **scotlandyard** deberán tener permiso de ejecución en el directorio.
- Los archivos y directorios nuevos obtendrán automáticamente los permisos de propiedad del grupo, de ACL y de archivos.

Andes de comenzar

- Restablezca su sistema serverX (*consulte la nota*).
- Inicie sesión en su sistema servidor y configúrelo (*consulte la nota*).

```
[student@serverX ~]$ lab acl setup
```

- Abra una terminal.
- Cambie a **root** usando **sudo -i**.

nota

Si restablece su servidor para el ejercicio de práctica "Uso de ACL para otorgar y limitar acceso" y no ha utilizado indebidamente el directorio **/shares/cases**, NO es necesario que restablezca el servidor ni que vuelva a ejecutar la configuración del laboratorio para este trabajo de laboratorio.

La agencia de detectives Baker Street está configurando un directorio compartido de colaboración para contener archivos de casos, para los cuales los miembros del grupo **bakerstreet** tendrán permiso de lectura y escritura.

El detective líder, Sherlock Holmes, ha decidido que los miembros del grupo **scotlandyard** también deban poder leer y escribir en el directorio compartido. Sin embargo, Holmes cree que el inspector Peter Jones (un miembro del grupo **scotlandyard**) es un imbécil, y por esto, Jones debe tener su acceso al directorio restringido a solo lectura.

La Sra. Hudson tiene habilidades de Linux limitadas y solo podía crear el directorio compartido y copiar algunos archivos en este. En la hora de la merienda, le solicitó a usted que complete el trabajo, mientras ella organiza el té y las galletas para Holmes y Watson.

Su tarea es completar la configuración del directorio compartido. El directorio y todo su contenido deben ser propiedad del grupo **bakerstreet**, y los archivos se deben actualizar para la lectura y la escritura para el propietario y el grupo (**bakerstreet**). Los otros usuarios no deben tener permisos. También debe proporcionar permisos de lectura y escritura para el grupo **scotlandyard**, con la excepción de **jones**, quien solo obtiene permisos de lectura. Asegúrese de que su configuración se aplique a archivos existentes y futuros.

Información importante:

- Directorio compartido: **/shares/cases**
- Grupo **bakerstreet**: **holmes**, **watson**
- Grupo **scotlandyard**: **lestrade**, **gregson**, **jones**
- Existen dos archivos en el directorio: **adventures.txt** y **moriarty.txt**.
- Las cinco contraseñas de usuario son **redhat**.
- Todos los cambios deben ocurrir en el directorio **cases** y sus archivos; no ajuste el directorio **shares**.

Cuando haya finalizado, ejecute el comando **lab acl grade** desde su máquina para verificar su trabajo.

1. El directorio **cases** y su contenido deben pertenecer al grupo **bakerstreet**. Los nuevos archivos agregados en el directorio **cases** deben pertenecer automáticamente al grupo **bakerstreet**. Los archivos existentes deben establecerse en **rw** para usuario y grupo. (**Sugerencia**: no use **setfacl**.)

2. Agregue ACL al directorio **cases** (y su contenido) que permitan a los miembros del grupo **scotlandyard** tener acceso de lectura/escritura en los archivos y de ejecución en el directorio. Restrinja al usuario **jones** a acceso de lectura en los archivos y de ejecución en el directorio.

3. Agregue ACL que aseguren que todos los archivos o directorios nuevos del directorio **cases** tengan los permisos correctos aplicados para TODOS los grupos y usuarios autorizados.

4. Verifique que haya hecho los cambios en el sistema de archivos y ACL correctamente.

   Use **ls** y **getfacl** para revisar su configuración en **/shares/cases**.

   Desde **student**, use **sudo -i -u *user*** para cambiar tanto a **holmes** como a **lestrade**. Verifique que puede escribir en un archivo, leer desde un archivo, hacer un directorio y escribir en un archivo en el directorio nuevo. Use **ls** para comprobar los permisos del directorio nuevo y **getfacl** para revisar las ACL del directorio nuevo.

   En **student**, utilice **sudo -i -u jones** para cambiar usuarios. Intente escribir en un archivo (*debería fallar*) e intente hacer un directorio nuevo (*debería fallar*). Al igual que **jones**, debe poder leer desde el archivo **adventures.txt** en el directorio **cases** y leer

desde el archivo "prueba" escrito en cualquiera de los directorios nuevos creados por **holmes** y **lestrade**.

nota

El conjunto de pruebas anteriores son algunas de las pruebas que podría realizar para comprobar que los permisos de acceso sean correctos. Debe idear pruebas de validación de acceso adecuadas para su entorno.

5. Cuando haya finalizado, ejecute el comando **lab acl grade** desde su máquina **serverX** para verificar su trabajo.

Solución

En este trabajo de laboratorio, actualizará un directorio de colaboración para tener la propiedad y los permisos del grupo correctos. Agregará ACL para permitir que otro grupo tenga permisos adecuados y, a su vez, limitará el permiso para un usuario específico.

Recursos:	
Archivos:	**/shares/cases/***
Máquinas:	serverX

Resultados:

- Los miembros del grupo de **bakerstreet** tendrán permisos de acceso correctos para el directorio **cases**.
- Los miembros del grupo de **scotlandyard** tendrán acceso de lectura/escritura para el directorio **cases**, excepto el usuario **jones**, que solo tiene acceso de lectura. Todos los miembros del grupo **scotlandyard** deberán tener permiso de ejecución en el directorio.
- Los archivos y directorios nuevos obtendrán automáticamente los permisos de propiedad del grupo, de ACL y de archivos.

Andes de comenzar

- Restablezca su sistema serverX (*consulte la nota*).
- Inicie sesión en su sistema servidor y configúrelo (*consulte la nota*).

```
[student@serverX ~]$ lab acl setup
```

- Abra una terminal.
- Cambie a **root** usando **sudo -i**.

nota

Si restablece su servidor para el ejercicio de práctica "Uso de ACL para otorgar y limitar acceso" y no ha utilizado indebidamente el directorio **/shares/cases**, NO es necesario que restablezca el servidor ni que vuelva a ejecutar la configuración del laboratorio para este trabajo de laboratorio.

La agencia de detectives Baker Street está configurando un directorio compartido de colaboración para contener archivos de casos, para los cuales los miembros del grupo **bakerstreet** tendrán permiso de lectura y escritura.

El detective líder, Sherlock Holmes, ha decidido que los miembros del grupo **scotlandyard** también deban poder leer y escribir en el directorio compartido. Sin embargo, Holmes cree que el inspector Peter Jones (un miembro del grupo **scotlandyard**) es un imbécil, y por esto, Jones debe tener su acceso al directorio restringido a solo lectura.

La Sra. Hudson tiene habilidades de Linux limitadas y solo podía crear el directorio compartido y copiar algunos archivos en este. En la hora de la merienda, le solicitó a usted que complete el trabajo, mientras ella organiza el té y las galletas para Holmes y Watson.

Su tarea es completar la configuración del directorio compartido. El directorio y todo su contenido deben ser propiedad del grupo **bakerstreet**, y los archivos se deben actualizar para la lectura y la escritura para el propietario y el grupo (**bakerstreet**). Los otros usuarios no deben tener permisos. También debe proporcionar permisos de lectura y escritura para el grupo **scotlandyard**, con la excepción de **jones**, quien solo obtiene permisos de lectura. Asegúrese de que su configuración se aplique a archivos existentes y futuros.

Información importante:

- Directorio compartido: **/shares/cases**
- Grupo **bakerstreet**: **holmes**, **watson**
- Grupo **scotlandyard**: **lestrade**, **gregson**, **jones**
- Existen dos archivos en el directorio: **adventures.txt** y **moriarty.txt**.
- Las cinco contraseñas de usuario son **redhat**.
- Todos los cambios deben ocurrir en el directorio **cases** y sus archivos; no ajuste el directorio **shares**.

Cuando haya finalizado, ejecute el comando **lab acl grade** desde su máquina para verificar su trabajo.

1. El directorio **cases** y su contenido deben pertenecer al grupo **bakerstreet**. Los nuevos archivos agregados en el directorio **cases** deben pertenecer automáticamente al grupo **bakerstreet**. Los archivos existentes deben establecerse en **rw** para usuario y grupo. (**Sugerencia**: no use **setfacl**.)

   1.1. Use **chgrp** para actualizar recursivamente la propiedad del grupo en el directorio y su contenido.

   ```
   [root@serverX ~]# chgrp -R bakerstreet /shares/cases
   ```

   1.2. Use **chmod** para actualizar la marca **setgid** en el directorio.

   ```
   [root@serverX ~]# chmod g+s /shares/cases
   ```

   1.3. Use **chmod** para actualizar todos los permisos de archivo existentes para **rw** para el propietario y el grupo.

   ```
   [root@serverX ~]# chmod 660 /shares/cases/*
   ```

2. Agregue ACL al directorio **cases** (y su contenido) que permitan a los miembros del grupo **scotlandyard** tener acceso de lectura/escritura en los archivos y de ejecución en el directorio. Restrinja al usuario **jones** a acceso de lectura en los archivos y de ejecución en el directorio.

   2.1. Use **setfacl** para actualizar recursivamente el directorio **cases** existente y su contenido. Otorgue al grupo **scotlandyard** permisos de lectura, escritura y ejecución condicionales.

```
[root@serverX ~]# setfacl -Rm g:scotlandyard:rwX /shares/cases
```

2.2. Use **setfacl** para actualizar recursivamente el directorio **cases** existente y su contenido. Otorgue al usuario **jones** permisos de lectura y ejecución condicionales.

```
[root@serverX ~]# setfacl -Rm u:jones:rX /shares/cases
```

3. Agregue ACL que aseguren que todos los archivos o directorios nuevos del directorio **cases** tengan los permisos correctos aplicados para TODOS los grupos y usuarios autorizados.

3.1. Use **setfacl** para actualizar los permisos *predeterminados* para los miembros del grupo **scotlandyard**. Los permisos predeterminados son de lectura, escritura y ejecución (necesarios para la creación y el acceso adecuados de subdirectorios).

```
[root@serverX ~]# setfacl -m d:g:scotlandyard:rwx /shares/cases
```

3.2. Use **setfacl** para actualizar los permisos *predeterminados* para el usuario de **scotlandyard jones**. Los permisos predeterminados son de lectura y ejecución (necesarios para el acceso adecuado a subdirectorios).

```
[root@serverX ~]# setfacl -m d:u:jones:rx /shares/cases
```

4. Verifique que haya hecho los cambios en el sistema de archivos y ACL correctamente.

Use **ls** y **getfacl** para revisar su configuración en **/shares/cases**.

Desde **student**, use **sudo -i -u *user*** para cambiar tanto a **holmes** como a **lestrade**. Verifique que puede escribir en un archivo, leer desde un archivo, hacer un directorio y escribir en un archivo en el directorio nuevo. Use **ls** para comprobar los permisos del directorio nuevo y **getfacl** para revisar las ACL del directorio nuevo.

En **student**, utilice **sudo -i -u jones** para cambiar usuarios. Intente escribir en un archivo (*debería fallar*) e intente hacer un directorio nuevo (*debería fallar*). Al igual que **jones**, debe poder leer desde el archivo **adventures.txt** en el directorio **cases** y leer desde el archivo "prueba" escrito en cualquiera de los directorios nuevos creados por **holmes** y **lestrade**.

4.1. Use **ls** para verificar el directorio **cases** y su contenido. Busque permisos de propietario de grupo, directorio y archivo, la marca **setgid** de directorio y el "**+**" que indica que existen ACL.

```
[root@serverX ~]# ls -ld /shares/cases
drwxrws---+ 2 root bakerstreet 46 Mar 18 06:56 /shares/cases
[root@serverX ~]# ls -l /shares/cases
total 16
-rw-rw----+ 1 root bakerstreet 22 Mar 18 06:56 adventures.txt
-rw-rw----+ 1 root bakerstreet  8 Mar 18 06:56 do_NOT_delete.grading.txt
-rw-rw----+ 1 root bakerstreet 38 Mar 18 06:56 moriarty.txt
```

4.2. Use **`getfacl`** y revise su resultado. Busque las entradas de usuarios nombrados y grupos nombrados en ACL estándares y predeterminadas.

```
[root@serverX ~]# getfacl /shares/cases
getfacl: Removing leading '/' from absolute path names
# file: shares/cases
# owner: root
# group: bakerstreet
# flags: -s-
user::rwx
user:jones:r-x
group::rwx
group:scotlandyard:rwx
mask::rwx
other::---
default:user::rwx
default:user:jones:r-x
default:group::rwx
default:group:scotlandyard:rwx
default:mask::rwx
default:other::---
```

4.3. Realice las siguientes operaciones como **`holmes`**. Repita el proceso como **`lestrade`**, reemplazando toda referencia a **`holmes`** en cada uno de los comandos. Compruebe que obtenga el comportamiento de acceso esperado.

```
[student@serverX ~]$ sudo -i -u holmes
[holmes@serverX ~]$ cd /shares/cases
[holmes@serverX cases]$ echo hello > holmes.txt
[holmes@serverX cases]$ cat adventures.txt
The Adventures of ...
[holmes@serverX cases]$ mkdir holmes.dir
[holmes@serverX cases]$ echo hello > holmes.dir/test.txt
[holmes@serverX cases]$ ls -ld holmes.dir
drwxrws---+ 2 holmes bakerstreet 21 Mar 18 07:35 holmes.dir
[holmes@serverX cases]$ ls -l holmes.dir
total 8
-rw-rw----+ 1 holmes bakerstreet 6 Mar 18 07:39 test.txt
[holmes@serverX cases]$ getfacl holmes.dir
# file: holmes.dir
# owner: holmes
# group: bakerstreet
# flags: -s-
user::rwx
user:jones:r-x
group::rwx
group:scotlandyard:rwx
mask::rwx
other::---
default:user::rwx
default:user:jones:r-x
default:group::rwx
default:group:scotlandyard:rwx
default:mask::rwx
default:other::---

[holmes@serverX cases]$ exit
logout
[student@serverX ~]$
```

4.4. Realice las siguientes operaciones como **jones**. Compruebe que obtenga el comportamiento de acceso esperado.

```
[student@serverX ~]# sudo -i -u jones
[jones@serverX ~]# cd /shares/cases
[jones@serverX cases]# echo hello > jones.txt
-bash: jones.txt: Permission denied
[jones@serverX cases]# cat adventures.txt
The Adventures of ...
[jones@serverX cases]# mkdir jones.dir
mkdir: cannot create directory ‘jones.dir’: Permission denied
[jones@serverX cases]# cat holmes.dir/test.txt
hello
[jones@serverX cases]# exit
logout
[student@serverX ~]#
```

nota

El conjunto de pruebas anteriores son algunas de las pruebas que podría realizar para comprobar que los permisos de acceso sean correctos. Debe idear pruebas de validación de acceso adecuadas para su entorno.

5. Cuando haya finalizado, ejecute el comando **lab acl grade** desde su máquina **serverX** para verificar su trabajo.

5.1.
```
[student@serverX ~]$ lab acl grade
```

Resumen

Listas de control de acceso (ACL) POSIX

- Las ACL proporcionan control de acceso detallado a archivos y directorios.
- El sistema de archivos se debe montar con soporte de ACL habilitado; XFS tiene soporte para ACL incorporado.
- **`ls -l`** indica la presencia de la configuración de ACL con el carácter "**+**". Los permisos del grupo muestran la configuración de la *máscara*.
- **`getfacl`** ***`file`*** muestra las ACL en un archivo o directorio; las ACL del directorio incluyen las ACL predeterminadas.
- Una máscara de ACL define los permisos máximos que los *usuarios nombrados*, el *propietario del grupo* y los *grupos nombrados* pueden obtener.
- Una precedencia de permisos de ACL es *usuario*, *usuarios nombrados*, *grupos* y luego *otros*.

Protección de archivos con ACL

- Cómo usar **`setfacl -m`** ***`acl_spec`*** para agregar o modificar.
- Cómo usar **`setfacl -x`** ***`acl_spec`*** para eliminar.
- Las ACL predeterminadas se pueden establecer en un directorio; delante de *acl_spec* agregue **`d:`**. Incluya permiso de ejecución para asegurar el acceso a nuevos subdirectorios.
- Cómo usar **`-R`** para recursivo, **`-b`** para eliminar todas las ACL, **`-k`** para eliminar las ACL predeterminadas.
- El *acl_spec* tiene el patrón ***`type:name:perms`***.
  - *type* puede ser **`u`**, **`g`**, **`o`**, o **`m`**.
  - *name* puede ser **`nombre de usuario`**, **`uid`**, **`nombre de grupo`**, o **`gid`**. Un nombre vacío implica *propietario del archivo* o *propietario del grupo*.
  - *perms* son **`r`**, **`w`**, **`x`**, o **`X`**. "**`-`**" significa no establecido.

redhat. TRAINING

CAPÍTULO 7

ADMINISTRACIÓN DE SEGURIDAD DE SELINUX

Descripción general	
Meta	Administrar el comportamiento de Security Enhanced Linux (SELinux) de un sistema para mantenerlo seguro en caso de un riesgo del servicio de red.
Objetivos	• Explicar los conceptos básicos de los permisos de SELinux. • Cambiar modos de SELinux con setenforce. • Cambiar contextos de archivos con semanage y restorecon. • Administrar booleanos de SELinux con setsebool. • Examinar registros y usar sealert para solucionar problemas de violaciones de SELinux.
Secciones	• Habilitación y supervisión de SELinux (y práctica) • Modificación de los modos de SELinux (y práctica) • Modificación de los contextos de SELinux (y práctica) • Modificación de los booleanos de SELinux (y práctica) • Resolución de problemas de SELinux (y práctica)
Trabajo de laboratorio	• Administración de seguridad de SELinux

Habilitación y supervisión de Security Enhanced Linux (SELinux)

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Explicar los conceptos básicos de las transiciones de contexto y los permisos de SELinux.
- Mostrar el modo actual de SELinux.
- Interpretar correctamente el contexto de SELinux de un archivo.
- Interpretar correctamente el contexto de SELinux de un proceso.
- Identificar la configuración de booleanos de SELinux actual.

Conceptos básicos de seguridad de SELinux

Security Enhanced Linux (SELinux) es una capa adicional de seguridad del sistema. Un objetivo principal de SELinux es proteger los datos del usuario de los servicios del sistema que han sido comprometidos. La mayoría de los administradores de Linux está familiarizado con el modelo de seguridad de permisos de usuario/grupo/otro. Este es un modelo basado en usuarios y grupos conocido como control de acceso discrecional. SELinux proporciona un nivel adicional de seguridad que está basado en objetos y controlado por reglas más sofisticadas, conocido como control de acceso obligatorio.

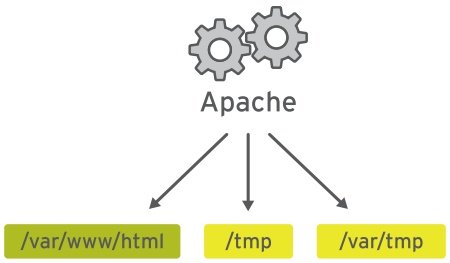

Figura 7.1: Servicio Apache sin protección de SELinux

Para permitir el acceso anónimo remoto a un servidor web, se deben abrir los puertos de firewall. Sin embargo, eso le da a la gente malintencionada la oportunidad de entrar al sistema a través de una vulnerabilidad de seguridad y, si ponen en riesgo el proceso del servidor web, obtienen sus permisos: los permisos del usuario **apache** y el grupo **apache**. Ese usuario o grupo tiene acceso de lectura a elementos como la raíz del documento (**`/var/www/html`**) y acceso de escritura a **`/tmp`**, **`/var/tmp`** y cualquier otro archivo o directorio que todos los usuarios puedan escribir.

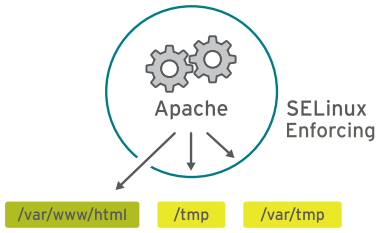

Figura 7.2: Servicio Apache con protección de SELinux

SELinux es un conjunto de reglas de seguridad que determina qué proceso puede acceder a qué archivos, directorios y puertos. Los archivos, procesos, directorios y puertos tienen etiquetas de seguridad especiales denominadas contextos de SELinux. Un contexto es simplemente un nombre que usa la política de SELinux para determinar si un proceso puede o no acceder a un archivo, directorio o puerto. De forma predeterminada, la política no permite ninguna interacción a menos que una regla explícita otorgue acceso. Si no hay ninguna regla de permiso, no se permite ningún tipo de acceso.

Las etiquetas de SELinux tienen varios contextos: usuario, rol, tipo y sensibilidad. La política de destino, que es la política predeterminada habilitada en Red Hat Enterprise Linux, basa sus reglas en el tercer contexto: el contexto de tipo. Por lo general, los nombres de contexto de tipo finalizan en **_t**. El contexto de tipo para el servidor web es **httpd_t**. El contexto de tipo para los archivos y los directorios que generalmente se encuentran en **/var/www/html** es **httpd_sys_content_t**. El contexto de tipo para los archivos y directorios que normalmente se encuentran en **/tmp** y **/var/tmp** es **tmp_t**. El contexto de tipo para los puertos del servidor web es **http_port_t**.

Hay una regla en la política que permite a Apache (el proceso de servidor web que se ejecuta como **httpd_t**) acceder a archivos y directorios con un contexto que normalmente se encuentra en **/var/www/html** y otros directorios de servidor web (**httpd_sys_content_t**). No hay una regla en la política para los archivos que normalmente se encuentran en **/tmp** y **/var/tmp**, de modo que no se permite el acceso. Con SELinux, un usuario malintencionado no podría acceder al directorio **/tmp**. SELinux tiene reglas para los sistemas de archivos remotos como NFS y CIFS, aunque todos los archivos en esos sistemas de archivos se etiquetan con el mismo contexto.

Muchos comandos que tienen que ver con archivos tienen una opción (generalmente **-Z**) para mostrar o configurar contextos de SELinux. Por ejemplo, **ps**, **ls**, **cp** y **mkdir** usan la opción **-Z** para mostrar o configurar contextos de SELinux.

```
[root@serverX ~]# ps axZ
LABEL                               PID TTY      STAT   TIME COMMAND
system_u:system_r:init_t:s0           1 ?        Ss     0:09 /usr/lib/systemd/...
system_u:system_r:kernel_t:s0         2 ?        S      0:00 [kthreadd]
system_u:system_r:kernel_t:s0         3 ?        S      0:00 [ksoftirqd/0]
[... Output omitted ...]
[root@serverX ~]# systemctl start httpd
[root@serverX ~]# ps -ZC httpd
LABEL                               PID TTY          TIME CMD
system_u:system_r:httpd_t:s0       1608 ?        00:00:05 httpd
system_u:system_r:httpd_t:s0       1609 ?        00:00:00 httpd
[... Output omitted ...]
[root@serverX ~]# ls -Z /home
```

```
drwx------. root    root    system_u:object_r:lost_found_t:s0 lost+found
drwx------. student student unconfined_u:object_r:user_home_dir_t:s0 student
drwx------. visitor visitor unconfined_u:object_r:user_home_dir_t:s0 visitor
[root@serverX ~]# ls -Z /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 icons
```

Modos de SELinux

Con fines de solución de problemas, la protección de SELinux puede deshabilitarse temporalmente usando los modos de SELinux.

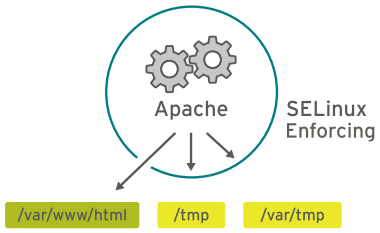

Figura 7.3: Modo de cumplimiento de SELinux

En *el modo de cumplimiento,* SELinux deniega de forma activa el acceso al servidor web que intente leer archivos con el contexto de tipo **`tmp_t`**. En el modo de cumplimiento, SELinux registra y protege.

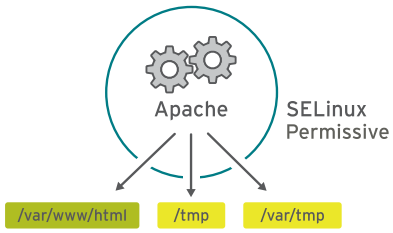

Figura 7.4: Modo permisivo de SELinux

El modo permisivo se usa generalmente para las cuestiones de solución de problemas. En el modo permisivo, SELinux permite todas las interacciones, incluso si no hay una regla explícita, y registra esas interacciones que habría denegado en el modo obligatorio. Este modo se puede usar temporalmente para permitir el acceso a contenido que SELinux está restringiendo. No se requiere reiniciar el sistema para pasar del modo de cumplimiento al modo permisivo, o viceversa.

Un tercer modo, *deshabilitado*, deshabilita SELinux por completo. Deberá reiniciar el sistema para deshabilitar SELinux por completo, o bien para pasar del modo deshabilitado al modo de cumplimiento o permisivo.

Importante

Es mejor usar el modo permisivo que apagar SELinux por completo. Esto se debe a que, incluso en el modo permisivo, el kernel mantendrá automáticamente las etiquetas del sistema de archivos de SELinux según sea necesario, con lo que se evitará la necesidad de volver a etiquetar el sistema de archivos cuando reinicie el sistema con SELinux habilitado.

Para visualizar el modo de SELinux actual en vigencia, use el comando **`getenforce`**.

```
[root@serverX ~]# getenforce
Enforcing
```

Booleanos de SELinux

Los booleanos de SELinux son opciones que modifican el comportamiento de la política de SELinux. Los booleanos de SELinux son reglas que pueden habilitarse o deshabilitarse. Los administradores de seguridad pueden utilizarlos para realizar ajustes selectivos en la política.

El comando **`getsebool`** se usa para mostrar booleanos de SELinux y su valor actual. La opción **`-a`** hace que este comando detalle todos los booleanos.

```
[root@serverX ~]# getsebool -a
abrt_anon_write --> off
allow_console_login --> on
allow_corosync_rw_tmpfs --> off
[... Output omitted ...]
```

nota

Muchos nombres booleanos han cambiado de Red Hat Enterprise Linux 6 a Red Hat Enterprise Linux 7.

Referencias

Páginas del manual: **`selinux`**(8), **`getenforce`**(8), **`ls`**(1), **`ps`**(1) y **`getsebool`**(8).

Práctica: Conceptos de SELinux

Establezca una coincidencia entre los siguientes elementos y sus equivalentes de la tabla.

Booleano	Contexto	El modo permisivo
Modo de cumplimiento	Modo deshabilitado	

Término	Descripción
Las reglas de la políticas se obedecen y las violaciones se registran	
Etiqueta en procesos, archivos y puertos que determina acceso	
Se requiere un nuevo arranque para pasar a este modo	
Cambio que habilita o deshabilita un conjunto de reglas de políticas	
Las violaciones de reglas de políticas solo producen mensajes de registro	

Solución

Establezca una coincidencia entre los siguientes elementos y sus equivalentes de la tabla.

Término	Descripción
Las reglas de la políticas se obedecen y las violaciones se registran	Modo de cumplimiento
Etiqueta en procesos, archivos y puertos que determina acceso	Contexto
Se requiere un nuevo arranque para pasar a este modo	Modo deshabilitado
Cambio que habilita o deshabilita un conjunto de reglas de políticas	Booleano
Las violaciones de reglas de políticas solo producen mensajes de registro	El modo permisivo

Cambio de modos de SELinux

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Modifique el modo actual de SELinux de un sistema.
- Configure el modo predeterminado de SELinux de un sistema

Con fines de solución de problemas, la protección de SELinux puede deshabilitarse temporalmente usando los modos de SELinux. En esta sección, se observará cómo cambiar los modos de SELinux de forma temporal entre el modo de cumplimiento y el modo permisivo. Solo se observará cómo configurar el modo predeterminado de SELinux que se determina en el arranque.

Cambio del modo actual de SELinux

El comando **`setenforce`** modifica el modo de SELinux actual:

```
[root@serverX ~]# getenforce
Enforcing
[root@serverX ~]# setenforce
usage:  setenforce [ Enforcing | Permissive | 1 | 0 ]
[root@serverX ~]# setenforce 0
[root@serverX ~]# getenforce
Permissive
[root@serverX ~]# setenforce Enforcing
[root@serverX ~]# getenforce
Enforcing
```

Otra manera de configurar temporalmente el modo SELinux es pasar un parámetro al kernel en el arranque. El paso de un argumento del kernel de **`enforcing=0`** hace que el sistema arranque en el modo permisivo. Un valor de **`1`** especificaría el modo de cumplimiento. SELinux se puede deshabilitar cuando se especifica el argumento **`selinux=0`**. Un valor de **`1`** habilitaría SELinux.

Configuración del modo predeterminado de SELinux

El archivo de configuración que determina el modo de SELinux en el que se establece al momento del arranque es **`/etc/selinux/config`**. Observe que contiene algunos comentarios útiles:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes
#               are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Use **/etc/selinux/config** para modificar el modo predeterminado de SELinux durante el arranque. En el ejemplo que se muestra, está configurado en el modo de cumplimiento.

Al pasar los argumentos del kernel **selinux=** o **enforcing=**, se anulan todos los valores predeterminados especificados en **/etc/selinux/config**.

Referencias

Páginas del manual: **getenforce**(1), **setenforce**(1), **selinux_config**(5)

Práctica: Cambio de modos de SELinux

En este trabajo de laboratorio, administrará modos de SELinux, tanto de forma temporal como de forma persistente.

Recursos	
Máquinas:	**serverX**

Resultados:
Obtendrá práctica al visualizar y configurar el modo actual de SELinux.

1. Inicie sesión como **raíz** en **serverX**. Muestre el modo actual de SELinux.

```
[root@serverX ~]# getenforce
Enforcing
```

2. Cambie el modo predeterminado de SELinux a permisivo y reinicie.

```
[root@serverX ~]# vi /etc/selinux/config
[root@serverX ~]# grep '^SELINUX' /etc/selinux/config
SELINUX=permissive
SELINUXTYPE=targeted
[root@serverX ~]# reboot
```

3. Cuando **serverX** funcione nuevamente, inicie sesión como **raíz** y muestre el modo actual de SELinux.

```
[root@serverX ~]# getenforce
Permissive
```

4. Modifique el modo predeterminado de SELinux al modo de cumplimiento.

```
[root@serverX ~]# vi /etc/selinux/config
[root@serverX ~]# grep '^SELINUX' /etc/selinux/config
SELINUX=enforcing
SELINUXTYPE=targeted
```

5. Configure el modo actual de SELinux al modo de cumplimiento.

```
[root@serverX ~]# setenforce 1
[root@serverX ~]# getenforce
Enforcing
```

Cambio de contextos de SELinux

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Configurar el contexto de seguridad de SELinux de los archivos en la política.
- Restaurar el contexto de seguridad de SELinux de los archivos.

Contexto inicial de SELinux

Generalmente, el contexto de SELinux del directorio principal de un archivo determina su contexto de SELinux inicial. El contexto de un directorio principal se asigna al archivo creado recientemente. Esto funciona para comandos como **`vim`**, **`cp`** y **`touch`**. Sin embargo, si un archivo se crea en otra parte y se conservan los permisos (como con **`mv`** o **`cp -a`**), el contexto original de SELinux no se modificará.

```
[root@serverX ~]# ls -Zd /var/www/html/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /var/www/html/
[root@serverX ~]# touch /var/www/html/index.html
[root@serverX ~]# ls -Z /var/www/html/index.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/
index.html
```

Cambio del contexto de SELinux de un archivo

Hay dos comandos que se utilizan para cambiar el contexto de SELinux de archivos: **`chcon`** y **`restorecon`**. El comando **`chcon`** cambia el contexto del archivo al contexto especificado como un argumento para el comando. A menudo, la opción **`-t`** se utiliza para especificar solo el tipo de componente del contexto.

El comando **`restorecon`** es el método preferido para cambiar el contexto de un archivo o directorio de SELinux. A diferencia de **`chcon`**, el contexto no se especifica explícitamente al usar este comando. Usa las reglas de la política de SELinux para determinar cuál debe ser el contexto del archivo.

nota

`chcon` no debe usarse para cambiar el contexto de archivos de SELinux. Se pueden cometer errores al especificar el contexto explícitamente. Los contextos de archivos se modificarán nuevamente a su contexto predeterminado si los sistemas de archivos del sistema se etiquetan nuevamente en el momento del arranque.

```
[root@serverX ~]# mkdir /virtual
[root@serverX ~]# ls -Zd /virtual
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /virtual
[root@serverX ~]# chcon -t httpd_sys_content_t /virtual
[root@serverX ~]# ls -Zd /virtual
drwxr-xr-x. root root unconfined_u:object_r:httpd_sys_content_t:s0 /virtual
[root@serverX ~]# restorecon -v /virtual
restorecon reset /virtual context unconfined_u:object_r:httpd_sys_content_t:s0->
```

```
unconfined_u:object_r:default_t:s0
[root@serverX ~]# ls -Zd /virtual
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /virtual
```

Definición de las reglas de contextos de archivos predeterminados de SELinux

Se puede usar el comando **semanage fcontext** para mostrar o modificar las reglas que usa el comando **restorecon** para configurar los contextos de archivos predeterminados. Utiliza expresiones regulares extendidas para especificar los nombres de archivo y las rutas de acceso. La expresión regular extendida más común utilizada en las reglas **fcontext** es **(/.*)?**, que significa "como opción, coincidir con un / seguido por una serie de caracteres". Busca coincidencias con el directorio detallado antes de la expresión y todo lo que contiene ese directorio de forma recursiva.

A continuación, se incluye una tabla de referencia para las opciones de operaciones de contexto de archivo básicas del comando **semanage fcontext**:

semanage fcontext opciones para agregar, eliminar o mostrar contextos de archivos de SELinux

opción	descripción
-a, --add	Agregar un registro del tipo de objeto especificado
-d, --delete	Eliminar un registro del tipo de objeto especificado
-l, --list	Mostrar registros del tipo de objeto especificado

El comando **restorecon** es parte del paquete **policycoreutil** y **semanage** es parte del paquete **policycoreutil-python**.

```
[root@serverX ~]# touch /tmp/file1 /tmp/file2
[root@serverX ~]# ls -Z /tmp/file*
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /tmp/file1
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /tmp/file2
[root@serverX ~]# mv /tmp/file1 /var/www/html/
[root@serverX ~]# cp /tmp/file2 /var/www/html/
[root@serverX ~]# ls -Z /var/www/html/file*
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /var/www/html/file1
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/
html/file2
[root@serverX ~]# semanage fcontext -l
...
/var/www(/.*)?       all files    system_u:object_r:httpd_sys_content_t:s0
...
[root@serverX ~]# restorecon -Rv /var/www/
restorecon reset /var/www/html/file1 context unconfined_u:object_r:user_tmp_t:s0
-> system_u:object_r:httpd_sys_content_t:s0
[root@serverX ~]# ls -Z /var/www/html/file*
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0
   /var/www/html/file1
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0
   /var/www/html/file2
```

En el siguiente ejemplo, se muestra cómo usar **semanage** para agregar un contexto para un directorio nuevo.

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

```
[root@serverX ~]# touch /virtual/index.html
[root@serverX ~]# ls -Zd /virtual/
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /virtual/
[root@serverX ~]# ls -Z /virtual/
-rw-r--r--. root root unconfined_u:object_r:default_t:s0 index.html
[root@serverX ~]# semanage fcontext -a -t httpd_sys_content_t '/virtual(/.*)?'
[root@serverX ~]# restorecon -RFvv /virtual
[root@serverX ~]# ls -Zd /virtual/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /virtual/
[root@serverX ~]# ls -Z /virtual/
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0 index.html
```

Referencias

Páginas del manual: **chcon**(1), **restorecon**(8), **semanage**(8) y **semanage-fcontext**(8)

Práctica: Cambio de contextos de SELinux

En este trabajo de laboratorio, cambiará persistentemente el contexto de SELinux de un directorio y su contenido.

Recursos	
Archivos:	`/etc/httpd/conf/httpd.conf`
Máquinas:	`serverX`

Resultados:
Tendrá un servidor web que publica contenido web de una raíz de documento no estándar.

Andes de comenzar
Debe contar con un sistema RHEL 7 en funcionamiento con SELinux en modo de cumplimiento.

1. Inicie sesión como **`raíz`** en **`serverX`**. Use **`yum`** para instalar el servidor web Apache.

```
[root@serverX ~]# yum install -y httpd
```

2. Configure Apache para usar una raíz de documento en una ubicación no estándar.

   2.1. Cree la nueva raíz del documento, **`/custom`**.

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

   2.2. Cree el **`index.html`** con algo de contenido reconocible.

```
[root@serverX ~]# echo 'This is serverX.' > /custom/index.html
```

   2.3. Configure Apache para que use la nueva ubicación. Debe reemplazar las dos apariciones de “/var/www/html” con “/custom” en el archivo de configuración de Apache, **`/etc/httpd/conf/httpd.conf`**.

```
[root@serverX ~]# vi /etc/httpd/conf/httpd.conf
[root@serverX ~]# grep custom /etc/httpd/conf/httpd.conf
DocumentRoot "/custom"
<Directory "/custom">
```

3. Inicie el servicio web Apache.

```
[root@serverX ~]# systemctl start httpd
```

4. Abra un navegador web en **`serverX`** e intente ver la siguiente URL: **`http://localhost/index.html`**. Recibirá un mensaje de error que dice que no tiene permiso para acceder al archivo.

5. Defina una regla de contextos de archivos de SELinux que establezca el tipo de contexto en **httpd_sys_content_t** para **/custom** y todos los archivos debajo de este.

```
[root@serverX ~]# semanage fcontext -a -t httpd_sys_content_t '/custom(/.*)?'
```

6. Use **restorecon** para cambiar sus contextos.

```
[root@serverX ~]# restorecon -Rv /custom
restorecon reset /custom context unconfined_u:object_r:default_t:s0-
>unconfined_u:object_r:httpd_sys_content_t:s0
restorecon reset /custom/index.html context unconfined_u:object_r:default_t:s0-
>unconfined_u:object_r:httpd_sys_content_t:s0
```

7. Intente ver **http://localhost/index.html** nuevamente. Debería ver el mensaje “This is serverX.” (Esto es serverX).

Cambio de booleanos de SELinux

Objetivos

Luego de completar esta sección, los estudiantes deberían poder usar los booleanos de SELinux para hacer ajustes en el comportamiento de la política.

Booleanos de SELinux

Los booleanos de SELinux son switches que modifican el comportamiento de la política de SELinux. Los booleanos de SELinux son reglas que pueden habilitarse o deshabilitarse. Los administradores de seguridad pueden utilizarlos para realizar ajustes selectivos en la política.

El paquete **selinux-policy-devel** proporciona muchas páginas del manual, ***_selinux**(8), que explican el propósito de los booleanos disponibles para varios servicios. Si este paquete ha sido instalado, el comando **man -k '_selinux'** puede detallar estos documentos.

El comando **getsebool** se utiliza para mostrar booleanos de SELinux y se utiliza **setsebool** para modificarlos. **setsebool -P** modifica la política de SELinux para que la modificación sea persistente. **semanage boolean -l** mostrará si un booleano es persistente o no, junto con una breve descripción del booleano.

```
[root@serverX ~]# getsebool -a
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
antivirus_use_jit --> off
...
[root@serverX ~]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> off
[root@serverX ~]# setsebool httpd_enable_homedirs on
[root@serverX ~]# semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs          (on   ,  off)  Allow httpd to enable homedirs
[root@serverX ~]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> on
[root@serverX ~]# setsebool -P httpd_enable_homedirs on
[root@serverX ~]# semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs          (on   ,   on)  Allow httpd to enable homedirs
```

Para solo detallar las modificaciones locales del estado de los booleanos de SELinux (cualquier configuración que difiera de los valores predeterminados de la política), se puede usar el comando **semanage boolean -l -C**.

```
[root@serverX ~]# semanage boolean -l -C
SELinux boolean                State  Default Description

cron_can_relabel               (off   ,   on)  Allow cron to can relabel
```

Referencias

Páginas del manual: **booleans**(8), **getsebool**(8), **setsebool**(8), **semanage**(8), **semanage-boolean**(8)

Práctica: Cambio de booleanos de SELinux

Apache puede publicar contenido web alojado en los directorios de inicio de los usuarios, pero SELinux evita esto de forma predeterminada. En este ejercicio, identificará y cambiará el booleano de SELinux que permitirá a Apache acceder a los directorios de inicio de los usuarios.

Recursos	
Archivos:	**/etc/httpd/conf.d/userdir.conf**
Máquinas:	**serverX**

Resultados:
Tendrá un servidor web que publica contenido web desde los directorios de inicio de los usuarios.

Andes de comenzar
El servidor web de Apache ya debe estar instalado y ejecutándose en serverX.example.com.

1. Inicie sesión como r**aíz** en **serverX**. Habilite la función Apache que permite a los usuarios publicar contenido web desde sus directorios de inicio. Edite el archivo de configuración **/etc/httpd/conf.d/userdir.conf** y cambie la línea con la directiva **UserDir** para que se lea lo siguiente:

```
#UserDir disabled
UserDir public_html
```

```
[root@serverX ~]# vi /etc/httpd/conf.d/userdir.conf
[root@serverX ~]# grep '#UserDir' /etc/httpd/conf.d/userdir.conf
#UserDir disabled
[root@serverX ~]# grep '^ *UserDir' /etc/httpd/conf.d/userdir.conf
UserDir public_html
```

2. Reinicie el servicio web Apache para que tengan efecto los cambios realizados.

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

3. Cree algo de contenido web que sea publicado desde un directorio de inicio de los usuarios.

   3.1. Inicie sesión como **student** en otra ventana y cree un directorio **public_html**.

```
[student@serverX ~]$ mkdir ~/public_html
```

   3.2. Cree algo de contenido en un archivo **index.html**.

```
[student@serverX ~]$ echo 'This is student content on serverX.' > ~/public_html/
index.html
```

3.3. Cambie los permisos en el directorio de inicio de **student** de modo que Apache pueda acceder al subdirectorio **public_html**.

```
[student@serverX ~]$ chmod 711 ~
```

4. Abra un navegador web en **serverX** e intente ver la siguiente URL: **http://localhost/~&stu;/index.html**. Recibirá un mensaje de error que dice que no tiene permiso para acceder al archivo.

5. En su ventana **raíz**, use el comando **getsebool** para ver si hay booleanos que restrinjan el acceso a los directorios de inicio.

```
[root@serverX ~]# getsebool -a | grep home
[... Output omitted ...]
httpd_enable_homedirs --> off
[... Output omitted ...]
```

6. Use **setsebool** para habilitar el acceso al directorio de inicio de forma persistente.

```
[root@serverX ~]# setsebool -P httpd_enable_homedirs on
```

7. Intente ver **http://localhost/~&stu;/index.html** nuevamente. Debería ver el mensaje “This is student content on serverX (Esto es contenido del estudiante en serverX).”

Solución de problemas de SELinux

Objetivos

Luego de completar esta sección, los estudiantes deberían poder usar las herramientas de análisis de registros de SELinux.

Solución de problemas de SELinux

¿Qué debe hacer cuando SELinux impide el acceso a archivos de un servidor? Hay una secuencia de pasos que debe realizarse cuando ocurre esto.

1. Antes de pensar en hacer ajustes, considere que SELinux puede estar haciendo este trabajo correctamente al prohibir el intento de acceso. Si un servidor web intenta acceder a archivos en **/home**, esto podría indicar un riesgo para el servicio si el contenido web no es publicado por usuarios. Si el acceso debería haberse otorgado, es necesario realizar pasos adicionales para resolver el problema.

2. El problema más común de SELinux es un contexto de archivos incorrecto. Esto puede ocurrir cuando un archivo se crea en una ubicación con un contexto de archivos y se traslada a una ubicación donde se espera un contexto diferente. En la mayoría de los casos, la ejecución de **restorecon** corregirá el problema. Corregir los problemas de este modo tiene poco impacto en la seguridad del resto del sistema.

3. Otra solución para un acceso demasiado restrictivo podría ser el ajuste de un booleano. Por ejemplo, el booleano **ftpd_anon_write** controla si usuarios del FTP anónimos pueden cargar archivos. Este booleano debería activarse si se desea permitir que usuarios del FTP anónimos carguen archivos en un servidor. El ajuste de booleanos requiere más cuidado porque estos pueden tener un amplio impacto en la seguridad del sistema.

4. Es posible que la política de SELinux tenga un error que evite un acceso legítimo. Debido a que SELinux se ha consolidado, es poco común que esto ocurra. Cuando está claro que se ha identificado un error en la política, comuníquese con el soporte de Red Hat para informar el error de modo que se pueda resolver.

Supervisión de las violaciones de SELinux

El paquete **setroubleshoot-server** debe estar instalado para enviar mensajes de SELinux a **/var/log/messages**. **setroubleshoot-server** escucha mensajes de auditoría en **/var/log/audit/audit.log** y envía un breve resumen a **/var/log/messages**. Este resumen incluye identificadores únicos (*UUID*) para violaciones de SELinux que se pueden usar para reunir más información. **sealert -l *UUID*** se usa para generar un informe para un incidente específico. **sealert -a /var/log/audit/audit.log** se usa para generar informes para todos los incidentes en ese archivo.

Considere el siguiente ejemplo de secuencia de comandos en un servidor web Apache estándar:

```
[root@serverX ~]# touch /root/file3
[root@serverX ~]# mv /root/file3 /var/www/html
[root@serverX ~]# systemctl start httpd
[root@serverX ~]# curl http://localhost/file3
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /file3
on this server.</p>
</body></html>
```

Si bien el contenido de **file3** es el esperado, el servidor web arroja un error de **permiso denegado**. Si se inspeccionan **/var/log/audit/audit.log** y **/var/log/messages**, se puede obtener más información sobre este error.

```
[root@serverX ~]# tail /var/log/audit/audit.log
...
type=AVC msg=audit(1392944135.482:429): avc:  denied  { getattr } for
  pid=1609 comm="httpd" path="/var/www/html/file3" dev="vda1" ino=8980981
  scontext=system_u:system_r:httpd_t:s0
  tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file
...
[root@serverX ~]# tail /var/log/messages
...
Feb 20 19:55:42 serverX setroubleshoot: SELinux is preventing /usr/sbin/httpd
  from getattr access on the file . For complete SELinux messages. run
  sealert -l 613ca624-248d-48a2-a7d9-d28f5bbe2763
```

Ambos archivos de registro indican que el motivo del error es una denegación de SELinux. El comando **sealert** detallado en **/var/log/messages** puede proporcionar más información, que incluye una posible corrección.

```
[root@serverX ~]# sealert -l 613ca624-248d-48a2-a7d9-d28f5bbe2763
SELinux is preventing /usr/sbin/httpd from getattr access on the file .

*****  Plugin catchall (100. confidence) suggests   *************************

If you believe that httpd should be allowed getattr access on the
  file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# grep httpd /var/log/audit/audit.log | audit2allow -M mypol
# semodule -i mypol.pp


Additional Information:
Source Context                system_u:system_r:httpd_t:s0
Target Context                unconfined_u:object_r:admin_home_t:s0
Target Objects                 [ file ]
Source                        httpd
Source Path                   /usr/sbin/httpd
Port                          <Unknown>
Host                          serverX.example.com
Source RPM Packages           httpd-2.4.6-14.el7.x86_64
Target RPM Packages
Policy RPM                    selinux-policy-3.12.1-124.el7.noarch
Selinux Enabled               True
Policy Type                   targeted
Enforcing Mode                Enforcing
Host Name                     serverX.example.com
Platform                      Linux serverX.example.com 3.10.0-84.el7.x86_64 #1
```

```
                              SMP Tue Feb 4 16:28:19 EST 2014 x86_64 x86_64
Alert Count                   2
First Seen                    2014-02-20 19:55:35 EST
Last Seen                     2014-02-20 19:55:35 EST
Local ID                      613ca624-248d-48a2-a7d9-d28f5bbe2763

Raw Audit Messages
type=AVC msg=audit(1392944135.482:429): avc:  denied  { getattr } for
  pid=1609 comm="httpd" path="/var/www/html/file3" dev="vda1" ino=8980981
  scontext=system_u:system_r:httpd_t:s0
  tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file

type=SYSCALL msg=audit(1392944135.482:429): arch=x86_64 syscall=lstat
  success=no exit=EACCES a0=7f9fed0edea8 a1=7fff7bffc770 a2=7fff7bffc770
  a3=0 items=0 ppid=1608 pid=1609 auid=4294967295 uid=48 gid=48 euid=48
  suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295
  comm=httpd exe=/usr/sbin/httpd subj=system_u:system_r:httpd_t:s0 key=(null)

Hash: httpd,httpd_t,admin_home_t,file,getattr
```

nota

La sección “Raw Audit Messages” (Mensajes de auditoría sin formato) revela el archivo de destino que presenta el problema, **`/var/www/html/file3`**. Además, el contexto objetivo, **`tcontext`**, no parece pertenecer a un servidor web. Use el comando **`restorecon /var/www/html/file3`** para arreglar el contexto de archivos. Si deben ajustarse otros archivos, **`restorecon`** puede restablecer de forma recursiva el contexto: **`restorecon -R /var/www/`**.

Referencias

Página del manual: **`sealert`**(8)

Práctica: Solución de problemas de SELinux

En este trabajo de laboratorio, aprenderá cómo solucionar problemas de denegaciones por seguridad de SELinux.

El cambio de **DocumentRoot** de un servidor web de Apache introduce denegaciones de acceso a SELinux. En este ejercicio, verá cómo ese problema podría haberse identificado y resuelto.

Recursos	
Máquinas:	**serverX**

Resultados:
Obtendrá algo de experiencia en el uso de herramientas de solución de problemas de SELinux.

Andes de comenzar
El servidor web de Apache ya debe estar instalado y ejecutándose en serverX.example.com.

Debe haber completado los pasos del ejercicio de práctica “Changing SELinux Contexts” (Cambio de contextos de SELinux).

1. Inicie sesión como **raíz** en **serverX**. Elimine la regla de contextos de archivos creada anteriormente y restaure la estructura del directorio **/custom** nuevamente a su contexto de SELinux original.

   1.1. Elimine la regla de contexto de archivos que agregó en el trabajo de laboratorio anterior.

   ```
   [root@serverX ~]# semanage fcontext -d -t httpd_sys_content_t '/custom(/.*)?'
   ```

   1.2. Cambie los contextos de archivos a sus valores originales.

   ```
   [root@serverX ~]# restorecon -Rv /custom
   restorecon reset /custom context unconfined_u:object_r:httpd_sys_content_t:s0
     ->unconfined_u:object_r:default_t:s0
   restorecon reset /custom/index.html context unconfined_u:object_r:httpd_sys_
     content_t:s0->unconfined_u:object_r:default_t:s0
   ```

2. Abra un navegador web en **serverX** e intente ver la siguiente URL: **http://localhost/index.html**. Recibirá un mensaje de error que dice que no tiene permiso para acceder al archivo.

3. Visualice los contenidos de **/var/log/messages**. Debería ver un resultado similar al siguiente:

   ```
   [root@serverX ~]# less /var/log/messages
   [... Output omitted ...]
   Feb 19 12:00:35 serverX setroubleshoot: SELinux is preventing /usr/sbin/httpd
   from getattr access on the file . For complete SELinux messages. run
     sealert -l 82ead554-c3cb-4664-85ff-e6f256437c6c
   ```

```
[... Output omitted ...]
```

4. Ejecute el comando **`sealert`** sugerido y vea si puede identificar el problema y hallar una posible solución.

```
[root@serverX ~]# sealert -l 82ead554-c3cb-4664-85ff-e6f256437c6c
SELinux is preventing /usr/sbin/httpd from getattr access on the file .

*****  Plugin catchall_labels (83.8 confidence) suggests   ******************

If you want to allow httpd to have getattr access on the  file
Then you need to change the label on $FIX_TARGET_PATH
Do
# semanage fcontext -a -t FILE_TYPE '$FIX_TARGET_PATH'
where FILE_TYPE is one of the following: NetworkManager_log_t, ...,
httpd_sys_content_t, httpd_sys_htaccess_t, httpd_sys_ra_content_t,
httpd_sys_rw_content_t, httpd_sys_script_exec_t, httpd_tmp_t, ...
Then execute:
restorecon -v '$FIX_TARGET_PATH'

*****  Plugin catchall (17.1 confidence) suggests   *************************

If you believe that httpd should be allowed getattr access on the  file by
  default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# grep httpd /var/log/audit/audit.log | audit2allow -M mypol
# semodule -i mypol.pp

Additional Information:
Source Context                system_u:system_r:httpd_t:s0
Target Context                unconfined_u:object_r:default_t:s0
Target Objects                 [ file ]
Source                        httpd
Source Path                   /usr/sbin/httpd
Port                          <Unknown>
Host                          serverX.example.com
Source RPM Packages           httpd-2.4.6-14.el7.x86_64
Target RPM Packages
Policy RPM                    selinux-policy-3.12.1-124.el7.noarch
Selinux Enabled               True
Policy Type                   targeted
Enforcing Mode                Enforcing
Host Name                     serverX.example.com
Platform                      Linux serverX.example.com 3.10.0-84.el7.x86_64 #1
                              SMP Tue Feb 4 16:28:19 EST 2014 x86_64 x86_64
Alert Count                   9
First Seen                    2014-02-19 10:33:06 EST
Last Seen                     2014-02-19 12:00:32 EST
Local ID                      82ead554-c3cb-4664-85ff-e6f256437c6c

Raw Audit Messages
type=AVC msg=audit(1392829232.3:1782): avc:  denied  { getattr } for
  pid=11870 comm="httpd" path="/custom/index.html" dev="vda1" ino=11520682
  scontext=system_u:system_r:httpd_t:s0
  tcontext=unconfined_u:object_r:default_t:s0 tclass=file

type=SYSCALL msg=audit(1392829232.3:1782): arch=x86_64 syscall=lstat success=no
  exit=EACCES a0=7f1854a3b068 a1=7fff493f2ff0 a2=7fff493f2ff0
  a3=ffffffffffffffff items=0 ppid=11866 pid=11870 auid=4294967295 uid=48
```

```
  gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none)
  ses=4294967295 comm=httpd exe=/usr/sbin/httpd
  subj=system_u:system_r:httpd_t:s0 key=(null)

Hash: httpd,httpd_t,default_t,file,getattr
```

5. Lea el resultado desde el comando **`sealert`**. Identifique con qué archivo el servidor web Apache está teniendo problemas y busque una posible solución.

   5.1. En la parte superior del resultado, se recomienda una solución.

   ```
   # semanage fcontext -a -t FILE_TYPE '$FIX_TARGET_PATH'
   where FILE_TYPE is one of the following: NetworkManager_log_t, ...,
     httpd_sys_content_t, httpd_sys_htaccess_t, httpd_sys_ra_content_t,
     httpd_sys_rw_content_t, httpd_sys_script_exec_t, httpd_tmp_t, ...
   Then execute:
   restorecon -v '$FIX_TARGET_PATH'
   ```

   5.2. Observe el mensaje AVC sin formato para identificar el archivo y el proceso relevantes que están provocando la alerta.

   ```
   Raw Audit Messages
   type=AVC msg=audit(1392829232.3:1782): avc:  denied  { getattr } for
     pid=11870 comm="httpd" path="/custom/index.html" dev="vda1" ino=11520682
     scontext=system_u:system_r:httpd_t:s0
     tcontext=unconfined_u:object_r:default_t:s0 tclass=file
   ```

   5.3. El proceso involucrado en la denegación por seguridad es el servidor web de Apache **`httpd`** y el archivo es **`/custom/index.html`**.

6. Anteriormente, resolvimos este problema usando **`semanage`** y **`restorecon`**. Debe decidir si la violación de SELinux es una violación de seguridad o si es un acceso legítimo que requiere un ajuste de SELinux para manejar una estructura de directorios no estándar.

Trabajo de laboratorio: Administración de seguridad de SELinux

En este trabajo de laboratorio, resolverá un problema de denegación de acceso de SELinux. Los administradores de sistemas tienen problemas para obtener un nuevo servidor web para proporcionar contenido a clientes cuando SELinux está en modo de cumplimiento.

Resuelva este problema al hacer ajustes a SELinux. No deshabilite SELinux ni lo ponga en modo permisivo. No traslade el contenido web ni reconfigure Apache de ningún modo.

Recursos	
Máquinas:	**`serverX`**

Resultados:
Iniciar un servidor web en **`serverX`** y dirigirlo a **`http://localhost/lab-content`** mostrará contenido web en lugar de un mensaje de error.

Andes de comenzar

- Restablezca su sistema **`serverX`**.
- Inicie sesión en su sistema **`serverX`** y configúrelo.

```
[student@serverX ~]$ lab selinux setup
```

1. Inicie un navegador web en **`serverX`** y diríjase a **`http://localhost/lab-content`**. Verá un mensaje de error.
2. Investigue e identifique el problema de SELinux que evita que Apache proporcione el contenido web.
3. Resuelva el problema de SELinux que evita que Apache proporcione el contenido web.
4. Verifique que el problema de SELinux se haya resuelto y que Apache pueda proporcionar contenido web.
5. Ejecute el comando **`lab selinux grade`** para confirmar sus hallazgos.

Solución

En este trabajo de laboratorio, resolverá un problema de denegación de acceso de SELinux. Los administradores de sistemas tienen problemas para obtener un nuevo servidor web para proporcionar contenido a clientes cuando SELinux está en modo de cumplimiento.

Resuelva este problema al hacer ajustes a SELinux. No deshabilite SELinux ni lo ponga en modo permisivo. No traslade el contenido web ni reconfigure Apache de ningún modo.

Recursos	
Máquinas:	**serverX**

Resultados:
Iniciar un servidor web en **serverX** y dirigirlo a **http://localhost/lab-content** mostrará contenido web en lugar de un mensaje de error.

Andes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo.

```
[student@serverX ~]$ lab selinux setup
```

1. Inicie un navegador web en **serverX** y diríjase a **http://localhost/lab-content**. Verá un mensaje de error.
2. Investigue e identifique el problema de SELinux que evita que Apache proporcione el contenido web.

   Observe en **/var/log/messages** para ver mensajes de error útiles.

```
[root@serverX ~]# tail /var/log/messages
[... Output omitted ...]
Feb 20 13:55:59 serverX dbus-daemon: dbus[427]: [system] Successfully activated
  service 'org.fedoraproject.Setroubleshootd'
Feb 20 13:55:59 serverX dbus[427]: [system] Successfully activated service
  'org.fedoraproject.Setroubleshootd'
Feb 20 13:56:01 serverX setroubleshoot: Plugin Exception restorecon
Feb 20 13:56:01 serverX setroubleshoot: SELinux is preventing /usr/sbin/httpd
  from open access on the file . For complete SELinux messages. run sealert -l
  160daebd-0359-4f72-9dde-46e7fd244e27
```

   Especialmente, observe los mensajes de **setroubleshootd**. Ejecute **sealert** para obtener información más detallada sobre el error de SELinux.

```
[root@serverX ~]# sealert -l 160daebd-0359-4f72-9dde-46e7fd244e27
SELinux is preventing /usr/sbin/httpd from open access on the file .

*****  Plugin catchall_boolean (89.3 confidence) suggests   ******************

If you want to allow httpd to read user content
Then you must tell SELinux about this by enabling the 'httpd_read_user_content'
boolean.
You can read 'None' man page for more details.
Do
```

```
setsebool -P httpd_read_user_content 1

*****  Plugin catchall (11.6 confidence) suggests   ************************

If you believe that httpd should be allowed open access on the  file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# grep httpd /var/log/audit/audit.log | audit2allow -M mypol
# semodule -i mypol.pp


Additional Information:
Source Context                system_u:system_r:httpd_t:s0
Target Context                unconfined_u:object_r:user_tmp_t:s0
Target Objects                 [ file ]
Source                        httpd
Source Path                   /usr/sbin/httpd
Port                          <Unknown>
Host                          serverX.example.com
Source RPM Packages           httpd-2.4.6-14.el7.x86_64
Target RPM Packages
Policy RPM                    selinux-policy-3.12.1-124.el7.noarch
Selinux Enabled               True
Policy Type                   targeted
Enforcing Mode                Enforcing
Host Name                     serverX.example.com
Platform                      Linux serverX.example.com 3.10.0-84.el7.x86_64 #1
                              SMP Tue Feb 4 16:28:19 EST 2014 x86_64 x86_64
Alert Count                   1
First Seen                    2014-02-20 13:55:56 EST
Last Seen                     2014-02-20 13:55:56 EST
Local ID                      160daebd-0359-4f72-9dde-46e7fd244e27

Raw Audit Messages
type=AVC msg=audit(1392922556.862:494): avc:  denied  { open } for  pid=24492
comm="httpd" path="/var/web-content/lab-content/index.html" dev="vda1"
ino=29062705 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:user_tmp_t:s0 tclass=file


type=SYSCALL msg=audit(1392922556.862:494): arch=x86_64 syscall=open success=no
exit=EACCES a0=7fda4c92eb40 a1=80000 a2=0 a3=0 items=0 ppid=24487 pid=24492
auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48
tty=(none) ses=4294967295 comm=httpd exe=/usr/sbin/httpd
subj=system_u:system_r:httpd_t:s0 key=(null)

Hash: httpd,httpd_t,user_tmp_t,file,open
```

Al mirar más de cerca los mensajes de auditoría sin formato, observará que Apache no puede acceder a **`/var/web-content/lab-content/index.html`**.

3. Resuelva el problema de SELinux que evita que Apache proporcione el contenido web.

   `/var/web-content` no es una ubicación estándar para contenido web de Apache. Muestre el contexto de **`/var/web-content`** de SELinux y la raíz del documento estándar, **`/var/www/html`**.

```
[root@serverX ~]# ls -d -Z /var/web-content /var/www/html
drwxr-xr-x. root root unconfined_u:object_r:var_t:s0   /var/web-content
```

```
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /var/www/html
```

Cree una regla de contextos de archivos que establezca el tipo predeterminado en **httpd_sys_content_t** para **/var/web-content** y todos los archivos debajo de este.

```
[root@serverX ~]# semanage fcontext -a -t httpd_sys_content_t '/var/web-
content(/.*)?'
```

Use el comando **restorecon** para establecer el contexto de SELinux para los archivos de **/var/web-content**.

```
[root@serverX ~]# restorecon -R /var/web-content/
```

4. Verifique que el problema de SELinux se haya resuelto y que Apache pueda proporcionar contenido web.

   Use su navegador web para actualizar el enlace **http://localhost/lab-content**. Ahora debería ver algo de contenido web.

```


This is the content for the SELinux chapter test.
```

5. Ejecute el comando **lab selinux grade** para confirmar sus hallazgos.

```
[root@serverX ~]# lab selinux grade
Confirming SELinux is in enforcing mode...PASS
Confirming files are in expected location...PASS
Confirming the Apache DocumentRoot is unchanged...PASS
Confirming the web content is accessible...PASS
```

Resumen

Habilitación y supervisión de Security Enhanced Linux (SELinux)

- **`getenforce`** muestra el modo de SELinux actual, que determina si las reglas de SELinux se aplican.
- La opción **`-Z`** para **`ls`** y **`ps`** muestra las etiquetas de contexto de SELinux en archivos y procesos.
- **`getsebool -a`** muestra todos los booleanos de SELinux y su valor actual.

Cambio de modos de SELinux

- **`setenforce`** modifica el modo actual de SELinux de un sistema.
- El modo predeterminado de SELinux de un sistema se define en el archivo **`/etc/selinux/config`**.

Cambio de contextos de SELinux

- El comando **`semanage fcontext`** se usa para administrar las reglas de políticas de SELinux que determinan el contexto predeterminado para archivos y directorios.
- **`restorecon`** aplica el contexto definido por la política de SELinux a archivos y directorios.
- Si bien el comando **`chcon`** puede cambiar los archivos de contexto de SELinux, no se debe usar porque es posible que el cambio no persista.

Cambio de booleanos de SELinux

- **`setsebool`** activa/desactiva reglas de políticas de SELinux.
- **`semanage boolean -l`** muestra el valor persistente de booleanos de SELinux.
- Las páginas del manual que finalizan con **`_selinux`** a menudo proporcionan información útil sobre booleanos de SELinux.

Solución de problemas de SELinux

- **`setroubleshootd`** genera los mensajes de registro en **`/var/log/messages`**.
- El comando **`sealert`** muestra información útil que ayuda con la solución de problemas de SELinux.

redhat. TRAINING

CAPÍTULO 8

CONEXIÓN DE USUARIOS Y GRUPOS DEFINIDOS POR LA RED

Descripción general	
Meta	Configurar sistemas para usar servicios de administración de identidades centrales.
Objetivos	Usar servicios de administración de identidades centralizados.
Secciones	• Uso de servicios de administración de identidades (y práctica)
Trabajo de laboratorio	• Conexión de usuarios y grupos definidos por la red

Uso de servicios de administración de identidad

Objetivos

Luego de completar esta sección, los estudiantes deberían poder usar servicios de administración de identidad centralizados.

Servicios de información del usuario y de autenticación

Necesidad de administración de identidad centralizada

Las infraestructuras de computación modernas tienden a constar de muchas máquinas, con varios servicios en ejecución. Mantener las cuentas de usuarios locales de todas estas máquinas y sus servicios en sincronización es una tarea abrumadora, más aún cuando las contraseñas deben mantenerse sincronizadas.

Una solución para esto es no almacenar información de las cuentas en sistemas locales, sino recuperar esta información de un almacenamiento centralizado. Tener la información del usuario y la información de autenticación asociada centralizadas también permite lo que se denomina *Single Sign-On* (SSO) (Inicio de sesión único). Con SSO, un usuario autentica una vez usando una contraseña (u otros medios) y luego obtiene una forma de vale o cookie que se puede usar para autenticar automáticamente a otros servicios.

Autenticación e información del usuario

Se necesitará un sistema de identidad centralizado para proporcionar al menos dos servicios:

1. *Información de la cuenta*: Esto incluye información como nombre de usuario, ubicación del directorio de inicio, UID y GID, membresías de grupos, etc. Las soluciones populares incluyen *LDAP* (Lightweight Directory Access Protocol), usada en varios productos como Active Directory y IPA Server, y *Network Information Services* (NIS).

2. *Información de autenticación*: Un medio para un sistema de validar que un usuario es quien dice que es. Esto se puede hacer al proporcionar un hash de contraseña criptográfico al sistema de cliente, o al enviar la contraseña (cifrada) al servidor, y recibir una respuesta. Un servidor LDAP puede proporcionar información de autenticación además de información de la cuenta. Kerberos solo proporciona servicios de autenticación SSO, y se usa típicamente junto con la información del usuario de LDAP. Kerberos se usa tanto en IPA Server como en Active Directory.

En un sistema Red Hat Enterprise Linux 7, **`/etc/passwd`** proporciona la información del usuario local, mientras que **`/etc/shadow`** proporciona la información de autenticación (en la forma de una contraseña con hash).

Conexión de un sistema a servidores LDAP y Kerberos centralizados

Authconfig
La configuración de un sistema Red Hat Enterprise Linux 7 para usar servicios de administración de identidad centralizados requiere la edición de varios archivos y la configuración de algunos daemons. Para conectar a servidores LDAP y Kerberos centrales, como mínimo, se deberán actualizar los siguientes archivos:

- **`/etc/openldap/ldap.conf`**: Para información sobre el servidor LDAP central y su configuración.
- **`/etc/krb5.conf`**: Para información sobre la infraestructura de Kerberos central.
- **`/etc/sssd/sssd.conf`**: Para configurar el *daemon de servicios de seguridad del sistema* (**`sssd`**), el daemon responsable de la recuperación y el almacenamiento en caché de la información del usuario e información de autenticación.
- **`/etc/nsswitch.conf`**: Para indicarle al sistema qué servicios de autenticación e información del usuario se deben usar.
- **`/etc/pam.d/*`**: Configuración de cómo se debe manejar la autenticación para varios servicios.
- **`/etc/openldap/cacerts`**: Para almacenar las *autoridades de certificación* (CA) raíz que pueden validar los certificados de SSL usados para identificar los servidores LDAP.

El daemon **`sssd`** deberá habilitarse e iniciarse para que el sistema pueda usarse.

Con esta cantidad de archivos y servicios para configurar, es fácil cometer un error. Red Hat Enterprise Linux 7 se envía con un conjunto de herramientas para automatizar estas configuraciones: **`authconfig`**. **`authconfig`** consta de tres herramientas relacionadas que pueden realizar las mismas acciones:

- **`authconfig`**: Una herramienta de línea de comandos. Esta herramienta se puede usar para automatizar configuraciones en varios sistemas. Los comandos usados con **`authconfig`** tienden a ser muy extensos, con múltiples opciones que se especifican. Esta herramienta se instala usando el paquete *authconfig*.
- **`authconfig-tui`**: La versión interactiva de **`authconfig`**. Usa una interfaz de texto guiada por un menú. Se puede usar sobre **`ssh`**. Esta herramienta se instala usando el paquete *authconfig*.
- **`authconfig-gtk`**: Esta versión inicia una interfaz gráfica. También se puede iniciar como **`system-config-authentication`**. Esta herramienta se instala usando el paquete **`authconfig-gtk`**.

Parámetros de LDAP necesarios
Para conectar a un servidor de LDAP central para obtener información del usuario, **`authconfig`** necesita varias configuraciones:

- El nombre del host de los servidores LDAP

- El *base DN* (nombre distinguido) de la parte del árbol de LDAP donde el sistema debe buscar usuarios. Generalmente, esto se ve de forma similar a **`dc=example,dc=com`**, o **`ou=People,o=PonyCorp`**. Esta información será proporcionada por su administrador de servidores de LDAP.
- Si se usa SSL/TLS para codificar comunicaciones con el servidor LDAP, el servidor LDAP ofrece un certificado CA raíz que puede validar el certificado.

Importante: Un sistema también necesitará que se instalen paquetes adicionales para proporcionar funcionalidad del cliente LDAP. La instalación de *sssd* proporcionará todas las dependencias necesarias.

Parámetros de Kerberos necesarios
Para configurar un sistema para que use un sistema Kerberos centralizado para la autenticación del usuario, **`authconfig`** necesitará las siguientes configuraciones:

- El nombre del *dominio Kerberos* que se utilizará. Un dominio Kerberos es un dominio de máquinas que usan un conjunto común de usuarios y servidores Kerberos para la autenticación.
- Uno o más *centros de distribución de claves* (KDC). Este es el nombre de host de sus servidores Kerberos.
- El nombre de host de uno o más *admin servers (servidores de administración)*. Esta es la máquina con la que el cliente hablará cuando desee cambiar su contraseña o realizar otras modificaciones de usuario. Generalmente, esta es la misma que la del KDC primario, pero puede ser una máquina diferente.

Además, un administrador puede especificar si DNS debe usarse para buscar el dominio que se usará para un nombre de host específico y para encontrar automáticamente los servidores de administración y los KDC. Se puede instalar un paquete adicional para ayudar a resolver problemas de Kerberos y para que funcionen con vales de Kerberos de la línea de comandos: *krb5-workstation*.

Uso de authconfig-gtk
Para usar **`authconfig-gtk`** para configurar un sistema para LDAP + Kerberos, use los siguientes pasos:

1. Instale todos los paquetes necesarios:

```
[student@demo ~]$ sudo yum -y install authconfig-gtk sssd krb5-workstation
```

2. Inicie **`authconfig-gtk`**, desde la línea de comandos o desde **Applications (Aplicaciones)** > **Sundry** > **Authentication (Autenticación)**. Ingrese la contraseña **`raíz`** cuando se la solicite.
3. En la pestaña **Identity & Authentication** (Identidad y autenticación), seleccione **LDAP** del menú desplegable **`User Account Database drop-down`**. Complete los campos **LDAP Search Base DN** (Nombre distinguido base de búsqueda de LDAP) y **LDAP Server** (Servidor LDAP).

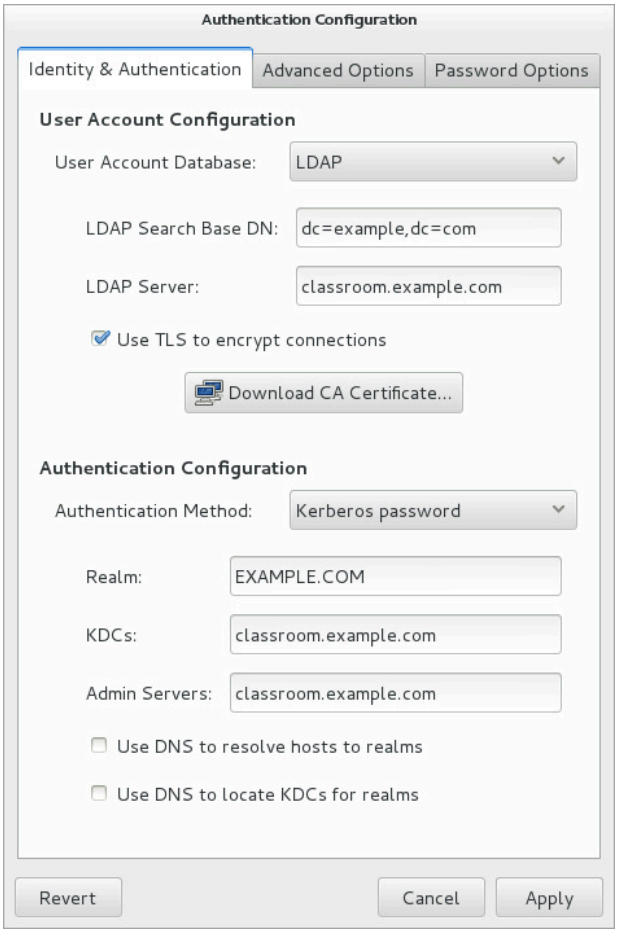

Figura 8.1: Ventana de authconfig-gtk principal

4. Si el servidor LDAP admite TLS, marque la casilla **Use TLS to encrypt connections** (Usar TLS para cifrar conexiones) y use el botón **Download CA Certificate** (Descargar certificado CA) para descargar el certificado CA.

5. En el menú desplegable **Authentication Method** (Método de autenticación), seleccione **Kerberos password** (Contraseña de Kerberos) y complete los campos **Realm** (Dominio), **KDCs** (KDC) y **Admin Servers** (Servidores de administración). Los últimos dos campos no están disponibles si la opción **Use DNS to locate KDCs for realms** (Usar DNS para localizar KDC para dominios) está marcada.

6. Si los directorios de inicio centrales no están disponibles, los usuarios pueden crear directorios en el primer inicio de sesión al marcar el cuadro **Create home directories on the first login** (Crear directorios de inicio en el primer inicio de sesión) en la pestaña **Advanced Options** (Opciones avanzadas).

7. Haga clic en el botón **Apply** (Aplicar) para guardar y activar los cambios. Esto escribirá todos los archivos de configuración relevantes y (re)iniciará el servicio **sssd**.

Advertencia

Debido a un error conocido (https://bugzilla.redhat.com/show_bug.cgi?id=1184639) en **`authconfig-6.2.8-8.el7`** genera un valor de krb5_realm falso como '**#**' en **`/etc/sssd/sssd.conf`**. Cuando utilice **`authconfig-gtk`**, se podrá evitar este problema si se elimina el valor predeterminado '**#**' del campo **`Realm`** (Dominio). Además, cuando utilice la línea de comandos de **`authconfig`**, asegúrese de utilizar la opción **`--krb5realm=`** para ingresar en un dominio cuando corresponda y verificar los archivos **`/etc/krb5.conf`** y **`/etc/sssd/sssd.conf`** en busca de valores dañados.

El soporte de producto de Red Hat proporcionó una versión de errata **`authconfig-6.2.8-10.el7`** que resuelve este problema para los entornos de producción. Consulte: https://rhn.redhat.com/errata/RHBA-2015-2403.html

Prueba de configuración
Para probar la configuración LDAP + Kerberos, un administrador puede simplemente intentar iniciar sesión en el sistema (mediante **`ssh`**) usando las credenciales de uno de los usuarios de red. Además, el comando **`getent`** se puede usar para recuperar información sobre un usuario de red, en la forma **`getent passwd <`*`USERNAME`*`>`**.

Importante: En la configuración predeterminada, **`sssd`** no enumerará usuarios de red cuando *no* se especifique un nombre de usuario para el comando **`getent`**. Esto se hace para mantener la pantalla de inicio de sesión gráfica despejada y para ahorrar tiempo y fuentes de red valiosos.

Conexión de un sistema a un servidor IPA

Red Hat proporciona una solución integrada para configurar LDAP y Kerberos: servidor IPA (Identity, Policy, and Auditing [Identidad, política y auditoría]). El servidor IPA proporciona LDAP y Kerberos, combinados con un conjunto de herramientas de administración basadas en la Web y de línea de comandos. Además de la información del usuario y de autenticación, el servidor IPA puede centralizar reglas **`sudo`**, claves públicas SSH, llaves de host SSH, certificados TLS, mapas de servicio de automontaje y mucho más.

Uso de ipa-client
Un sistema Red Hat Enterprise Linux 7 se puede configurar para usar un servidor IPA mediante el conjunto de herramientas **`authconfig`**, pero también existe una herramienta especializada: **`ipa-client-install`**. Este comando se puede instalar desde el paquete *ipa-client*, que extrae todas las dependencias (como *sssd*).

Uno de los beneficios de usar **`ipa-client-install`** es que puede recuperar casi toda la información necesaria de DNS (cuando es configurado por el servidor IPA o manualmente por un administrador), así como crear entradas de host y más en el servidor IPA. Esto permite que un administrador de servidores IPA establezca políticas de acceso, cree *directores de servicio* (p. ej., para exportaciones NFSv4) y más.

Cuando **`ipa-client-install`** se ejecuta sin ningún argumento, primero intentará recuperar información sobre el servidor IPA configurado para su dominio DNS de DNS. Si eso falla, se le solicitará al administrador la información necesaria, como el nombre del dominio del servidor de IPA y el dominio que se usará. Otra información que debe proporcionarse

es el nombre de usuario y la contraseña de una cuenta que tiene permitido crear nuevas entradas de la máquina en el servidor IPA. Se puede usar la cuenta del administrador del servidor IPA predeterminada (**admin**), a menos que se haya creado otra cuenta para esto.

A continuación, se muestra un ejemplo de una configuración guiada (mayormente) por DNS:

```
[student@desktop ~]$ sudo ipa-client-install
Discovery was successful!
Hostname: desktop.domain0.example.com
Realm: DOMAIN0.EXAMPLE.COM
DNS Domain: server.domain0.example.com
IPA Server: server.domain0.example.com
BaseDN: dc=server,dc=domain0,dc=example,dc=com

Continue to configure the system with these values? [no]: yes
User authorized to enroll computers: admin
Synchronizing time with KDC...
Password for admin@DOMAIN0.EXAMPLE.COM: redhat123
Successfully retrieved CA cert
    Subject:     CN=Certificate Authority,O=DOMAIN0.EXAMPLE.COM
    Issuer:      CN=Certificate Authority,O=DOMAIN0.EXAMPLE.COM
    Valid From:  Thu Feb 27 13:31:04 2014 UTC
    Valid Until: Mon Feb 27 13:31:04 2034 UTC

Enrolled in IPA realm DOMAIN0.EXAMPLE.COM
Created /etc/ipa/default.conf
New SSSD config will be created
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm DOMAIN0.EXAMPLE.COM
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Client configuration complete.
```

Es posible especificar toda la información necesaria como argumentos de línea de comando, permitiendo configuraciones desatendidas como parte de una configuración inicial del sistema; por ejemplo, desde un *kickstart*. Consulte la página del manual para **ipa-client-install**(1) para obtener más información.

Unión de un sistema con Active Directory

Red Hat Enterprise Linux 7 presenta varios métodos de unión de un sistema con Active Directory. Los administradores pueden elegir instalar el paquete *samba-winbind* y configurar **winbind** a través de la familia de herramientas **authconfig**, o los administradores pueden instalar los paquetes *sssd* y *realmd* y usar **sssd** y el comando **realm**.

nota

El comando **realm** también se puede usar para unirse a dominios de Kerberos, o dominios de servidores IPA, pero la configuración final será ligeramente diferente; por ejemplo, los usuarios tendrán **@domain** anexado a sus nombres de usuario. **ipa-client-install** es el método preferido para unirse a dominios IPA.

nota

Debido a que no hay un servidor de Active Directory ejecutándose en el aula, no hay una posibilidad actual de practicar estos pasos.

El siguiente es un ejemplo del uso de **realmd** para unirse un dominio de Active Directory y permitir a los usuarios de Active Directory iniciar sesión en el sistema local. En este ejemplo, se supone que el dominio de Active Directory se denomina **domain.example.com**.

1. Instale los paquetes necesarios: *realmd*.

```
[student@demo ~]$ sudo yum -y install realmd
```

2. Descubra la configuración para el dominio **domain.example.com**.

```
[student@demo ~]$ sudo realm discover domain.example.com
```

3. Únase al dominio de Active Directory; esto instalará todos los paquetes necesarios y configurará **sssd**, **pam**, **/etc/nsswitch.conf**, etcétera.

```
[student@demo ~]$ sudo realm join domain.example.com
```

   Esto intentará unir el sistema local con Active Directory usando la cuenta **Administrator**; ingrese la contraseña para esta cuenta cuando se lo solicite. Para usar una cuenta diferente, use el argumento **--user**.

4. Las cuentas de Active Directory ahora se pueden utilizar en el sistema local, pero los inicios de sesión usando Active Directory aún están deshabilitados. Para habilitar inicios de sesión, use el siguiente comando:

```
[student@demo ~]$ sudo realm permit --realm domain.example.com --all
```

   Para solo permitir a ciertos usuarios iniciar sesión, reemplace **--all** con una lista de esos usuarios. Por ejemplo:

```
[student@demo ~]$ sudo realm permit --realm domain.example.com DOMAIN\\Itchy DOMAIN\
\Scratchy
```

nota

De forma predeterminada, los usuarios del dominio deben usar su nombre calificado completo para iniciar sesión; p. ej., **ipauser@ipa.example.com** para usuarios IPA o **DOMAIN\Picard** para Active Directory. Para deshabilitar esto, cambie la configuración de **use_fully_qualified_names** en el bloque del dominio correcto en **/etc/sssd/sssd.conf** a False (Falso) o elimínelo por completo; luego reinicie el servicio **sssd**.

Referencias

Páginas del manual: **authconfig**(8), **authconfig-tui**(8), **authconfig-gtk**(8), **sssd**(8), **sssd-ipa**(8), **sssd.conf**(5), **sssd-ad** y **realm**(8)

Práctica: Conexión a un servidor LDAP y Kerberos central

En este trabajo de laboratorio, conectará su sistema **desktopX** para convertirlo en un cliente del servidor LDAP que se ejecuta en **classroom.example.com**. Configurará su sistema **desktopX** para usar la infraestructura Kerberos proporcionada por **classroom.example.com** para obtener una autenticación adicional.

Recursos:	
Archivos:	**http://&clrmfqdn;/pub/example-ca.crt**
Máquinas:	**desktopX**

Resultados:
desktopX configurado para información de usuario de LDAP y autenticación de Kerberos desde **classroom.example.com**.

Andes de comenzar
- Restablezca su sistema **desktopX**.

Para simplificar la administración del usuario, su empresa ha decidido cambiar a administración de usuario centralizada. Otro equipo ya ha configurado todos los servicios de LDAP y Kerberos obligatorios. Los directorios iniciales centralizados aún no están disponibles, de modo que el sistema debe configurarse para crear directorios iniciales locales cuando un usuario inicie sesión por primera vez.

Dada la siguiente información, configure su sistema **desktopX** para que use la información de usuario del servidor LDAP y los servicios de autenticación del KDC de Kerberos. Los registros del servicio DNS para el dominio aún no se han configurado, de modo que tendrá que configurar manualmente los parámetros de Kerberos.

Nombre	Valor
Servidor LDAP	**ldap://classroom.example.com**
DN de base de LDAP	**dc=example,dc=com**
Usar TLS	Sí
CA raíz	**http://classroom.example.com/pub/example-ca.crt**
Dominio de Kerberos	**EXAMPLE.COM**
KDC de Kerberos	**classroom.example.com**
Servidor de administración de Kerberos:	**classroom.example.com**

1. Comience por instalar los paquetes necesarios: *sssd*, *krb5-workstation* y *authconfig-gtk*.

   1.1.
```
[student@desktopX ~]$ sudo yum -y install sssd authconfig-gtk krb5-workstation
```

2. Inicie la aplicación **Authentication Configuration** (Configuración de autenticación), luego aplique la configuración de la tabla para las opciones LDAP y Kerberos.

   2.1. Inicie **`system-config-authentication`** desde la línea de comandos o inicie **Applications (Aplicaciones)** > **Sundry** > **Authentication (Autenticación)**. Ingrese la contraseña de **`student`** (**`student`**) cuando se le solicite.

   2.2. Asegúrese de que la pestaña **Identity & Authentication** (Identidad y autenticación) esté abierta.

   2.3. En **User Account Database** (Base de datos de la cuenta del usuario), seleccione **LDAP**.

   2.4. Ingrese **`dc=example,dc=com`** en el campo **LDAP Search Base DN** (DN de base de búsqueda de LDAP) y **`classroom.example.com`** en el campo **LDAP Server** (Servidor LDAP).

   2.5. Asegúrese de que el cuadro **Use TLS to encrypt connections** (Usar TLS para cifrar conexiones) esté marcado, y luego haga clic en el botón **Download CA Certificate**... (Descargar certificado de CA...).

   2.6. Ingrese **`http://classroom.example.com/pub/example-ca.crt`** en el campo **Certificate URL** (URL del certificado) y, luego haga clic en **OK** (Aceptar).

   2.7. Seleccione **Kerberos password** (Contraseña de Kerberos) en el menú desplegable **Authentication Method** (Método de autenticación) y quite la marca de los dos cuadros **Use DNS...** (Usar DNS...).

   2.8. Ingrese **`EXAMPLE.COM`** en el campo **REALM** (DOMINIO) y **`classroom.example.com`** en los campos **KDCs** (KDC) y **Admin Servers** (Servidores de administración).

   2.9. Cambie a la pestaña **Advanced Options** (Opciones avanzadas) y coloque una marca de verificación en el cuadro **Create home directories on the first login** (Crear directorios iniciales en el primer inicio de sesión).

   2.10 Haga clic en el botón **Apply** (Aplicar) para aplicar los cambios.

3. Use tanto **`getent`** como **`ssh`** para verificar su trabajo. Puede usar el nombre de usuario **`ldapuser`*`X`*** (donde ***`X`*** es el número de su estación) con la contraseña **`kerberos`**. Tenga en cuenta que sus usuarios aún no tienen un directorio de inicio montado.

   3.1.
   ```
   [student@desktopX ~]$ getent passwd ldapuserX
   ldapuserX:*:170X:170X:LDAP Test User X:/home/guests/ldapuserX:/bin/bash
   ```

   3.2.
   ```
   [student@desktopX ~]$ ssh ldapuserX@localhost
   The authenticity of host 'localhost (::1)' can't be established.
   EDCSA key fingerprint is XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX.
   Are you sure you want to continue connecting (yes/no)? yes
   Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
   ldapuserX@localhost's password: kerberos
   Creating home directory for ldapuserX.
   [ldapuserX@desktopX ~]$ pwd
   /home/guests/ldapuserX
   [ldapuserX@desktopX ~]$ ls -a
   .   .bash_history  .bash_profile  .cache   .mozilla
   ```

```
..  .bash_logout   .bashrc        .config
[ldapuserX@desktopX ~]$ logout
```

Trabajo de laboratorio: Conexión de usuarios y grupos definidos por la red

En este trabajo de laboratorio, configurará su sistema **desktopX** para convertirlo en un cliente del servidor IPA que se ejecuta en **serverX**.

Recursos:	
Máquinas:	**desktopX** y **serverX**

Resultados:
Su sistema **desktopX** debe usar los usuarios y grupos de red definidos por el servidor IPA que se ejecuta en **serverX** tanto para la información del usuario como para la autenticación.

Andes de comenzar
Si aún no lo ha hecho al inicio del ejercicio anterior:

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo. Observación: Este paso llevará unos 15 minutos aproximadamente.

```
[student@serverX ~]$ lab ipaclient setup
```

Siempre realice este paso:

- Restablezca su sistema **desktopX**. Puede restablecer su sistema **desktopX** mientras la configuración de **serverX** aún se está ejecutando.
- Espere a que la configuración en **serverX** finalice antes de continuar.

En la búsqueda de su empresa de un sistema de autenticación e información del usuario central, ha resuelto usar un servidor IPA para la administración central de usuarios. Otro departamento ya ha configurado un servidor IPA en su máquina **serverX**. Este servidor IPA está configurado con todos los registros DNS SRV relevantes para la siguiente configuración:

Nombre	Valor
Dominio	**SERVER*X*.EXAMPLE.COM**, donde ***X*** es el número de su estación.
Dominio	**server*X*.example.com**, donde ***X*** es el número de su estación. Observe que su máquina **desktopX** no es parte de este dominio DNS.
Usuario administrativo	**admin**
Contraseña	**redhat123**

Ya se ha configurado a un usuario para que realice la evaluación. El nombre de usuario es **ipauser** y la contraseña es **password**. Debido a la política de contraseñas, esta contraseña deberá cambiarse en el primer inicio de sesión. Cambie esta contraseña a **redhat123**.

Los directorios de inicio centrales aún no se han configurado, de modo que, por ahora, configure el sistema para que cree automáticamente un nuevo directorio de inicio local cuando un usuario inicia sesión por primera vez.

Cuando haya finalizado su trabajo, ejecute **`lab ipaclient grade`** en su máquina **`desktopX`** para verificar su trabajo.

1. Instale el paquete *ipa-client* en su máquina **`desktopX`**.

2. Configure su sistema, con **`ipa-client-install`**, para usar la configuración del servidor IPA para el dominio DNS de **`server`*`X`*`.example.com`**. Los directorios de inicio deben crearse automáticamente y, durante este proceso, NTP no se debe configurar.

3. Verifique que ahora pueda iniciar sesión satisfactoriamente en **`desktopX`** con el usuario **`ipauser`** mediante el uso de **`ssh`**. La contraseña inicial es **`password`**, pero se debe cambiar a **`redhat123`**. Debido al requisito de cambio de contraseña, tendrá que iniciar sesión dos veces.

4. Ejecute **`lab ipaclient grade`** en su máquina **`desktopX`** para verificar su trabajo.

Solución

En este trabajo de laboratorio, configurará su sistema **desktopX** para convertirlo en un cliente del servidor IPA que se ejecuta en **serverX**.

Recursos:	
Máquinas:	**desktopX** y **serverX**

Resultados:
Su sistema **desktopX** debe usar los usuarios y grupos de red definidos por el servidor IPA que se ejecuta en **serverX** tanto para la información del usuario como para la autenticación.

Andes de comenzar
Si aún no lo ha hecho al inicio del ejercicio anterior:

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo. Observación: Este paso llevará unos 15 minutos aproximadamente.

```
[student@serverX ~]$ lab ipaclient setup
```

Siempre realice este paso:

- Restablezca su sistema **desktopX**. Puede restablecer su sistema **desktopX** mientras la configuración de **serverX** aún se está ejecutando.
- Espere a que la configuración en **serverX** finalice antes de continuar.

En la búsqueda de su empresa de un sistema de autenticación e información del usuario central, ha resuelto usar un servidor IPA para la administración central de usuarios. Otro departamento ya ha configurado un servidor IPA en su máquina **serverX**. Este servidor IPA está configurado con todos los registros DNS SRV relevantes para la siguiente configuración:

Nombre	Valor
Dominio	**SERVER*X*.EXAMPLE.COM**, donde ***X*** es el número de su estación.
Dominio	**server*X*.example.com**, donde ***X*** es el número de su estación. Observe que su máquina **desktopX** no es parte de este dominio DNS.
Usuario administrativo	**admin**
Contraseña	**redhat123**

Ya se ha configurado a un usuario para que realice la evaluación. El nombre de usuario es **ipauser** y la contraseña es **password**. Debido a la política de contraseñas, esta contraseña deberá cambiarse en el primer inicio de sesión. Cambie esta contraseña a **redhat123**.

Los directorios de inicio centrales aún no se han configurado, de modo que, por ahora, configure el sistema para que cree automáticamente un nuevo directorio de inicio local cuando un usuario inicia sesión por primera vez.

Cuando haya finalizado su trabajo, ejecute **lab ipaclient grade** en su máquina **desktopX** para verificar su trabajo.

1. Instale el paquete *ipa-client* en su máquina **desktopX**.

   1.1.
   ```
   [student@desktopX ~]$ sudo yum -y install ipa-client
   ```

2. Configure su sistema, con **ipa-client-install**, para usar la configuración del servidor IPA para el dominio DNS de **server*X*.example.com**. Los directorios de inicio deben crearse automáticamente y, durante este proceso, NTP no se debe configurar.

   2.1.
   ```
   [student@desktopX ~]$ sudo ipa-client-install --domain=serverX.example.com --no-
   ntp --mkhomedir
   Discovery was successful!
   Hostname: desktopX.example.com
   Realm: SERVERX.example.com
   DNS Domain: serverX.example.com
   IPA Server: serverX.example.com
   BaseDN: dc=serverX,dc=example,dc=com

   Continue to configure the system with these values? [no]: yes
   User authorized to enroll computers: admin
   Password for admin@SERVERX.EXAMPLE.COM: redhat123
   ...
   Client configuration complete.
   ```

3. Verifique que ahora pueda iniciar sesión satisfactoriamente en **desktopX** con el usuario **ipauser** mediante el uso de **ssh**. La contraseña inicial es **password**, pero se debe cambiar a **redhat123**. Debido al requisito de cambio de contraseña, tendrá que iniciar sesión dos veces.

   3.1.
   ```
   [student@desktopX ~]$ ssh ipauser@desktopX.example.com
   ipauser@desktopX.example.com's password: password
   Password expired. Change your password now.
   Creating home directory for ipauser.
   WARNING: Your password has expired.
   You must change your password now and login again!
   Changing password for user ipauser.
   Current password: password
   New password: redhat123
   Retype new password: redhat123
   passwd: all authentication tokens updated successfully.
   Connection to desktopX.example.com closed.
   [student@desktopX ~]$ ssh ipauser@desktopX.example.com
   ipauser@desktopX.example.com's password: redhat123
   Last login: Wed Feb 26 05:19:15 2014 from desktopX.example.com
   -sh-4.2$ logout
   ```

4. Ejecute **lab ipaclient grade** en su máquina **desktopX** para verificar su trabajo.

   4.1.
   ```
   [student@desktopX ~]$ lab ipaclient grade
   ```

Resumen

Uso de servicios de administración de identidad

- **`authconfig{,-gtk,-tui}`** se puede usar para configurar un sistema para usar servicios de administración de identidad centralizados.
- **`sssd`** se configura para recuperar, validar y almacenar en memoria caché información de autenticación y del usuario en segundo plano.

redhat. TRAINING

CAPÍTULO 9

ADICIÓN DE DISCOS, PARTICIONES Y SISTEMAS DE ARCHIVOS A UN SISTEMA LINUX

Descripción general	
Meta	Crear y administrar discos, particiones y sistemas de archivos desde la línea de comandos.
Objetivos	• Gestionar particiones y sistemas de archivos sencillos. • Administrar espacio swap (intercambio).
Secciones	• Adición de particiones, sistemas de archivos y montajes persistentes (y práctica) • Adición y habilitación de espacio swap (intercambio) (y práctica)
Trabajo de laboratorio	• Adición de discos, particiones y sistemas de archivos a un sistema Linux

Adición de particiones, sistemas de archivos y montajes persistentes

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Crear y eliminar particiones de disco en discos con esquema de partición MBR usando **`fdisk`**.
- Crear y eliminar particiones de disco en discos con esquema de partición GPT usando **`gdisk`**.
- Formatear dispositivos con sistemas de archivos usando **`mkfs`**.
- Montar sistemas de archivos en el árbol del directorio.

Partición del disco

La partición de discos permite la división de un disco duro en varias unidades de almacenamiento lógico denominadas particiones. Al separar un disco en particiones, los administradores de sistemas pueden usar diferentes particiones para realizar diferentes funciones. Algunos ejemplos de situaciones en las cuales la partición del disco es necesaria o beneficiosa son:

- Limitar espacio disponible para aplicaciones o usuarios.
- Permitir varios arranques de diferentes sistemas operativos desde el mismo disco.
- Separar archivos de programa y de sistemas operativos de archivos de usuarios.
- Crear un área separada para el swapping (intercambio) de memoria virtual del sistema operativo.
- Limitar el uso de espacio en disco para mejorar el rendimiento de herramientas de diagnóstico e imágenes de copia de seguridad.

Esquema de partición MBR

Desde 1982, el esquema de partición de *registro de arranque maestro (Master Boot Record, MBR)* ha dictado cómo los discos se deben particionar en sistemas que ejecutan firmware de BIOS. Este esquema admite un máximo de cuatro particiones principales. En sistemas Linux, con el uso de particiones extendidas y lógicas, el administrador puede crear un máximo de 15 unidades. Dado que los datos del tamaño de la partición se almacenan como valores de 32 bits, los discos particionados con el esquema MBR tienen un límite de tamaño de disco y partición máximo de 2 TiB.

Con la aparición de discos duros de cada vez más capacidad, el límite de tamaño de disco y partición de 2 TiB del esquema de partición MBR antiguo ya no es un límite teórico sino un problema del mundo real que se presenta cada vez con más frecuencia en entornos de producción. Como consecuencia, el esquema MBR heredado está en proceso de ser sustituido por el nuevo *esquema GUID Partition Table (GPT)* para la partición de disco.

Esquema de partición de GPT
Para sistemas que ejecutan *firmware Unified Extensible Firmware Interface (UEFI),* GPT es el estándar para el diseño de tablas de partición en discos duros físicos. GPT es parte del estándar UEFI y aborda muchas de las limitaciones impuestas por el antiguo esquema basado en MBR. Según las especificaciones de UEFI, de forma predeterminada, GPT admite hasta 128 particiones. A diferencia de MBR, que usa 32 bits para almacenar información de tamaño y direcciones en bloques lógicos, GPT asigna 64 bits para direcciones en bloques lógicos. Esto asigna GPT para incluir particiones y discos de hasta 8 *zebibyte (ZiB)*, u 8 mil millones de tebibytes.

nota

El límite de 8 ZiB de GPT se basa en un tamaño de bloque de 512 bytes. Con proveedores de discos duros que cambian a bloques de 4096 bytes, este límite aumentará a 64 ZiB.

Además de abordar las limitaciones del esquema de partición MBR, GPT también ofrece algunas funciones y beneficios adicionales. Como lo indica su nombre, GPT usa GUID de 128 bits para identificar de forma única cada disco y partición. En contraste con MBR, que tiene un único punto de falla, GPT ofrece redundancia de la información de su tabla de particiones. El GPT principal reside en el cabezal del disco, mientras que una copia de seguridad, el GPT secundario, se aloja en el extremo del disco. Además, GPT emplea el uso de la suma de comprobación CRC para detectar errores y daños en la tabla de particiones y el encabezado de GPT.

Administración de particiones MBR con fdisk

Los editores de particiones son programas que permiten a los administradores hacer cambios en particiones de discos, como crear particiones, eliminar particiones y cambiar el tipo de partición. En el caso de discos con esquema de partición MBR, el editor de particiones **`fdisk`** se puede usar para realizar estas operaciones.

Creación de particiones de disco MBR
La creación de una partición de disco estilo MBR incluye ocho pasos:

1. Especifique el dispositivo de disco donde creará la partición.

   Como usuario **`raíz`**, ejecute el comando **`fdisk`** y especifique el nombre del dispositivo de disco como un argumento. Esto iniciará el comando **`fdisk`** en modo interactivo, y presentará un prompt de **`comando`**.

```
[root@serverX ~]# fdisk /dev/vdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help):
```

2. Solicite una nueva partición primaria o extendida.

Ingrese **n** para solicitar una nueva partición y especifique si esta debe ser creada como una *partición* primaria *o* extendida. La selección predeterminada es el tipo de partición *primaria*.

```
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
```

nota

En el caso de situaciones donde se necesitan más de cuatro particiones en un disco, este límite se puede omitir al crear tres particiones primarias y una partición extendida. Esta partición extendida sirve como contenedor dentro del cual se pueden crear varias particiones lógicas.

3. Especifique un número de partición.

   Este número de partición sirve como número de identificación de la nueva partición en el disco para usar en futuras operaciones de partición. El valor predeterminado es el número de partición no usado más bajo.

```
Partition number (1-4, default 1): 1
```

4. Especifique el primer sector en el disco donde se iniciará la nueva partición.

   El valor predeterminado es el primer sector disponible en el disco.

```
First sector (2048-20971519, default 2048): 2048
```

5. Especifique el último sector en el disco donde finalizará la nueva partición.

   El valor predeterminado es el último de los sectores disponibles, no asignados, contiguos al primer sector de la nueva partición.

```
Last sector, +sectors or +size{K,M,G} (6144-20971519, default 20971519): 1050623
```

   Además del número de sector final, **fdisk** también puede aceptar un número que represente el tamaño deseado de la partición expresado en sectores.

```
Last sector, +sectors or +size{K,M,G} (6144-20971519, default 20971519): +52488
```

   La opción de entrada final, y la más simple para el usuario, ofrecida por **fdisk** es especificar el tamaño de la nueva partición en unidades de KiB, MiB o GiB.

```
Last sector, +sectors or +size{K,M,G} (6144-20971519, default 20971519): +512M
```

Una vez que se ingresa la delimitación final de la partición, **fdisk** mostrará una confirmación de la creación de la partición.

```
Partition 1 of type Linux and of size 512 MiB is set
```

6. Defina el tipo de partición.

   Si la partición recientemente creada debe tener un tipo diferente de *Linux*, ingrese el comando **t** para cambiar un tipo de partición. Ingrese el código hex para el nuevo tipo de partición. En caso de ser necesario, con el comando **L**, se puede mostrar una tabla de códigos hex para todos los tipos de partición. La configuración correcta del tipo de partición es fundamental, dado que algunas herramientas se basan en esta para funcionar adecuadamente. Por ejemplo, cuando el kernel de Linux encuentra una partición de tipo *0xfd*, Linux RAID, intentará iniciar automáticamente el volumen de RAID.

```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 82
Changed type of partition 'Linux' to 'Linux swap / Solaris'
```

7. Guarde los cambios de la tabla de particiones.

   Emita el comando **w** para finalizar la solicitud de creación de la partición; para ello, escriba los cambios en la tabla de particiones del disco y salga del programa **fdisk**.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource
busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

8. Inicie una nueva lectura del kernel de la nueva tabla de particiones.

   Ejecute el comando **partprobe** con el nombre del dispositivo del disco como argumento para forzar una nueva lectura de su tabla de particiones.

```
[root@serverX ~]# partprobe /dev/vdb
```

Importante

El programa **fdisk** pone en cola todas las ediciones de la tabla de particiones y las escribe en el disco solo cuando el administrador emite el comando **w** para escribir todos los cambios de la tabla de particiones en el disco. Si el nuevo comando **w** no se ejecuta antes de salir de la sesión de **fdisk** interactiva, todos los cambios solicitados para la tabla de particiones se descartarán y la tabla de particiones del disco permanecerá igual. Esta función es especialmente útil cuando se emiten comandos erróneos a **fdisk**. Para descartar los comandos erróneos y evitar consecuencias no deseadas, simplemente salga de **fdisk** sin guardar los cambios de la tabla de particiones.

Eliminación de particiones del disco MBR

Se deben seguir cinco pasos para eliminar una partición de un disco con un diseño de partición MBR usando **fdisk**.

1. Especifique el disco que contiene la partición que se eliminará.

   Ejecute el comando **fdisk** y especifique el nombre del dispositivo de disco como un argumento.

```
[root@serverX ~]# fdisk /dev/vdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help):
```

2. Identifique el número de partición de la partición que se eliminará.

   Ingrese **p** para imprimir la tabla de particiones y **fdisk** mostrará información sobre el disco y sus particiones.

```
Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xd2368130

   Device Boot      Start         End      Blocks   Id  System
/dev/vdb1            2048     1050623      524288   82  Linux swap / Solaris
```

3. Solicite la eliminación de la partición.

   Ingrese el comando **d** para iniciar la eliminación de la partición y especifique el número de partición de la partición que se eliminará.

```
Command (m for help): d
Selected partition 1
Partition 1 is deleted
```

4. Guarde los cambios de la tabla de particiones.

   Emita el comando **w** para finalizar la solicitud de eliminación de la partición; para ello, escriba los cambios en la tabla de particiones del disco.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource
 busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

5. Inicie una nueva lectura del kernel de la nueva tabla de particiones.

   Informe al kernel que vuelva a leer la tabla de particiones con **partprobe**.

```
[root@serverX ~]# partprobe /dev/vdb
```

Administración de particiones GPT con gdisk

En el caso de discos con esquema de partición GPT, el editor de particiones **gdisk** se puede usar para administrar particiones.

Advertencia

Si bien se ha agregado el soporte GPT a **fdisk**, aún se considera experimental, de modo que se debe usar el comando **gdisk** para hacer cambios en las particiones en discos particionado con el esquema de partición GPT.

Creación de particiones de disco GPT

Son ocho los pasos que se requieren para crear una partición de estilo GPT.

1. Especifique el dispositivo de disco donde creará la partición.

   Ejecute el comando **gdisk** y especifique el nombre del dispositivo de disco como un argumento. Esto iniciará el comando **gdisk** en modo interactivo, y presentará un prompt de **comando**.

```
[root@serverX ~]# gdisk /dev/vdb
GPT fdisk (gdisk) version 0.8.6

Partition table scan:
  MBR: not present
  BSD: not present
```

```
  APM: not present
  GPT: not present

Creating new GPT entries.

Command (? for help):
```

2. Solicite una nueva partición.

   Ingrese **n** para crear una nueva partición.

```
Command (? for help): n
```

3. Especifique el número de partición.

   Este número de partición sirve como número de identificación de la partición en el disco para usar en futuras operaciones de partición. El valor predeterminado es el número de partición no usado más bajo.

```
Partition number (1-128, default 1): 1
```

4. Especifique la ubicación del disco desde donde se iniciará la nueva partición.

   gdisk permite dos tipos de entradas diferentes. El primer tipo de entrada es un número de sector de disco absoluto que representa el primer sector de la nueva partición.

```
First sector (34-20971486, default = 2048) or {+-}size{KMGTP}: 2048
```

   El segundo tipo de entrada indica el sector de inicio de la partición por su posición relativa al primero o último sector del primer bloque contiguo de sectores libres en el disco. Al usar este formato de posición de sector relativo, la entrada se especifica en unidades de KiB, MiB, GiB, TiB o PiB.

   Por ejemplo, un valor de **+**512 M significa una posición de sector que está 512 MiB **luego** del comienzo del siguiente grupo de sectores disponibles contiguos. Por otra parte, un valor de **-**512 M denota un sector posicionado 512 MiB *antes* del final de este grupo de sectores disponibles contiguos.

5. Especifique el último sector en el disco donde finalizará la nueva partición.

   El valor predeterminado es el último de los sectores disponibles, no asignados, contiguos al primer sector de la nueva partición.

```
Last sector (2048-20971486, default = 20971486) or {+-}size{KMGTP}: 1050623
```

   Además del número de sector de finalización absoluto, **gdisk** también ofrece la opción de entrada más simple para el usuario de especificar la delimitación final de la nueva partición en unidades de KiB, MiB, GiB, TiB, o PiB desde el comienzo o el final del grupo de sectores disponibles contiguos. Un valor de **+**512 M significa una posición de partición final de 512 MiB **luego** del primer sector.

```
Last sector (2048-20971486, default = 20971486) or {+-}size{KMGTP}: +512M
```

Un valor de **-**512 M indica una posición de partición final de 512 MiB *antes* del final de sectores disponibles contiguos.

```
Last sector (2048-20971486, default = 20971486) or {+-}size{KMGTP}: -512M
```

6. Defina el tipo de partición.

   Las nuevas particiones creadas por **gdisk** se establecen de forma predeterminada en el sistema de archivos de tipo *Linux*. Si se desea un tipo de partición diferente, ingrese el código hex correspondiente. En caso de ser necesario, con el comando **L**, se puede mostrar una tabla de códigos hex para todos los tipos de partición.

```
Current type is 'Linux filesystem'

Hex code or GUID (L to show codes, Enter = 8300): 8e00
Changed type of partition to 'Linux LVM'
```

7. Guarde los cambios de la tabla de particiones.

   Emita el comando **w** para finalizar la solicitud de creación de la partición; para ello, escriba los cambios en la tabla de particiones del disco. Ingrese **y** cuando **gdisk** solicite una confirmación final.

```
Command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!

Do you want to proceed? (Y/N): y
OK; writing new GUID partition table (GPT) to /dev/vdb.
The operation has completed successfully.
```

8. Inicie una nueva lectura del kernel de la nueva tabla de particiones.

   Ejecute el comando **partprobe** con el nombre del dispositivo del disco como argumento para forzar una nueva lectura de su tabla de particiones.

```
[root@serverX ~]# partprobe /dev/vdb
```

Importante

El programa **gdisk** pone en cola todas las ediciones de la tabla de particiones y las escribe en el disco solo cuando el administrador emite el comando **w** para escribir todos los cambios de la tabla de particiones en el disco. Si el nuevo comando **w** no se ejecuta antes de salir de la sesión de **gdisk** interactiva, todos los cambios solicitados para la tabla de particiones se descartarán y la tabla de particiones del disco permanecerá igual. Esta función es especialmente útil cuando se emiten comandos erróneos a **gdisk**. Para descartar los comandos erróneos y evitar consecuencias no deseadas, simplemente salga de **gdisk** sin guardar los cambios de la tabla de particiones.

Eliminación de particiones del disco GPT

Son cinco los pasos necesarios para eliminar una partición de un disco con un diseño de partición GPT usando **gdisk**.

1. Especifique el disco que contiene la partición que se eliminará.

   Ejecute el comando **gdisk** y especifique el nombre del dispositivo de disco como un argumento.

```
[root@serverX ~]# gdisk /dev/vdb
GPT fdisk (gdisk) version 0.8.6

Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present

Found valid GPT with protective MBR; using GPT.

Command (? for help):
```

2. Identifique el número de partición de la partición que se eliminará.

   Ingrese **p** para imprimir la tabla de particiones. Anote el número en el campo *Number* (Número) de la partición que se eliminará.

```
Command (? for help): p
Disk /dev/vdb: 20971520 sectors, 10.0 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): 8B181B97-5259-4C8F-8825-1A973B8FA553
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 20971486
Partitions will be aligned on 2048-sector boundaries
Total free space is 19922877 sectors (9.5 GiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048         1050623   512.0 MiB   8E00  Linux LVM
```

3. Solicite la eliminación de la partición.

   Ingrese el comando **d** para iniciar la eliminación de la partición.

```
Command (? for help): d
Using 1
```

4. Guarde los cambios de la tabla de particiones.

   Emita el comando **w** para finalizar la solicitud de eliminación de la partición; para ello, escriba los cambios en la tabla de particiones del disco. Ingrese **y** cuando **gdisk** solicite una confirmación final.

```
Command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!

Do you want to proceed? (Y/N): y
OK; writing new GUID partition table (GPT) to /dev/vdb.
The operation has completed successfully.
```

5. Inicie una nueva lectura del kernel de la nueva tabla de particiones.

   Informe al kernel que vuelva a leer la tabla de particiones con **partprobe**.

```
[root@serverX ~]# partprobe /dev/vdb
```

Creación de sistemas de archivos

Luego de haberse creado un dispositivo de bloque, el siguiente paso es aplicar un formato de sistema de archivos. Un sistema de archivos aplica una estructura al dispositivo de bloque de modo que se puedan almacenar y recuperar datos de este. Red Hat Enterprise Linux admite muchos tipos de sistema de archivos diferentes, pero dos tipos comunes son **xfs** y **ext4**. **xfs** se utiliza de forma predeterminada en **anaconda**, el instalador de Red Hat Enterprise Linux.

El comando **mkfs** se puede usar para aplicar un sistema de archivos a un dispositivo de bloque. Si no se especifica un tipo específico, se usará un sistema de archivos de tipo extendido dos (ext2), el cual no es deseable para muchos usos. Para especificar el tipo de sistema de archivos, se debe usar un **-t**.

```
[root@serverX ~]# mkfs -t xfs /dev/vdb1
meta-data=/dev/vdb1              isize=256    agcount=4, agsize=16384 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0
data     =                       bsize=4096   blocks=65536, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal log           bsize=4096   blocks=853, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

Montaje de sistemas de archivos

Una vez aplicado el formato de sistema de archivos, el último paso para agregar un nuevo sistema de archivos es adjuntar el sistema de archivos en la estructura de directorios. Cuando

el sistema de archivos se adjunta en una jerarquía de directorios, se puede acceder a las utilidades de espacio del usuario o escribirlas en el dispositivo.

Montaje manual de sistemas de archivos
Los administradores pueden usar el comando **`mount`** para adjuntar manualmente el dispositivo en una ubicación del directorio, o *punto de montaje,*al especificar el dispositivo y el punto de montaje así como cualquier opción que se pueda desear para personalizar el comportamiento del dispositivo.

```
[root@serverX ~]# mount /dev/vdb1 /mnt
```

El comando **`mount`** también se puede utilizar para ver los sistemas de archivos montados actualmente, los puntos de montaje y las opciones.

```
[root@serverX ~]# mount | grep vdb1
/dev/vdb1 on /mnt type xfs (rw,relatime,seclabel,attr2,inode64,noquota)
```

Montar manualmente un sistema de archivos es una manera excelente de verificar que un dispositivo formateado sea accesible o funcione de la manera deseada. No obstante, una vez que el sistema se reinicia, si bien aún existe y tiene datos intactos, no se montará en el árbol de directorios nuevamente. Si un administrador desea que el sistema de archivos se monte de forma persistente, es necesario agregar un listado para el sistema de archivos a **`/etc/fstab`**.

Montaje de forma persistente de sistemas de archivos
Al agregar un listado para un dispositivo en el archivo **`/etc/fstab`**, los administradores pueden configurar un dispositivo para montarlo en un punto de montaje en el arranque del sistema.

`/etc/fstab` es un archivo delimitado por espacios en blanco con seis campos por línea.

```
[root@serverX ~]# cat /etc/fstab
#
# /etc/fstab
# Created by anaconda on Thu Mar 20 14:52:46 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=7a20315d-ed8b-4e75-a5b6-24ff9e1f9838  /  xfs  defaults  1 1
```

El primer campo especifica el dispositivo que se usará. En el ejemplo anterior, el **`UUID`** se usa para especificar el dispositivo. De forma alternativa, se podría usar el archivo del dispositivo, por ejemplo, **`/dev/vdb1`**. El **`UUID`** se almacena en el superbloque del sistema de archivos y se crea cuando se crea el sistema de archivos.

nota

Es preferible el uso de **UUID** porque los identificadores del dispositivo de bloques pueden cambiar en determinadas situaciones, como en el caso de que un proveedor de la nube cambie la capa de almacenamiento subyacente de una máquina virtual. El archivo del dispositivo de bloques puede cambiar, pero el **UUID** permanecerá intacto en el superbloque del dispositivo.

Se puede usar el comando **blkid** para escanear los dispositivos de bloques conectados a una máquina e informar los datos como el **UUID** asignado y el formato del sistema de archivos.

```
[root@serverX ~]# blkid /dev/vdb1
/dev/vdb1: UUID="226a7c4f-e309-4cb3-9e76-6ef972dd8600" TYPE="xfs"
```

El segundo campo es el punto de montaje donde el dispositivo debe adjuntarse en la jerarquía del directorio. El punto de montaje ya debe existir; si no, se puede crear con **mkdir**.

El tercer campo contiene el tipo de sistema de archivos que se ha aplicado al dispositivo de bloques.

El cuarto campo es la lista de opciones que debe aplicarse al dispositivo, cuando se lo monta, para personalizar el comportamiento. El campo es obligatorio, y hay un conjunto de opciones que se usan comúnmente denominadas **defaults** (valores predeterminados). Otras opciones están documentadas en la página del manual **mount**.

Los últimos dos campos son la marca dump y el orden fsck. La marca se usa con el comando **dump** para hacer una copia de seguridad del contenido del dispositivo. El campo de orden determina si el **fsck** debe ejecutarse en el momento del arranque, en el caso de que el sistema de archivos no se haya montado de forma ordenada. El valor del orden indica el orden en el que los sistemas de archivos deben ejecutar **fsck** en ellos si se requiere la revisión de múltiples sistemas.

```
UUID=226a7c4f-e309-4cb3-9e76-6ef972dd8600  /mnt  xfs  defaults  1 2
```

nota

Si hay una entrada incorrecta en **/etc/fstab**, es posible que la máquina no pueda volver a arrancarse. Para evitar esa situación, un administrador debe comprobar que la entrada sea válida al desmontar el sistema de archivos nuevo y usar **mount -a**, que lee **/etc/fstab**, para montar el sistema de archivos nuevamente en su lugar. Si el comando **mount -a** arroja un error, se debe corregir antes de volver a arrancar la máquina.

Referencias

Páginas del manual: **fdisk**(8), **gdisk**(8), **mkfs**(8), **mount**(8), **fstab**(5)

Práctica: Agregar particiones, sistemas de archivos y montajes persistentes

En este trabajo de laboratorio, creará una partición MBR en un disco recientemente asignado, formateará la partición con un sistema de archivos ext4 y configurará el sistema de archivos para un montaje persistente.

Recursos:	
Máquinas:	serverX

Resultados:
Sistema de archivos ext4 de 1 GiB en segundo disco montado de forma persistente en **`/archive`**.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en serverX.
- Cambie a **`raíz`** usando **`sudo -i`**.

Se le ha solicitado archivar datos en un nuevo directorio, **`/archive`**, en serverX. Se le ha asignado un segundo disco para este propósito. El directorio **`/archive`** requerirá 1 GiB de espacio. Para asegurarse de que el directorio **`/archive`** esté siempre disponible para usar, deberá configurar el sistema de archivos recientemente creado para montarlo de forma persistente en **`/archive`**, incluso luego de reiniciar el servidor.

Una vez que haya completado su trabajo, reinicie su máquina serverX y compruebe que el sistema de archivos creado recientemente se monte de forma persistente en **`/archive`** luego del reinicio.

1. Cree una partición MBR de 1 GiB en **`/dev/vdb`** de tipo **Linux**.

   1.1. Use **`fdisk`** para modificar el segundo disco.

   ```
   [root@serverX ~]# fdisk /dev/vdb
   ```

   1.2. Muestre la tabla de particiones originales, y luego agregue una nueva partición que tenga un tamaño de 1 GiB.

   ```
   Command (m for help): p

   Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
   Units = sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disk label type: dos
   Disk identifier: 0xfd41a9d3

   Device Boot    Start      End   Blocks  Id  System

   Command (m for help): n
   ```

```
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): Enter
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519): +1G
Partition 1 of type Linux and of size 1 GiB is set
```

1.3. Guarde los cambios de la tabla de particiones.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

1.4. Si **fdisk** emite una advertencia, ejecute el comando **partprobe** para hacer que el kernel tenga conocimiento del cambio realizado en la tabla de particiones. Esto no será necesario si el dispositivo del disco se encuentra actualmente en desuso.

```
[root@serverX ~]# partprobe
```

2. Formatee la partición recientemente creada con el sistema de archivos ext4.

```
[root@serverX ~]# mkfs -t ext4 /dev/vdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
65536 inodes, 262144 blocks
13107 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=268435456
8 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Configure el sistema de archivos recientemente creado para montarlo de forma persistente en **/archive**.

3.1. Cree el punto de montaje del directorio **/archive**.

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

3.2. Determine el UUID de la nueva partición en el segundo disco.

```
[root@serverX ~]# blkid /dev/vdb1
/dev/vdb1: UUID="5fcb234a-cf18-4d0d-96ab-66a4d1ad08f5" TYPE="ext4"
```

3.3. Agregue una entrada a **/etc/fstab**.

```
UUID=5fcb234a-cf18-4d0d-96ab-66a4d1ad08f5 /archive ext4 defaults 0 2
```

4. Pruebe montar el sistema de archivos recientemente creado.

4.1. Ejecute el comando **mount** para montar el sistema de archivos nuevo usando la nueva entrada agregada a **/etc/fstab**.

```
[root@serverX ~]# mount -a
```

4.2. Verifique que el sistema de archivos nuevo esté montado en **/archive**.

```
[root@serverX ~]# mount | grep -w /archive
/dev/vdb1 on /archive type ext4 (rw,relatime,seclabel,data=ordered)
```

5. Reinicie serverX. Luego de reiniciar el servidor, inicie sesión y verifique que **/dev/vdb1** se monte en **/archive**.

```
[student@serverX ~]$ mount | grep ^/
/dev/vda1 on / type xfs (rw,relatime,seclabel,attr2,inode64,noquota)
/dev/vdb1 on /archive type ext4 (rw,relatime,seclabel,data=ordered)
```

Administración de espacio swap (intercambio)

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Crear y formatear una partición para espacio swap (intercambio).
- Activar el espacio swap (intercambio).

Conceptos de espacio swap (intercambio)

Un *espacio swap (intercambio)* es un área del disco que se puede usar con el subsistema de administración de memoria del kernel Linux. Los espacios swap (intercambio) se utilizan para complementar la memoria RAM del sistema al contener páginas inactivas de memoria. La combinación de la memoria RAM del sistema con los espacios swap (intercambio) se denomina *memoria virtual*.

Cuando el uso de la memoria en un sistema supera un límite definido, el kernel hará un barrido de la memoria RAM en busca de páginas de memoria asignadas a los procesos, pero inactivas. El kernel escribe la página inactiva en el área swap (intercambio), y luego reasignará la página RAM que será usada por otro proceso. Si el programa requiere acceso a una página que ha sido escrita en el disco, el kernel localizará otra página de memoria inactiva, la escribirá en el disco y luego volverá a convocar la página necesaria desde el área swap (intercambio).

Dado que las áreas swap (intercambio) residen en el disco, el swap (intercambio) es increíblemente lento cuando se lo compara con la memoria RAM. Si bien se usa para aumentar la memoria RAM del sistema, el uso de espacios swap (intercambio) debe mantenerse al mínimo siempre que sea posible.

Crear un espacio swap (intercambio)

Para crear un espacio swap (intercambio), un administrador debe realizar tres acciones:

- Crear una partición.
- Establecer el tipo de partición como **`82 Linux Swap`**.
- Formatear una firma swap (intercambio) en el dispositivo.

Crear una partición

Use una herramienta, como **`fdisk`**, para crear una partición del tamaño deseado. En el siguiente ejemplo, se creará una partición de 256 MiB.

```
[root@serverX ~]# fdisk /dev/vdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0x34e4e6d7.
```

```
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): Enter
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519): +256M
Partition 1 of type Linux and of size 256 MiB is set

Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x34e4e6d7

   Device Boot      Start         End      Blocks   Id  System
/dev/vdb1            2048      526335      262144   83  Linux
```

Asignar el tipo de partición

Luego de haber creado la partición swap (intercambio), una práctica recomendada es cambiar el tipo de partición, o la id. del sistema a **`82 Linux Swap`**. Anteriormente, las herramientas observaban el tipo de partición para determinar si el dispositivo debía activarse; no obstante, eso ya no sucede. Si bien el tipo de partición ya no es usado por utilidades, tener el tipo establecido permite a los administradores determinar rápidamente el propósito de la partición. El siguiente ejemplo continua desde **`fdisk`**.

```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 82
Changed type of partition 'Linux' to 'Linux swap / Solaris'

Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x34e4e6d7

   Device Boot      Start         End      Blocks   Id  System
/dev/vdb1            2048      526335      262144   82  Linux swap / Solaris
```

Formatear el dispositivo

El comando **`mkswap`** aplica una *firma swap (intercambio)* al dispositivo. A diferencia de otras utilidades de formateo, **`mkswap`** escribe un único bloque de datos al inicio del dispositivo, dejando el resto del dispositivo sin formatear de modo que pueda utilizarse para almacenar páginas de memoria.

```
[root@serverX ~]# mkswap /dev/vdb1
Setting up swapspace version 1, size = 262140 KiB
no label, UUID=fbd7fa60-b781-44a8-961b-37ac3ef572bf
```

Activar un espacio swap (intercambio)

Un administrador puede usar el comando **swapon** para activar un espacio swap (intercambio) formateado. **swapon** se puede invocar en el dispositivo, o **swapon -a** activará todos los espacios swap (intercambio) que figuran en el archivo **/etc/fstab**.

```
[root@serverX ~]# free
             total       used       free     shared    buffers     cached
Mem:       1885252     791812    1093440      17092        688     292024
-/+ buffers/cache:     499100    1386152
Swap:            0          0          0
[root@serverX ~]# swapon /dev/vdb1
[root@serverX ~]# free
             total       used       free     shared    buffers     cached
Mem:       1885252     792116    1093136      17092        692     292096
-/+ buffers/cache:     499328    1385924
Swap:       262140          0     262140
```

Activar de forma persistente un espacio swap (intercambio)

Es probable que se requiera un espacio swap (intercambio) para activar automáticamente cada vez que arranque la máquina. Para que la máquina active el espacio swap (intercambio) en cada arranque, se debe configurar en el archivo **/etc/fstab**.

En caso de ser necesario, un administrador puede desactivar un espacio swap (intercambio) usando el comando **swapoff**. Un **swapoff** solo proporcionará resultados satisfactorios si cualquier dato swapped (intercambiado) se puede escribir en otros espacios swap (intercambio) activos o nuevamente en la memoria. Si no se pueden escribir datos en otros lugares, el **swapoff** fallará, con un error, y el espacio swap (intercambio) permanecerá activo.

A continuación, se muestra una línea de ejemplo en **/etc/fstab** donde se agrega un espacio swap (intercambio) creado anteriormente.

```
UUID=fbd7fa60-b781-44a8-961b-37ac3ef572bf  swap  swap  defaults  0 0
```

El ejemplo anterior usa el **UUID** como el primer campo. El **UUID** está almacenado en la firma swap (intercambio) almacenada en el dispositivo, y era parte del resultado de **mkswap**. Si el resultado de **mkswap** se ha perdido, se puede usar el comando **blkid** para escanear el sistema e informar sobre todos los dispositivos de bloques conectados. Si el administrador no desea usar el **UUID**, el nombre del dispositivo sin formato también se puede usar en el primer campo.

El segundo campo se reserva típicamente para el **punto de montaje**. Sin embargo, para dispositivos swap (intercambio), que no son accesibles a través de la estructura del directorio, este campo es el valor del marcador de posición **swap**.

El tercer campo es el tipo de sistema de archivos. El tipo de sistemas de archivos para un espacio swap (intercambio) es **swap**.

El cuarto campo es para opciones. En el ejemplo, se utiliza la opción **defaults** (valores predeterminados). **defaults** (valores predeterminados) incluye la opción de montaje **auto**, que es lo que hace que el espacio swap (intercambio) se active automáticamente en el arranque.

Los dos campos finales son la marca dump y el orden fsck. Los espacios swap (intercambio) no requieren copias de seguridad ni revisión del sistema de archivos.

nota

De forma predeterminada, los espacios swap (intercambio) se usan en serie, lo que significa que se usará el primer espacio swap (intercambio) activado hasta que esté lleno, luego el kernel empezará a usar el segundo espacio swap (intercambio). Las prioridades de los espacios swap (intercambio) se muestran con **`swapon -s`**, y se pueden establecer con la opción de montaje **`pri=`**. Si los espacios swap (intercambio) tienen la misma prioridad, el kernel los escribirá en turnos rotativos en lugar de escribir en un único espacio swap (intercambio) hasta que complete su capacidad.

Referencias

Páginas del manual: **`mkswap`**(8), **`swapon`**(8), **`swapoff`**(8), **`mount`**(8), **`fdisk`**(8)

Práctica: Agregar y habilitar espacio swap (intercambio)

En este trabajo de laboratorio, creará una partición swap (intercambio) y la habilitará para su uso.

Recursos:	
Máquinas:	serverX

Resultados:
Su host serverX tendrá 500 MiB de espacio swap (intercambio) ejecutándose en su segundo disco.

Andes de comenzar
- Inicie sesión en serverX.
- Cambie a **raíz** usando **sudo -i**.

No se creó ninguna partición de intercambio durante la instalación de serverX. Durante el uso pico, el servidor se ha ejecutado fuera de la memoria física. Ha solicitado memoria RAM adicional y está esperando ansiosamente su llegada. Mientras tanto, decide aliviar el problema al habilitar espacio swap (intercambio) en el segundo disco. Para asegurarse de que el espacio swap (intercambio) agregado recientemente esté siempre disponible para su uso, también necesitará configurarlo para que esté habilitado en el arranque.

Una vez que haya completado su trabajo, vuelva a arrancar su máquina serverX y verifique que el espacio swap (intercambio) esté disponible luego del reinicio.

1. Cree una partición de 500 MiB en **/dev/vdb** de tipo **Linux swap** (intercambio de Linux).

   1.1. Use **fdisk** para modificar el segundo disco.

```
[root@serverX ~]# fdisk /dev/vdb
```

   1.2. Imprima la tabla de particiones originales, y luego cree una nueva partición que tenga un tamaño de 500 GiB.

```
Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xfd41a9d3

   Device Boot      Start         End      Blocks   Id  System
/dev/vdb1            2048     2099199     1048576   83  Linux

Command (m for help): n
Partition type:
   p   primary (1 primary, 0 extended, 3 free)
```

```
   e   extended
Select (default p): p
Partition number (2-4, default 2): 2
First sector (2099200-20971519, default 2099200): Enter
Using default value 2099200
Last sector, +sectors or +size{K,M,G} (2099200-20971519, default
 20971519): +500M
Partition 2 of type Linux and of size 500 MiB is set

Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xfd41a9d3

   Device Boot      Start         End      Blocks   Id  System
/dev/vdb1            2048     2099199     1048576   83  Linux
/dev/vdb2         2099200     3123199      512000   83  Linux
```

1.3. Establezca la partición creada recientemente al tipo **Linux swap** (intercambio de Linux).

```
Command (m for help): t
Partition number (1,2, default 2): 2
Hex code (type L to list all codes): L

...
 1 FAT12  27 Hidden NTFS Win  82 Linux swap / So c1  DRDOS/sec (FAT-
...
Hex code (type L to list all codes): 82
Changed type of partition 'Linux' to 'Linux swap / Solaris'

Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xfd41a9d3

Device Boot    Start      End   Blocks  Id  System
/dev/vdb1       2048  2099199  1048576  83  Linux
/dev/vdb2    2099200  3123199   512000  82  Linux swap / Solaris
```

1.4. Guarde los cambios de la tabla de particiones.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource
 busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

1.5. Ejecute **partprobe** para hacer que el kernel tenga conocimiento del cambio en la tabla de particiones.

```
[root@serverX ~]# partprobe
```

2. Inicialice la partición creada recientemente como espacio swap (intercambio).

```
[root@serverX ~]# mkswap /dev/vdb2
Setting up swapspace version 1, size = 511996 KiB
no label, UUID=74f8f3e1-6af3-4e51-9ab5-c48e52bf4a7b
```

3. Habilite el espacio swap (intercambio) creado recientemente.

3.1. La creación y la inicialización del espacio swap (intercambio) no lo habilita aún para su uso como se muestra mediante los comandos **free** y **swapon -s**.

```
[root@serverX ~]# free
             total       used       free     shared    buffers     cached
Mem:       1885252     557852    1327400      17096       1080     246040
-/+ buffers/cache:     310732    1574520
Swap:            0          0          0
```

```
[root@serverX ~]# swapon -s
[root@serverX ~]#
```

3.2. Habilite el espacio swap (intercambio) creado recientemente.

```
[root@serverX ~]# swapon /dev/vdb2
```

3.3. Verifique que el espacio swap (intercambio) creado recientemente ahora esté disponible.

```
[root@serverX ~]# swapon -s
Filename    Type  Size Used Priority
/dev/vdb2                               partition 511996 0 -1
```

3.4. Deshabilite el espacio swap (intercambio).

```
[root@serverX ~]# swapoff /dev/vdb2
```

3.5. Verifique que el espacio swap (intercambio) esté deshabilitado.

```
[root@serverX ~]# swapon -s
[root@serverX ~]#
```

4. Configure el nuevo espacio swap (intercambio) de modo que esté habilitado en el arranque.

4.1. Determine el UUID de la nueva partición de intercambio en el segundo disco.

```
[root@serverX ~]# blkid /dev/vdb2
/dev/vdb2: UUID="74f8f3e1-6af3-4e51-9ab5-c48e52bf4a7b" TYPE="swap"
```

4.2. Agregue una entrada a **/etc/fstab**.

```
UUID=74f8f3e1-6af3-4e51-9ab5-c48e52bf4a7b swap swap defaults 0 0
```

4.3. Evalúe la habilitación del espacio swap (intercambio) usando la nueva entrada recién agregada a **/etc/fstab**.

```
[root@serverX ~]# swapon -a
```

4.4. Verifique que el nuevo espacio swap (intercambio) fue habilitado.

```
[root@serverX ~]# swapon -s
Filename                        Type            Size    Used    Priority
/dev/vdb2                       partition       511996  0       -1
```

5. Reinicie serverX. Luego de reiniciar el servidor, inicie sesión y verifique que el espacio swap (intercambio) esté habilitado.

```
[student@serverX ~]# swapon -s
Filename                        Type            Size    Used    Priority
/dev/vdb2                       partition       511996  0       -1
```

Trabajo de laboratorio: Adición de discos, particiones y sistemas de archivos a un sistema Linux

En este trabajo de laboratorio, creará una partición GPT en un disco recientemente asignado, formateará la partición con un sistema de archivos XFS y configurará el sistema de archivos para un montaje persistente. También creará dos particiones swap (intercambio) de 512 MiB. Configurará una de las particiones swap (intercambio) para que tenga una prioridad 1.

Recursos:	
Máquinas:	serverX

Resultados:

- Sistema de archivos XFS de 2 GiB en una partición GPT, en el segundo disco. El sistema de archivos se monta persistentemente en **`/backup`**.
- Una partición swap (intercambio) de 512 MiB habilitada en el segundo disco con prioridad predeterminada.
- Otra partición swap (intercambio) de 512 MiB habilitada en el segundo disco con una prioridad 1.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en serverX.
- Cambie a **`raíz`** usando **`sudo -i`**.

Se le ha solicitado que copie datos importantes del disco principal en serverX a un disco separado para mantener la seguridad. Se le ha asignado un segundo disco en serverX para este propósito. Ha decidido crear una partición de GPT de 2 GiB en el segundo disco y formatearlo con el sistema de archivos XFS. Para asegurarse de que este nuevo sistema de archivos esté siempre disponible, lo configurará para montarlo de forma persistente.

Para compensar la escasez de memoria física en serverX, se recomienda crear y habilitar algo de espacio swap (intercambio) para usar. Creará dos particiones swap (intercambio) de 512 MiB en el segundo disco y establecerá la prioridad de una de las particiones en 1, de modo que sea la preferida con respecto a la otra partición swap (intercambio).

Reinicie su máquina serverX. Verifique que el sistema de archivos XFS recientemente creado se monte de forma persistente en **`/backup`**. Asimismo, confirme que se activen dos espacios swap (intercambio) en el arranque y uno de los espacios swap (intercambio) tenga la prioridad -1 predeterminada y la otra tenga la prioridad 1.

Cuando haya finalizado su trabajo, ejecute **`lab disk grade`** en su máquina serverX para verificar su trabajo.

1. Cree una partición GPT de 2 GiB en **`/dev/vdb`** de tipo **Linux**.

2. Cree dos particiones de 512 MiB en **/dev/vdb** del tipo **Linux swap** (intercambio de Linux).

3. Formatee las particiones creadas recientemente. Formatee la partición de 2 GiB con un sistema de archivos XFS. Inicialice las dos particiones de 512 MiB como espacio swap (intercambio).

4. Configure el sistema de archivos recientemente creado para montarlo de forma persistente en **/backup**.

5. Configure los espacios swap (intercambio) recientemente creados para que estén habilitados en el arranque. Establezca uno de los espacios swap (intercambio) para que se prefiera sobre el otro.

6. Reinicie serverX. Luego de reiniciar el servidor, inicie sesión y verifique que **/dev/vdb1** se monte en **/backup**. También verifique que dos particiones swap (intercambio) de 512 MiB estén habilitadas y que una tenga la prioridad predeterminada y la otra tenga una prioridad 1.

7. Cuando haya completado su trabajo, ejecute **lab disk grade** en su máquina serverX para verificar su trabajo.

Solución

En este trabajo de laboratorio, creará una partición GPT en un disco recientemente asignado, formateará la partición con un sistema de archivos XFS y configurará el sistema de archivos para un montaje persistente. También creará dos particiones swap (intercambio) de 512 MiB. Configurará una de las particiones swap (intercambio) para que tenga una prioridad 1.

Recursos:	
Máquinas:	serverX

Resultados:

- Sistema de archivos XFS de 2 GiB en una partición GPT, en el segundo disco. El sistema de archivos se monta persistentemente en **`/backup`**.
- Una partición swap (intercambio) de 512 MiB habilitada en el segundo disco con prioridad predeterminada.
- Otra partición swap (intercambio) de 512 MiB habilitada en el segundo disco con una prioridad 1.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en serverX.
- Cambie a **`raíz`** usando **`sudo -i`**.

Se le ha solicitado que copie datos importantes del disco principal en serverX a un disco separado para mantener la seguridad. Se le ha asignado un segundo disco en serverX para este propósito. Ha decidido crear una partición de GPT de 2 GiB en el segundo disco y formatearlo con el sistema de archivos XFS. Para asegurarse de que este nuevo sistema de archivos esté siempre disponible, lo configurará para montarlo de forma persistente.

Para compensar la escasez de memoria física en serverX, se recomienda crear y habilitar algo de espacio swap (intercambio) para usar. Creará dos particiones swap (intercambio) de 512 MiB en el segundo disco y establecerá la prioridad de una de las particiones en 1, de modo que sea la preferida con respecto a la otra partición swap (intercambio).

Reinicie su máquina serverX. Verifique que el sistema de archivos XFS recientemente creado se monte de forma persistente en **`/backup`**. Asimismo, confirme que se activen dos espacios swap (intercambio) en el arranque y uno de los espacios swap (intercambio) tenga la prioridad -1 predeterminada y la otra tenga la prioridad 1.

Cuando haya finalizado su trabajo, ejecute **`lab disk grade`** en su máquina serverX para verificar su trabajo.

1. Cree una partición GPT de 2 GiB en **`/dev/vdb`** de tipo **Linux**.

   1.1. Use **`gdisk`** para modificar el segundo disco.

   ```
   [root@serverX ~]# gdisk /dev/vdb
   ```

   1.2. Agregue una partición swap (intercambio) que tenga un tamaño de 2 GiB.

```
Command (? for help): n
Partition number (1-128, default 1): 1
First sector (34-20971486, default = 2048) or {+-}size{KMGTP}: Enter
Last sector (2048-20971486, default = 20971486) or {+-}size{KMGTP}: +2G
Current type is 'Linux filesystem'
```

1.3. Establezca la nueva partición al tipo **Linux**.

```
Hex code or GUID (L to show codes, Enter = 8300): Enter
Changed type of partition to 'Linux filesystem'
```

2. Cree dos particiones de 512 MiB en **/dev/vdb** del tipo **Linux swap** (intercambio de Linux).

2.1. Agregue una partición que sea de 512 MiB.

```
Command (? for help): n
Partition number (2-128, default 2): 2
First sector (34-20971486, default = 4196352) or {+-}size{KMGTP}: Enter
Last sector (4196352-20971486, default = 20971486) or {+-}size{KMGTP}: +512M
Current type is 'Linux filesystem'
```

2.2. Establezca la partición al tipo **Linux swap** (intercambio de Linux).

```
Hex code or GUID (L to show codes, Enter = 8300): L
...
8200 Linux swap            8300 Linux filesystem      8301 Linux reserved
...
Hex code or GUID (L to show codes, Enter = 8300): 8200
Changed type of partition to 'Linux swap'
```

2.3. Agregue otra partición que sea de 512 MiB, y configúrela con el tipo **Linux swap** (intercambio de Linux).

```
Command (? for help): n
Partition number (3-128, default 3): 3
First sector (34-20971486, default = 5244928) or {+-}size{KMGTP}: Enter
Last sector (5244928-20971486, default = 20971486) or {+-}size{KMGTP}: +512M
Current type is 'Linux filesystem'
Hex code or GUID (L to show codes, Enter = 8300): 8200
Changed type of partition to 'Linux swap'
```

2.4. Verifique las particiones.

```
Command (? for help): p
Disk /dev/vdb: 20971520 sectors, 10.0 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): 9918D507-7344-406A-9902-D2503FA028EF
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 20971486
Partitions will be aligned on 2048-sector boundaries
Total free space is 14679997 sectors (7.0 GiB)
```

```
Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048         4196351   2.0 GiB     8300  Linux filesystem
   2         4196352         5244927   512.0 MiB   8200  Linux swap
   3         5244928         6293503   512.0 MiB   8200  Linux swap
```

2.5. Guarde los cambios en la tabla de particiones.

```
Command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!

Do you want to proceed? (Y/N): y
OK; writing new GUID partition table (GPT) to /dev/vdb.
The operation has completed successfully.
```

2.6. Ejecute **partprobe** para hacer que el kernel tenga conocimiento del cambio en la tabla de particiones.

```
[root@serverX ~]# partprobe
```

3. Formatee las particiones creadas recientemente. Formatee la partición de 2 GiB con un sistema de archivos XFS. Inicialice las dos particiones de 512 MiB como espacio swap (intercambio).

3.1. Formatee la partición recientemente creada con el sistema de archivos XFS.

```
[root@serverX ~]# mkfs -t xfs /dev/vdb1
    meta-data=/dev/vdb1              isize=256    agcount=4, agsize=131072 blks
             =                       sectsz=512   attr=2, projid32bit=1
             =                       crc=0
    data     =                       bsize=4096   blocks=524288, imaxpct=25
             =                       sunit=0      swidth=0 blks
    naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
    log      =internal log           bsize=4096   blocks=2560, version=2
             =                       sectsz=512   sunit=0 blks, lazy-count=1
    realtime =none                   extsz=4096   blocks=0, rtextents=0
```

3.2. Inicialice las dos particiones como espacio swap (intercambio).

```
[root@serverX ~]# mkswap /dev/vdb2
    Setting up swapspace version 1, size = 524284 KiB
    no label, UUID=d00554b7-dfac-4034-bdd1-37b896023f2c
```

```
[root@serverX ~]# mkswap /dev/vdb3
    Setting up swapspace version 1, size = 524284 KiB
    no label, UUID=af30cbb0-3866-466a-825a-58889a49ef33
```

4. Configure el sistema de archivos recientemente creado para montarlo de forma persistente en **/backup**.

4.1. Cree el punto de montaje del directorio **/backup**.

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

4.2. Determine el UUID de la primera partición en el segundo disco.

```
[root@serverX ~]# blkid /dev/vdb1
/dev/vdb1: UUID="748ca35a-1668-4a2f-bfba-51ebe550f6f0" TYPE="xfs"
 PARTLABEL="Linux filesystem" PARTUUID="83b18afb-9c12-48bf-a620-7f8a612df5a8"
```

4.3. Agregue una entrada a **/etc/fstab**.

```
UUID=748ca35a-1668-4a2f-bfba-51ebe550f6f0 /backup xfs defaults 0 2
```

5. Configure los espacios swap (intercambio) recientemente creados para que estén habilitados en el arranque. Establezca uno de los espacios swap (intercambio) para que se prefiera sobre el otro.

5.1. Agregue entradas a **/etc/fstab** usando los UUID generados en los pasos de **mkswap** anteriores. Establezca la prioridad en uno de los espacios swap (intercambio) en 1.

```
UUID=d00554b7-dfac-4034-bdd1-37b896023f2c swap swap defaults 0 0
UUID=af30cbb0-3866-466a-825a-58889a49ef33 swap swap pri=1 0 0
```

6. Reinicie serverX. Luego de reiniciar el servidor, inicie sesión y verifique que **/dev/vdb1** se monte en **/backup**. También verifique que dos particiones swap (intercambio) de 512 MiB estén habilitadas y que una tenga la prioridad predeterminada y la otra tenga una prioridad 1.

```
[student@serverX ~]$ mount | grep ^/
/dev/vda1 on / type xfs (rw,relatime,seclabel,attr2,inode64,noquota)
/dev/vdb1 on /backup type xfs (rw,relatime,seclabel,attr2,inode64,noquota)
```

```
[student@serverX ~]$ free
             total       used       free     shared    buffers     cached
Mem:       1885252     563528    1321724      17096        696     245224
-/+ buffers/cache:     317608    1567644
Swap:      1048568          0    1048568
```

```
[student@serverX ~]$ swapon -s
Filename                        Type       Size    Used  Priority
/dev/vdb2                       partition  524284  0     -1
/dev/vdb3                       partition  524284  0     1
```

7. Cuando haya completado su trabajo, ejecute **lab disk grade** en su máquina serverX para verificar su trabajo.

```
[student@serverX ~]$ lab disk grade
```

Resumen

Adición de particiones, sistemas de archivos y montajes persistentes

- **`fdisk`** se puede usar para agregar, modificar y eliminar particiones en discos con esquemas de partición MBR.
- **`gdisk`** se puede usar para agregar, modificar y eliminar particiones en discos con esquemas de partición GPT.
- Los sistemas de archivos se crean en particiones de discos usando **`mkfs`**.
- Para que los montajes de sistemas de archivos sean persistentes, se deben agregar a **`/etc/fstab`**.

Administración de espacio swap (intercambio)

- Cree y active un espacio swap (intercambio).

redhat. TRAINING

CAPÍTULO 10

ADMINISTRACIÓN DEL ALMACENAMIENTO DE GESTIÓN DE VOLÚMENES LÓGICOS (LVM)

Descripción general	
Meta	Gestionar volúmenes lógicos desde la línea de comandos.
Objetivos	• Describir los componentes y conceptos de la gestión de volúmenes lógicos. • Gestionar volúmenes lógicos. • Extender volúmenes lógicos.
Secciones	• Conceptos de gestión de volúmenes lógicos (y práctica) • Gestión de volúmenes lógicos (y práctica) • Extensión de volúmenes lógicos (y práctica)
Trabajo de laboratorio	• Administración del almacenamiento de gestión de volúmenes lógicos (LVM)

Conceptos de la gestión de volúmenes lógicos

Objetivos

Luego de completar esta sección, los estudiantes deberían poder describir componentes de la gestión de volúmenes lógicos (logical volumen management, LVM).

Conceptos de la gestión de volúmenes lógicos (LVM)

Los volúmenes lógicos y la gestión de volúmenes lógicos facilitan la administración del espacio del disco. Si un sistema de archivos alojado en LVM necesita más espacio, se puede asignar a su volumen lógico del espacio libre en su grupo de volúmenes y se puede cambiar el tamaño del sistema de archivos. Si un disco comienza a fallar, se puede registrar un disco de reemplazo como volumen físico con el grupo de volúmenes y las extensiones del volumen lógico se pueden migrar al disco nuevo.

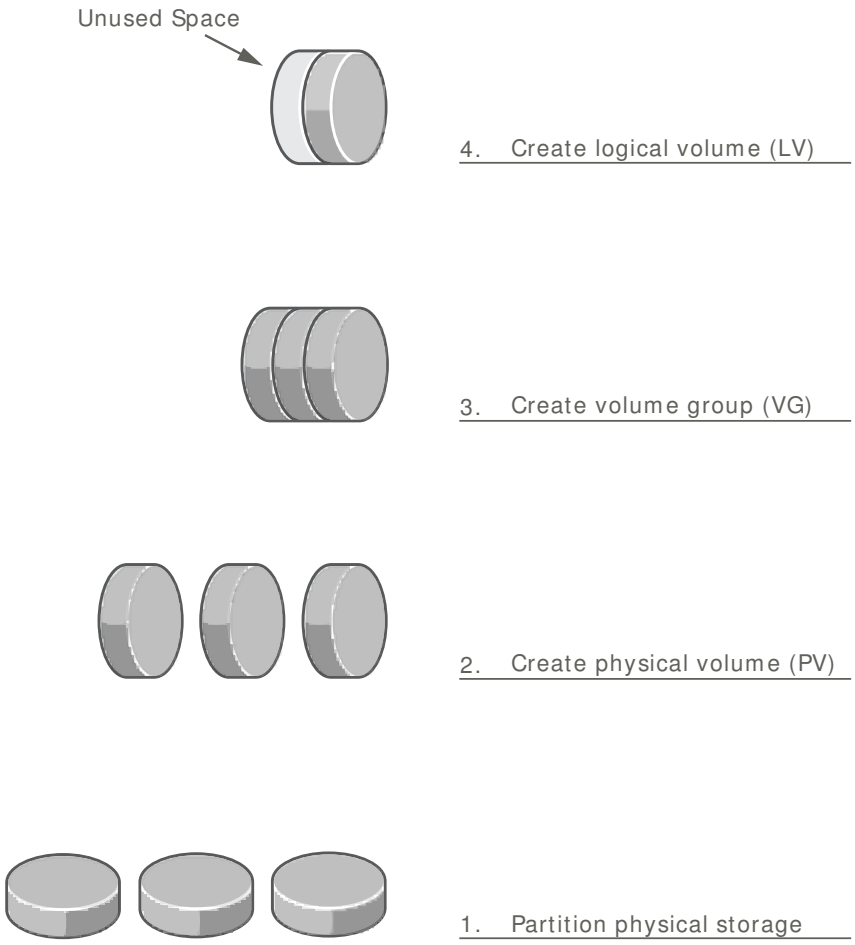

Figura 10.1: Componentes de la gestión de volúmenes lógicos

Definiciones de LVM

- Los *dispositivos físicos* son los dispositivos de almacenamiento usados para que los datos almacenados persistan en un volumen lógico. Estos son dispositivos en bloques y podrían ser particiones de discos, discos enteros, arreglos RAID o discos SAN. Un dispositivo debe inicializarse como un volumen físico de LVM para poder ser usado con LVM. Todo el "dispositivo" se usará como un volumen físico.

- Los *volúmenes físicos* (phisical volumes, PV) se utilizan para registrar dispositivos físicos subyacentes para ser usados en grupos de volúmenes. LVM segmenta automáticamente PV en *extensiones físicas* (physical extents, PE); estas son pequeños conjuntos de datos que actúan como el bloque de almacenamiento más pequeño en un PV.

- Los *grupos de volúmenes* (volume groups, VG) son grupos de almacenamiento conformados por uno o más volúmenes físicos. Un PV solo puede ser asignado a un único VG. Un VG puede constar de espacio sin usar y de cualquier cantidad de volúmenes lógicos.
- Los *volúmenes lógicos* (logical volumes, LV) se crean desde extensiones físicas libres en un grupo de volúmenes y proporcionan el dispositivo de "almacenamiento" usado por aplicaciones, usuarios y el sistema operativo. Los LV son una colección de *extensiones lógicas* (LE), que se asignan a extensiones físicas, la porción de almacenamiento más pequeña de un PV. De forma predeterminada, cada LE se asignará a una PE. La configuración de opciones de LV específicas cambiará esta asignación; por ejemplo, la *creación de reflejo* hace que cada LE se asigne a dos PE.

Práctica: Conceptos de la gestión de volúmenes lógicos

Establezca una coincidencia entre los siguientes elementos y sus equivalentes de la tabla.

Disco, partición, arreglo RAID	Extensión física
Extensión lógica	Grupo de volúmenes (VG)
Volumen físico (PV)	Volumen lógico (LV)

Descripción del componente	Componente
Formateado con un sistema de archivos y montado para usar en el tiempo de ejecución	
Se asigna a un dispositivo de almacenamiento físico, como un disco o partición	
Porción de almacenamiento de un LV, generalmente se asigna a una PE	
Se usa para identificar un bloque de PV para usar en la creación de uno o más LV	
Nombre usado para la porción de almacenamiento de un PV; también la porción de almacenamiento más pequeña de un LV	
Candidatos potenciales para usar como un único PV	

Solución

Establezca una coincidencia entre los siguientes elementos y sus equivalentes de la tabla.

Descripción del componente	Componente
Formateado con un sistema de archivos y montado para usar en el tiempo de ejecución	Volumen lógico (LV)
Se asigna a un dispositivo de almacenamiento físico, como un disco o partición	Volumen físico (PV)
Porción de almacenamiento de un LV, generalmente se asigna a una PE	Extensión lógica
Se usa para identificar un bloque de PV para usar en la creación de uno o más LV	Grupo de volúmenes (VG)
Nombre usado para la porción de almacenamiento de un PV; también la porción de almacenamiento más pequeña de un LV	Extensión física
Candidatos potenciales para usar como un único PV	Disco, partición, arreglo RAID

Gestión de volúmenes lógicos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Implementar almacenamiento del LVM.
- Visualizar información de componentes del LVM.

Implementación de almacenamiento del LVM

LVM viene con un conjunto integral de herramientas de línea de comandos para implementar y administrar almacenamiento del LVM. Estas herramientas de línea de comandos se pueden usar en scripts, lo que las hace más adecuadas para la automatización.

Importante

Los siguientes ejemplos usan el dispositivo **vda** y sus particiones para ilustrar comandos de LVM. En la práctica, estos ejemplos deberían usar los dispositivos correctos para el disco y las particiones del disco utilizados por el sistema.

Creación de un volumen lógico

Son cinco los pasos necesarios para crear un volumen lógico utilizable:

1. **Prepare el dispositivo físico**.

   Use **`fdisk`**, **`gdisk`** o **`parted`** para crear una nueva partición para usar con LVM. Siempre configure el tipo de partición en **`Linux LVM`** (LVM Linux) en las particiones de LVM; use **`0x8e`** para particiones estilo MBR. Si es necesario, use **`partprobe`** para registrar la nueva partición con el kernel.

   De forma alternativa, use un disco entero, un arreglo RAID o un disco SAN.

   Solo se necesita preparar un dispositivo físico si no hay ninguno ya preparado, y se requiere un volumen físico nuevo para crear o ampliar un grupo de volúmenes.

   ```
   [root@serverX ~]# fdisk /dev/vda
   ```

   Use **`m`** para obtener ayuda, **`p`** para imprimir la tabla de particiones existentes, **`n`** para crear una partición nueva, **`t`** para cambiar el tipo de partición, **`w`** para escribir los cambios y **`q`** para salir.

2. **Cree un volumen físico**.

   `pvcreate` se usa para etiquetar la partición (u otro dispositivo físico) para su uso con el LVM como volumen físico. Se escribe un encabezado para almacenar los datos de configuración del LVM directamente en el PV. Un PV se divide en extensiones físicas (PE) de un tamaño fijo; por ejemplo, bloques de 4 MiB. Etiquete varios dispositivos al mismo tiempo con nombres de dispositivos delimitados por espacios como argumentos para **`pvcreate`**.

```
[root@serverX ~]# pvcreate /dev/vda2 /dev/vdb1
```

Esto etiquetará dispositivos **/dev/vda2** y **/dev/vdb1** como PV, listos para la asignación en un grupo de volúmenes.

Un PV solo debe crearse si no hay PV libres para crear o ampliar un VG.

3. **Cree un un grupo de volúmenes**.

vgcreate se usa para crear un bloque de uno o más volúmenes físicos, a los que se denomina grupo de volúmenes. El tamaño del VG se determina mediante la cantidad total de extensiones físicas en el bloque. Un VG es responsable de alojar uno o más volúmenes lógicos al asignar PE libres a un LV; por lo tanto, debe tener suficientes PE libres disponibles en el momento en que se crea el LV.

Como argumentos para **vgcreate**, defina un nombre de VG y detalle uno o más PV para asignar al VG.

```
[root@serverX ~]# vgcreate vg-alpha /dev/vda2 /dev/vdb1
```

Esto creará un VG denominado **vg-alpha** que tiene el tamaño combinado, en unidades de PE, de los dos PV: **/dev/vda2** y **/dev/vdb1**.

Un VG solo debe crearse cuando no haya ninguno en existencia. Se pueden crear más VG por motivos administrativos para administrar el uso de PV y LV. O bien, los VG existentes se pueden ampliar para alojar nuevos LV cuando sea necesario.

4. **Cree un volumen lógico**.

lvcreate crea un nuevo volumen lógico desde las extensiones físicas disponibles en un grupo de volúmenes. Use estos argumentos para **lvcreate** como mínimo: use la opción **-n** para configurar el nombre del LV, la opción **-L** para configurar el tamaño del LV en bytes, e identifique el nombre del VG donde se creará el LV.

```
[root@serverX ~]# lvcreate -n hercules -L 2G vg-alpha
```

Esto creará un LV denominado **hercules**, con un tamaño de **2 GiB**, en el VG **vg-alpha**. Debe haber suficientes extensiones físicas libres para distribuir 2 GiB, y si es necesario, se redondeará a un factor del tamaño de unidades de PE.

Hay varias maneras de especificar el tamaño: **-L** anticipa el tamaño en bytes, o valores nombrados más grandes, como mebibytes (megabytes binarios, 1048576 bytes) y gibibytes (gigabytes binarios). La opción **-l** anticipa tamaños medidos como una cantidad de extensiones físicas.

Algunos ejemplos:

- **lvcreate -L 128M**: Cambia el tamaño del volumen lógico a exactamente 128 MiB.
- **lvcreate -l 128** : Cambia el tamaño del volumen lógico a exactamente 128 extensiones. El número total de bytes depende del tamaño del bloque de extensiones físicas en el volumen físico subyacente.

Importante

Diferentes herramientas mostrarán el nombre del volumen lógico, ya sea usando el nombre tradicional **/dev/*vgname/lvname*** o el nombre del asignador de dispositivos del kernel **/dev/mapper/*vgname-lvname***.

5. **Agregue el sistema de archivos**.

   Use **mkfs** para crear un sistema de archivos **xfs** en el nuevo volumen lógico. De forma alternativa, cree un sistema de archivos basado en su sistema de archivos preferido; por ejemplo, **ext4**.

```
[root@serverX ~]# mkfs -t xfs /dev/vg-alpha/hercules
```

   Para hacer que el sistema de archivos esté disponible luego de los reinicios:

   - Use **mkdir** para crear un directorio de punto de montaje.

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

   - Agregue una entrada al archivo **/etc/fstab**:

```
/dev/vg-alpha/hercules  /mnt/hercules  xfs  defaults 1 2
```

   - Ejecute **mount -a** para montar todos los sistemas de archivos en **/etc/fstab**, incluida la entrada que agregó recientemente.

```
[root@serverX ~]# mount -a
```

Eliminación de un volumen lógico

Son cuatro los pasos necesarios para eliminar *todos* los componentes de un volumen lógico:

1. **Prepare el sistema de archivos**.

   Traslade todos los datos que se deben conservar a otro sistema de archivos, y luego use **umount** para desmontar el sistema de archivos. No olvide eliminar todas las entradas **/etc/fstab** asociadas con este sistema de archivos.

```
[root@serverX ~]# umount /mnt/hercules
```

Advertencia

Al eliminar un volumen lógico se destruirán todos los datos almacenados en este. Realice una copia de seguridad de los datos o trasládelos *ANTES* de eliminar el volumen lógico.

2. **Elimine el volumen lógico**.

   lvremove se usa para eliminar un volumen lógico que ya no es necesario. Use el nombre del dispositivo como el argumento.

```
[root@serverX ~]# lvremove /dev/vg-alpha/hercules
```

   Antes de ejecutar este comando, se debe desmontar el sistema de archivos del LV. Se le solicitará una confirmación antes de eliminar el LV.

   Las extensiones físicas del LV se liberarán y estarán disponibles para ser asignadas a LV existentes o nuevos en el grupo de volúmenes.

3. **Elimine el grupo de volúmenes**.

   vgremove se usa para eliminar un grupo de volúmenes que ya no es necesario. Use el nombre del VG como el argumento.

```
[root@serverX ~]# vgremove vg-alpha
```

   Los volúmenes físicos del VG se liberarán y estarán disponibles para ser asignados a VG existentes o nuevos en el sistema.

4. **Elimine los volúmenes físicos**.

   pvremove se usa para eliminar volúmenes físicos que ya no son necesarios. Use una lista delimitada por espacios de dispositivos del PV para eliminar más de uno a la vez. Los metadatos del PV se borran de la partición (o disco). Ahora, la partición está libre para una nueva asignación o para ser formateada.

```
[root@serverX ~]# pvremove /dev/vda2 /dev/vdb1
```

Revisión de la información de estado de LVM

Volúmenes físicos

Use **pvdisplay** para visualizar información sobre volúmenes físicos (VP). Si no se especifica ningún argumento con el comando, este detallará información sobre todos los PV del sistema. Si el argumento es el nombre de un dispositivo específico, la información que se mostrará se limitará a este PV específico.

```
[root@serverX ~]# pvdisplay /dev/vda2
  --- Physical volume ---
  PV Name               /dev/vda2                     1
  VG Name               vg-alpha                      2
  PV Size               256.00 MiB / not usable 4.00 MiB 3
  Allocatable           yes
  PE Size               4.00 MiB                      4
  Total PE              63
  Free PE               26                            5
  Allocated PE          37
```

```
  PV UUID               JWzDpn-LG3e-n2oi-9Etd-VT2H-PMem-1ZXwP1
```

1. **PV Name** (Nombre de PV) corresponde al nombre del dispositivo.
2. **VG Name** (Nombre de VG) muestra el grupo de volúmenes donde se encuentra el PV.
3. **PV Size** (Tamaño de PV) muestra el tamaño físico del PV, incluido todo el espacio no utilizable.
4. **PE Size** (Tamaño de PE) es el tamaño de la extensión física, que es el tamaño más pequeño a donde puede ser asignado un volumen lógico.

   Es también el factor de multiplicación que se utiliza en el cálculo del tamaño de cualquier valor informado en las unidades de PE, como *Free PE* (PE libre); por ejemplo: 26 PE x 4 MiB (el *PE Size* [Tamaño de PE]) da 104 MiB de espacio libre. El tamaño de un volumen lógico se redondeará a un factor de unidades de PE.

   LVM establece el tamaño de la PE automáticamente, aunque es posible especificarlo.
5. **Free PE** (PE libre) muestra cuántas unidades de PE están disponibles para la asignación para nuevos volúmenes lógicos.

Grupos de volúmenes

Use **vgdisplay** para visualizar información sobre grupos de volúmenes (GV). Si no se especifica ningún argumento para el comando, mostrará información sobre todos los VG. Si se usa el nombre del VG como un argumento, la información que se muestra se limitará a ese VG específico.

```
[root@serverX ~]# vgdisplay vg-alpha
  --- Volume group ---
  VG Name               vg-alpha          (1)
  System ID
  Format                lvm2
  Metadata Areas        3
  Metadata Sequence No  4
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                1
  Open LV               1
  Max PV                0
  Cur PV                3
  Act PV                3
  VG Size               1012.00 MiB       (2)
  PE Size               4.00 MiB
  Total PE              253               (3)
  Alloc PE / Size       175 / 700.00 MiB
  Free  PE / Size       78 / 312.00 MiB   (4)
  VG UUID               3snNw3-CF71-CcYG-Llk1-p6EY-rHEv-xfUSez
```

1. **VG Name** (Nombre de VG) es el nombre del grupo de volúmenes.
2. **VG Size** (Tamaño de VG) es el tamaño total del bloque de almacenamiento disponible para la asignación de volúmenes lógicos.
3. **Total PE** (PE total) es el tamaño total expresado en unidades de PE.
4. **Free PE / Size** (PE libre/tamaño) muestra cuánto espacio libre hay en el VG para distribuir para nuevos LV o para ampliar los LV existentes.

Volúmenes lógicos

Use **lvdisplay** para visualizar información sobre volúmenes lógicos (LV). Una vez más, ningún argumento con el comando mostrará información sobre todos los LV, y el uso del nombre del dispositivo del LV como un argumento mostrará información sobre ese dispositivo específico.

```
[root@serverX ~]# lvdisplay /dev/vg-alpha/hercules
  --- Logical volume ---
  LV Path                /dev/vg-alpha/hercules  (1)
  LV Name                hercules
  VG Name                vg-alpha                (2)
  LV UUID                5IyRea-W8Zw-xLHk-3h2a-IuVN-YaeZ-i3IRrN
  LV Write Access        read/write
  LV Creation host, time server1.example.com 2014-02-19 00:26:48 -0500
  LV Status              available
  # open                 1
  LV Size                700 MiB                 (3)
  Current LE             175                     (4)
  Segments               3
  Allocation             inherit
  Read ahead sectors     auto
  - current set to       8192
  Block device           252:0
```

1. **LV Path** (Ruta de LV) muestra el nombre del dispositivo de este volumen lógico.

   Es posible que algunas herramientas informen el nombre del dispositivo como **/dev/mapper/*vgname-lvname***; ambos representan el mismo LV.
2. **VG Name** (Nombre de VG) muestra el grupo de volúmenes donde se encuentra el PV.
3. **LV Size** (Tamaño de LV) muestra el tamaño total del LV. Use herramientas del sistema de archivos para comprobar el espacio libre y el espacio usado para el almacenamiento de datos.
4. **Current LE** (LE actual) muestra la cantidad de extensiones lógicas usadas por este LV. Una LE generalmente se asigna a una extensión física del VG y, por lo tanto, al volumen físico.

Referencias

Páginas del manual: **lvm**(8), **pvcreate**(8), **vgcreate**(8), **lvcreate**(8), **pvremove**(8), **vgremove**(8), **lvremove**(8), **pvdisplay**(8), **vgdisplay**(8), **lvdisplay**(8), **fdisk**(8), **gdisk**(8), **parted**(8), **partprobe**(8) y **mkfs**(8)

Práctica: Adición de un volumen lógico

En este trabajo de laboratorio, agregará un volumen físico, un grupo de volúmenes, un volumen lógico y un sistema de archivos XFS. Montará de forma persistente el sistema de archivos de volúmenes lógicos.

Recursos:	
Máquinas:	serverX

Resultados:
Un volumen lógico de 400 MiB denominado **`storage`** en el grupo de volúmenes **`shazam`**, montado en **`/storage`**. El grupo de volúmenes consta de dos volúmenes físicos, cada uno de 256 MiB.

Andes de comenzar
- Restablezca su sistema serverX.
- Inicie sesión en serverX.
- Abra una terminal.
- Cambie a raíz (**`sudo -i`**).

1. **Crear los recursos físicos**
   1.1. Use **`fdisk`** para crear dos particiones de 256 MiB cada una y configúrelas con el tipo Linux LVM.

```
[root@serverX ~]# fdisk /dev/vdb
```

   Nota: Los siguientes pasos omiten algunos resultados.

   1.2. Agregue una nueva partición primaria de 256 MiB.

```
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): Enter
Using default response p
Partition number (1-4, default 1): Enter
First sector (2048-20971519, default 2048): Enter
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519): +256M
```

   1.3. Cambie el tipo de partición a *Linux LVM - 0x8e*.

```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'
```

1.4. Repita los dos pasos anteriores para agregar una segunda partición primaria del mismo tamaño en el siguiente espacio disponible para particiones.

1.5. Escriba los cambios en la tabla de particiones y salga.

```
Command (m for help): w
The partition table has been altered!
```

1.6. Use **partprobe** para registrar las nuevas particiones con el kernel.

```
[root@serverX ~]# partprobe
```

2. **Crear los volúmenes físicos**
Use **pvcreate** para agregar las dos nuevas particiones como PV.

```
[root@serverX ~]# pvcreate /dev/vdb1 /dev/vdb2
  Physical volume "/dev/vdb1" successfully created
  Physical volume "/dev/vdb2" successfully created
```

3. **Crear el grupo de volúmenes**
Use **vgcreate** para crear un nuevo VG denominado **shazam** creado a partir de los dos PV.

```
[root@serverX ~]# vgcreate shazam /dev/vdb1 /dev/vdb2
  Volume group "shazam" successfully created
```

4. **Crear el volumen lógico**
Use **lvcreate** para crear un LV de 400 MiB denominado **storage** desde el VG **shazam**.

```
[root@serverX ~]# lvcreate -n storage -L 400M shazam
  Logical volume "storage" created
```

Esto creará un dispositivo denominado **/dev/shazam/storage**, actualmente sin un sistema de archivos.

5. **Agregar un sistema de archivos persistente**
5.1. Use **mkfs** para colocar un sistema de archivos **xfs** en el LV **storage**; use el nombre del dispositivo del LV.

```
[root@serverX ~]# mkfs -t xfs /dev/shazam/storage
meta-data=/dev/shazam/storage    isize=256    agcount=4, agsize=25600 blks
...
```

5.2. Use **mkdir** para crear un punto de montaje en **/storage**.

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

5.3. Use **vim** para agregar la siguiente línea en la parte inferior de **/etc/fstab** en serverX:

```
/dev/shazam/storage    /storage    xfs  defaults  1 2
```

5.4. Use **mount** para verificar la entrada **/etc/fstab** y monte el nuevo dispositivo del LV **storage**.

```
[root@serverX ~]# mount -a
```

6. **Evaluar y revisar su trabajo**

6.1. Como prueba final, copie algunos archivos en **/storage** y verifique cuántos se copiaron.

```
[root@serverX ~]# cp -a /etc/*.conf /storage
[root@serverX ~]# ls /storage | wc -l
47
```

Comprobaremos que aún tengamos la misma cantidad de archivos en el siguiente ejercicio de práctica.

6.2. **fdisk -l /dev/*vdb*** le mostrará las particiones que existen en **/dev/vdb**.

```
[root@serverX ~]# fdisk -l /dev/vdb
```

Compruebe las entradas **/dev/vdb1** y **/dev/vdb2**, y observe las columnas **Id** (Id.) y **System** (Sistema) que muestran **8e** y **Linux LVM**, respectivamente.

6.3. **pvdisplay** le mostrará información sobre cada uno de los volúmenes físicos. De forma opcional, incluya el nombre del dispositivo para limitar detalles a un PV específico.

```
[root@serverX ~]# pvdisplay /dev/vdb2
  --- Physical volume ---
  PV Name               /dev/vdb2
  VG Name               shazam
  PV Size               256.00 MiB / not usable 4.00 MiB
  Allocatable           yes
  PE Size               4.00 MiB
  Total PE              63
  Free PE               26
  Allocated PE          37
  PV UUID               N64t6x-URdJ-fVU3-FQ67-zU6g-So7w-hvXMcM
```

Esto muestra que nuestro PV está asignado al VG *shazam*, tiene un tamaño de 256 MiB (aunque 4 MiB no se pueden utilizar) y el tamaño de nuestra extensión física (**PE Size** [Tamaño de PE]) es de 4 MiB (el tamaño de un LV asignable más pequeño).

Hay 63 PE, de las cuales 26 PE están libres para la asignación para LV en el futuro y 37 PE están asignadas actualmente a LV. Esto se traduce a los siguientes valores de MiB:

- Un total de 252 MiB (63 PE x 4 MiB); recuerde, 4 MiB no se pueden utilizar.
- 104 MiB libres (26 PE x 4 MiB)

- 148 MiB asignados (37 PE x 4 MiB)

6.4. **vgdisplay *vgname*** mostrará información sobre el grupo de volúmenes denominado **vgname**.

```
[root@serverX ~]# vgdisplay shazam
```

Compruebe lo siguiente:

- El valor de **VG Size** (Tamaño de VG) es **504,00 MiB**.
- El valor de **Total PE** (PE total) es **126**.
- El valor de **Alloc PE / Size** (PE asign. / Tamaño) es **100 / 400,00 MiB**.
- El valor de **Free PE / Size** (PE libre / Tamaño) es **26 / 104,00 MiB**.

6.5. **lvdisplay /dev/*vgname/lvname*** mostrará información sobre el volumen lógico denominado **lvname**.

```
[root@serverX ~]# lvdisplay /dev/shazam/storage
```

Observe los valores de **LV Path** (Ruta de LV), **LV Name** (Nombre de LV), **VG Name** (Nombre de VG), **LV Status** (Estado de LV), **LV Size** (Tamaño de LV) y **Current LE** (LE actual) (extensiones lógicas, que se asignan a extensiones físicas).

6.6. **mount** mostrará todos los dispositivos que están montados y todas las opciones de montaje. Debe incluir **/dev/shazam/storage**.

nota

Recordatorio: Muchas herramientas informarán en cambio el nombre del asignador de dispositivos, **/dev/mapper/shazam-storage**; es el mismo volumen lógico.

```
[root@serverX ~]# mount
```

Debe observar (probablemente, en la última línea) **/dev/mapper/shazam-storage** montado en **/storage** y la información de montaje asociada.

6.7. **df -h** mostrará espacio libre legible para el ser humano. De forma opcional, incluya el punto de montaje para limitar detalles a ese sistema de archivos.

```
[root@serverX ~]# df -h /storage
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/shazam-storage  397M   21M  377M   6% /storage
```

Estos valores, permitidos para metadatos del sistema de archivos, son lo que esperaríamos.

Extensión de volúmenes lógicos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Extender y reducir un grupo de volúmenes.
- Extender un LV con un sistema de archivos XFS.
- Extender un LV con un sistema de archivos ext4.

Extensión y reducción de un grupo de volúmenes

Se puede agregar más espacio en disco a un grupo de volúmenes mediante la adición de más volúmenes físicos. Esto se denomina extensión del grupo de volúmenes. Las nuevas extensiones físicas proporcionadas mediante los volúmenes físicos adicionales luego se pueden reasignar a volúmenes lógicos.

Los volúmenes físicos no usados se pueden eliminar de un grupo de volúmenes. Esto se denomina reducción del grupo de volúmenes. Se puede utilizar una herramienta denominada *pvmove* para trasladar datos desde extensiones de un volumen físico a extensiones de otros volúmenes físicos en el grupo de volúmenes. De esta manera, se puede agregar un nuevo disco a un grupo de volúmenes existentes, se pueden trasladar los datos desde un disco más antiguo o más lento hacia el disco nuevo y se puede eliminar el disco viejo del grupo de volúmenes. Esto se puede hacer mientras los volúmenes lógicos del grupo de volúmenes están en uso.

Importante

En los siguientes ejemplos, se usa el dispositivo **vdb** y sus particiones para ilustrar comandos LVM. En la práctica, estos ejemplos deberían usar los dispositivos correctos para el disco y las particiones del disco utilizados por el sistema.

Ampliación de un grupo de volúmenes

Potencialmente, son cuatro los pasos necesarios para ampliar un grupo de volúmenes:

1. **Prepare el dispositivo físico**.

   Al igual que en la creación de un nuevo grupo de volúmenes, se debe crear y preparar una nueva partición para usar como volumen físico de LVM.

   Use **`fdisk`**, **`gdisk`** o **`parted`** para crear una nueva partición para usar con LVM. Siempre configure el tipo de partición en **`Linux LVM`** (LVM Linux) en las particiones de LVM; use **`0x8e`** para particiones estilo MBR. Si es necesario, use **`partprobe`** para registrar la nueva partición con el kernel.

   De forma alternativa, use un disco entero, un arreglo RAID o un disco SAN.

   Solo se necesita preparar un dispositivo físico si no hay ninguno ya preparado, y se requiere un volumen físico nuevo para ampliar el grupo de volúmenes.

```
[root@serverX ~]# fdisk /dev/vdb
```

Use **m** para obtener ayuda, **p** para imprimir la tabla de particiones existentes, **n** para crear una partición nueva, **t** para cambiar el tipo de partición, **w** para escribir los cambios y **q** para salir.

2. **Cree el volumen físico**.

pvcreate se usa para etiquetar la partición (u otro dispositivo físico) para su uso con el LVM como volumen físico. Se escribe un encabezado para almacenar los datos de configuración del LVM directamente en el PV. Un PV se divide en extensiones físicas de un tamaño fijo; por ejemplo, bloques de 4 MiB. Use el nombre del dispositivo como el argumento para **pvcreate**.

```
[root@serverX ~]# pvcreate /dev/vdb2
```

Esto etiquetará el dispositivo **/dev/vdb2** como un PV, listo para la asignación en el grupo de volúmenes.

Un PV solo debe crearse si no hay PV libres para extender el VG.

3. **Amplíe un grupo de volúmenes**.

vgextend se usa para agregar un nuevo volumen físico al grupo de volúmenes existente. Use el nombre del VG y el nombre del dispositivo del PV como argumentos para **vgextend**.

```
[root@serverX ~]# vgextend vg-alpha /dev/vdb2
```

Esto ampliará el VG **vg-alpha** al tamaño del PV **/dev/vdb2**.

4. **Verifique que el nuevo espacio esté disponible**.

Use **vgdisplay** para confirmar que las extensiones físicas adicionales estén disponibles. Compruebe el **Free PE / Size** (PE libre/tamaño) en el resultado. No debe ser cero.

```
[root@serverX ~]# vgdisplay vg-alpha
  --- Volume group ---
  VG Name               vg-alpha
...
  Free  PE / Size       178 / 712.00 MiB
...
```

Reducción de un grupo de volúmenes

Son solo dos los pasos necesarios para ampliar un grupo de volúmenes:

1. **Traslade las extensiones físicas**.

pvmove se utiliza para reubicar todas las extensiones físicas usadas en el volumen físico para otros PV del VG. Esto solo es posible si hay suficientes extensiones libres en el VG y si todas corresponden a otros PV. Use el nombre del dispositivo del PV para el cual las PE se trasladarán como el argumento para el comando.

```
[root@serverX ~]# pvmove /dev/vdb2
```

Esto trasladará las PE desde **/dev/vdb2** a otros PV con PE libres en el mismo VG.

Advertencia

Antes de usar **pvmove**, se recomienda efectuar una copia de seguridad de los datos en los volúmenes lógicos del grupo de volúmenes. Una pérdida de energía imprevista durante la operación puede hacer que el grupo de volúmenes quede en un estado incoherente. Esto provocaría la pérdida de datos en volúmenes lógicos en el grupo de volúmenes.

2. **Reduzca el grupo de volúmenes**.

   vgreduce se usa para eliminar el volumen físico del grupo de volúmenes. Use el nombre del VG y el nombre del dispositivo del PV como argumentos para el comando.

```
[root@serverX ~]# vgreduce vg-alpha /dev/vdb2
```

   El PV **/dev/vdb2** ahora se elimina del VG **vg-alpha** y se puede agregar a otro VG. De forma alternativa, se puede usar **pvremove** para dejar de usar el dispositivo como un PV de forma permanente.

Ampliar un volumen lógico y su sistema de archivos XFS

Uno de los beneficios de los volúmenes lógicos es la capacidad para aumentar su tamaño sin experimentar tiempo de inactividad. Las extensiones físicas libres en un grupo de volúmenes se pueden agregar a un volumen lógico para extender su capacidad, que luego se puede usar para extender el sistema de archivos que contiene.

Ampliación de un volumen lógico

Son tres los pasos necesarios para ampliar un volumen lógico:

1. **Verifique que el grupo de volúmenes tenga espacio disponible**.

   vgdisplay se usa para verificar que haya suficientes extensiones físicas disponibles para su uso.

```
[root@serverX ~]# vgdisplay vg-alpha
  --- Volume group ---
  VG Name               vg-alpha
...
  Free  PE / Size       178 / 712.00 MiB
...
```

   Compruebe el **Free PE / Size** (PE libre/tamaño) en el resultado. Debe informar un valor igual o mayor que el espacio adicional requerido. Si no hay suficiente espacio

disponible, amplíe el grupo de volúmenes en al menos el espacio requerido. Consulte "Ampliación y reducción de un grupo de volúmenes".

2. **Amplíe el volumen lógico**.

   lvextend amplía el volumen lógico a un nuevo tamaño. Agregue el nombre del dispositivo del LV como el último argumento para el comando.

```
[root@serverX ~]# lvextend -L +300M /dev/vg-alpha/hercules
```

   Esto aumentará el tamaño del volumen lógico **hercules** en 300 MiB. Observe el signo "**+**" delante del tamaño: significa agregar este valor al tamaño existente; de lo contrario, el valor define el tamaño final exacto del LV.

   Al igual que **lvcreate**, hay varias maneras de especificar el tamaño: **-l** generalmente espera valores de extensiones físicas, mientras que **-L** espera tamaños en bytes o valores nombrados más grandes, como mebibytes y gibibytes.

   Algunos ejemplos:

   - **lvextend -l 128**: Cambia el tamaño del volumen lógico a *exactamente* 128 extensiones.
   - **lvextend -l +128**: Agrega 128 extensiones al tamaño actual del volumen.
   - **lvextend -L 128M**: Cambia el tamaño del volumen lógico a *exactamente* 128 MiB.
   - **lvextend -L +128M**: Agrega 128 MiB al tamaño actual del volumen lógico.
   - **lvextend -l +50%FREE**: Agrega el 50 % del espacio libre actual en el VG al LV.

3. **Amplíe el sistema de archivos**.

   xfs_growfs *`/mountpoint`* amplía el sistema de archivos para que ocupe el LV ampliado. **xfs_growfs** requiere que el sistema de archivos se monte mientras se está ejecutando; puede continuar usándose durante la operación de modificación del tamaño.

```
[root@serverX ~]# xfs_growfs /mnt/hercules
```

nota

Un error común es ejecutar **lvextend** y olvidarse de ejecutar **xfs_growfs**. Una alternativa a ejecutar estos pasos de forma consecutiva es incluir **-r** como una opción con el comando **lvextend**. Esto modifica el tamaño del sistema de archivos luego de que el VL se extienda, usando **fsadm**(8). Funciona con varios sistemas de archivos diferentes.

   - Es una buena idea verificar el nuevo tamaño del sistema de archivos montado:

     df -h *`/mountpoint`*.

Ampliar un volumen lógico y su sistema de archivos ext4

Ampliación de un volumen lógico
Los pasos para ampliar un volumen lógico basado en **ext4** son básicamente los mismos que para un LV basado en **xfs**, excepto por el paso para modificar el tamaño del sistema de archivos. Consulte "Ampliar un volumen lógico y su sistema de archivos XFS" para obtener más detalles.

1. **Verifique que el grupo de volúmenes tenga espacio disponible**.

   vgdisplay *vgname* se usa para verificar que haya suficientes extensiones físicas disponibles para su uso.

2. **Amplíe el volumen lógico**.

   lvextend -l +*extents* /dev/*vgname/lvname* amplía el volumen lógico */dev/vgname/lvname* en el valor de las *extenciones*.

3. **Amplíe el sistema de archivos**.

   resize2fs /dev/*vgname/lvname* amplía el sistema de archivos para ocupar el nuevo LV ampliado. Al igual que **xfs_growfs**, el sistema de archivos se puede montar y estar en uso mientras se encuentra en ejecución. Como alternativa, incluya la opción **-p** para ver el progreso de la operación de modificación del tamaño.

```
[root@serverX ~]# resize2fs /dev/vg-alpha/hercules
```

nota

La principal diferencia entre **xfs_growfs** y **resize2fs** es el argumento que se pasó para identificar el sistema de archivos. **xfs_growfs** toma el punto de montaje y **resize2fs** toma el nombre del volumen lógico.

Referencias

Páginas del manual: **lvm**(8), **pvcreate**(8), **pvmove**(8), **vgdisplay**(8), **vgextend**(8), **vgreduce**(8), **vgdisplay**(8), **vgextend**(8), **vgreduce**(8), **lvextend**(8), **fdisk**(8), **gdisk**(8), **parted**(8), **partprobe**(8), **xfs_growfs**(8) y **resize2fs**(8)

Práctica: Ampliación de un volumen lógico

En este trabajo de laboratorio, ampliará el volumen lógico agregado en el ejercicio de práctica anterior.

Recursos:	
Máquinas:	serverX

Resultados:
Un volumen lógico con el tamaño modificado, 700 MiB en total, denominado **`storage`** (almacenamiento) en el grupo de volúmenes **`shazam`**, montado en **`/storage`**. Modificación del tamaño llevada a cabo mientras el sistema de archivos aún está montado y en uso. Grupo de volúmenes ampliado para incluir un volumen físico adicional de 512 MiB, con un tamaño del VG total de 1 GiB.

Andes de comenzar
Completar Práctica: Adición de un volumen lógico

1. **Comprobar el espacio en el grupo de volúmenes**
   Use **`vgdisplay`** para comprobar si el VG tiene suficiente espacio libre para ampliar el LV hasta un tamaño total de 700 MiB.

```
[root@serverX ~]# vgdisplay shazam
  --- Volume group ---
  VG Name               shazam
  System ID
  Format                lvm2
...
  VG Size               504.00 MiB
  PE Size               4.00 MiB
  Total PE              126
  Alloc PE / Size       100 / 400.00 MiB
  Free  PE / Size       26 / 104.00 MiB
  VG UUID               OBBAtU-2nBS-4SW1-khmF-yJzi-z7bD-DpCrAV
```

   Solo hay 104 MiB disponibles (26 PE x extensiones de 4 MiB) y necesitamos al menos 300 MiB para tener un total de 700 MiB. Necesitamos ampliar el VG.

   Para una posterior comparación, use **`df`** para comprobar el espacio libre en el disco actual:

```
[root@serverX ~]# df -h /storage
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/shazam-storage  397M   21M  377M   6% /storage
```

2. Crear los recursos físicos

   Use **`fdisk`** para crear una partición adicional de 512 MiB y configúrela con el tipo Linux LVM.

   2.1.
```
[root@serverX ~]# fdisk /dev/vdb
```

Nota: Los siguientes pasos omiten algunos resultados.

2.2. Agregue una nueva partición primaria de 512 MiB.

```
Command (m for help): n
Partition type:
   p   primary (2 primary, 0 extended, 2 free)
   e   extended
Select (default p): Enter
Using default response p
Partition number (3,4, default 3): Enter
First sector (1050624-20971519, default 1050624): Enter
Using default value 1050624
Last sector, +sectors or +size{K,M,G} (1050624-20971519, default
 20971519): +512M
Partition 3 of type Linux and of size 512 MiB is set
```

2.3. Cambie el tipo de partición a *Linux LVM - 0x8e*.

```
Command (m for help): t
Partition number (1-3, default 3): Enter
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'
```

2.4. Escriba los cambios en la tabla de particiones y salga.

```
Command (m for help): w
The partition table has been altered!
```

2.5. Use **partprobe** para registrar las nuevas particiones con el kernel.

```
[root@serverX ~]# partprobe
```

3. **Crear el volumen físico**
Use **pvcreate** para agregar la nueva partición como un PV.

```
[root@serverX ~]# pvcreate /dev/vdb3
  Physical volume "/dev/vdb3" successfully created
```

4. **Ampliar el grupo de volúmenes**
4.1. Use **vgextend** para ampliar el VG denominado **shazam**, mediante el nuevo PV **/dev/vdb3**.

```
[root@serverX ~]# vgextend shazam /dev/vdb3
  Volume group "shazam" successfully extended
```

4.2. Use **vgdisplay** para comprobar nuevamente el espacio libre del VG **shazam**. Ahora, debe haber suficiente espacio libre.

```
[root@serverX ~]# vgdisplay shazam
  --- Volume group ---
```

```
  VG Name               shazam
  System ID
  Format                lvm2
...
  VG Size               1012.00 MiB
  PE Size               4.00 MiB
  Total PE              253
  Alloc PE / Size       100 / 400.00 MiB
  Free  PE / Size       153 / 612.00 MiB
  VG UUID               OBBAtU-2nBS-4SW1-khmF-yJzi-z7bD-DpCrAV
```

Ahora hay 612 MiB disponibles (153 PE x extensiones de 4MiB); perfecto.

5. **Ampliar el volumen lógico**
Use **`lvextend`** para ampliar el LV existente a 700 MiB.

```
[root@serverX ~]# lvextend -L 700M /dev/shazam/storage
  Extending logical volume storage to 700.00 MiB
  Logical volume storage successfully resized
```

nota

En nuestro ejemplo, especificamos el tamaño exacto para hacer el LV final, pero también podríamos haber usado:

- **`-L +300M`** para agregar el nuevo espacio usando el tamaño en MiB.
- **`-l 175`** para especificar el número total de extensiones (175 PE x 4 MiB).
- **`-l +75`** para agregar las extensiones adicionales necesarias.

6. **Modificar el tamaño del sistema de archivos**
Use **`xfs_growfs`** para ampliar el sistema de archivos XFS hasta el resto del espacio libre del LV.

```
[root@serverX ~]# xfs_growfs /storage
meta-data=/dev/mapper/shazamstorage  isize=256    agcount=4, agsize=25600 blks
...
```

7. **Verificar la disponibilidad del contenido y el nuevo tamaño del sistema de archivos**
Use **`df`** y **`ls | wc`** para revisar el nuevo tamaño del sistema de archivos y verifique que los archivos existentes aún estén presentes.

```
[root@serverX ~]# df -h /storage
Filesystem                 Size  Used Avail Use% Mounted on
/dev/mapper/shazam-storage  697M   21M  677M   3% /storage
[root@serverX ~]# ls /storage | wc -l
47
```

Los archivos aún están allí y el sistema de archivos tiene el tamaño esperado.

Trabajo de laboratorio: Administración del almacenamiento de gestión de volúmenes lógicos (LVM)

En este ltrabajo de aboratorio, modificará el tamaño de un volumen lógico existente, agregará recursos de LVM según sea necesario, y luego agregará un nuevo volumen lógico con un sistema de archivos XFS montado de manera persistente en este.

Recursos:	
Máquinas:	serverX

Resultados:

- Volumen lógico **`loans`** con tamaño modificado a 768 MiB y montado de forma persistente en **`/finance/loans`**.
- Un nuevo volumen lógico de 128 MiB denominado **`risk`** con un sistema de archivos XFS, montado de forma persistente en **`/finance/risk`**.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

```
[student@serverX ~]$ lab lvm setup
```

- Abra una terminal.
- Cambie a **`raíz`** usando **`sudo -i`**.

El departamento de finanzas de su empresa tiene un volumen lógico denominado **`loans`** que está empezando a ejecutarse sin espacio en el disco, y se le ha solicitado a usted que amplíe el espacio a un tamaño de 768 MiB.

También se le ha solicitado crear un nuevo sistema de archivos para alojar documentos para el equipo de administración de riesgos, que es parte del departamento de finanzas; se ha acordado un volumen lógico de 128 MiB denominado **`risk`** y debe montarse en **`/finance/risk`**. El sistema de archivos estándar de su empresa es XFS.

Hay un grupo de volúmenes denominado **`finance`** usado para alojar volúmenes lógicos del departamento, pero desafortunadamente no tiene espacio suficiente para ampliar el volumen lógico existente y agregar uno nuevo, de modo que a usted se le han asignado 512 MiB más desde el disco duro actual. Se debe crear la partición.

Cuando haya finalizado, reinicie su máquina **`serverX`**, y luego ejecute el comando **`lab lvm grade`** desde su máquina **`serverX`** para verificar su trabajo.

1. Cree una partición de 512 MiB en **`/dev/vdb`**; inicialícela como un volumen físico y amplíe el grupo de volúmenes **`finance`** con esta.

2. Amplíe el volumen lógico **loans** a 768 MiB, que incluye el sistema de archivos.

3. En el grupo de volúmenes existente, cree un nuevo volumen lógico denominado **risk** de un tamaño de 128 MiB. Agregue un sistema de archivos XFS y móntelo de forma persistente en **/finance/risk**.

4. Cuando haya finalizado, reinicie su máquina **serverX**, y luego ejecute el comando **lab lvm grade** desde su máquina **serverX** para verificar su trabajo.

Solución

En este ltrabajo de aboratorio, modificará el tamaño de un volumen lógico existente, agregará recursos de LVM según sea necesario, y luego agregará un nuevo volumen lógico con un sistema de archivos XFS montado de manera persistente en este.

Recursos:	
Máquinas:	serverX

Resultados:

- Volumen lógico **loans** con tamaño modificado a 768 MiB y montado de forma persistente en **/finance/loans**.
- Un nuevo volumen lógico de 128 MiB denominado **risk** con un sistema de archivos XFS, montado de forma persistente en **/finance/risk**.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

```
[student@serverX ~]$ lab lvm setup
```

- Abra una terminal.
- Cambie a **raíz** usando **sudo -i**.

El departamento de finanzas de su empresa tiene un volumen lógico denominado **loans** que está empezando a ejecutarse sin espacio en el disco, y se le ha solicitado a usted que amplíe el espacio a un tamaño de 768 MiB.

También se le ha solicitado crear un nuevo sistema de archivos para alojar documentos para el equipo de administración de riesgos, que es parte del departamento de finanzas; se ha acordado un volumen lógico de 128 MiB denominado **risk** y debe montarse en **/finance/risk**. El sistema de archivos estándar de su empresa es XFS.

Hay un grupo de volúmenes denominado **finance** usado para alojar volúmenes lógicos del departamento, pero desafortunadamente no tiene espacio suficiente para ampliar el volumen lógico existente y agregar uno nuevo, de modo que a usted se le han asignado 512 MiB más desde el disco duro actual. Se debe crear la partición.

Cuando haya finalizado, reinicie su máquina **serverX**, y luego ejecute el comando **lab lvm grade** desde su máquina **serverX** para verificar su trabajo.

1. Cree una partición de 512 MiB en **/dev/vdb**; inicialícela como un volumen físico y amplíe el grupo de volúmenes **finance** con esta.

   1.1. Use **fdisk** para crear una partición de 512 MiB y configúrela con el tipo Linux LVM.

   ```
   [root@serverX ~]# fdisk /dev/vdb
   ```

   Nota: Los siguientes pasos omiten algunos resultados.

1.2. Agregue una nueva partición primaria de 512 MiB.

```
Command (m for help): n
Partition type:
   p   primary (1 primary, 0 extended, 3 free)
   e   extended
Select (default p): Enter
Partition number (2-4, default 2): Enter
First sector (1050624-20971519, default 1050624): Enter
Last sector, +sectors or +size{K,M,G} (1050624-20971519, default
 20971519): +512M
```

1.3. Cambie el tipo de partición a *Linux LVM - 0x8e*.

```
Command (m for help): t
Partition number (1,2, default 2): Enter
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'
```

1.4. Escriba los cambios en la tabla de particiones y salga.

```
Command (m for help): w
The partition table has been altered!
```

1.5. Use **partprobe** para registrar la nueva partición con el kernel.

```
[root@serverX ~]# partprobe
```

1.6. Use **pvcreate** para agregar la partición como un PV.

```
[root@serverX ~]# pvcreate /dev/vdb2
  Physical volume "/dev/vdb2" successfully created
```

1.7. Use **vgextend** para ampliar el VG denominado **finance**, usando el nuevo PV **/dev/vdb2**.

```
[root@serverX ~]# vgextend finance /dev/vdb2
  Volume group "finance" successfully extended
```

2. Amplíe el volumen lógico **loans** a 768 MiB, que incluye el sistema de archivos.

2.1. Use **lvextend** para ampliar el LV **loans** a 768 MiB.

```
[root@serverX ~]# lvextend -L 768M /dev/finance/loans
  Extending logical volume loans to 768.00 MiB
  Logical volume loans successfully resized
```

nota

De forma alternativa, podría haber usado **`-L +512M`** para modificar el tamaño del LV.

2.2. Use **`xfs_growfs`** para ampliar el sistema de archivos XFS hasta el resto del espacio libre del LV.

```
[root@serverX ~]# xfs_growfs /finance/loans
meta-data=/dev/mapper/finance-loans isize=256    agcount=4, agsize=16384 blks
...
```

nota

En este ejemplo, se muestra el paso **`xfs_growfs`** para ampliar el sistema de archivos. Una alternativa hubiese sido agregar la opción "**`-r`**" al comando **`lvextend`**.

3. En el grupo de volúmenes existente, cree un nuevo volumen lógico denominado **`risk`** de un tamaño de 128 MiB. Agregue un sistema de archivos XFS y móntelo de forma persistente en **`/finance/risk`**.

3.1. Use **`lvcreate`** para crear un LV de 128 MiB denominado **`risk`** desde el VG **`finance`**.

```
[root@serverX ~]# lvcreate -n risk -L 128M finance
  Logical volume "risk" created
```

3.2. Use **`mkfs`** para colocar un sistema de archivos **`xfs`** en el LV **`risk`**; use el nombre del dispositivo del LV.

```
[root@serverX ~]# mkfs -t xfs /dev/finance/risk
meta-data=/dev/finance/risk      isize=256    agcount=4, agsize=8192 blks
...
```

3.3. Use **`mkdir`** para crear un punto de montaje en **`/finance/risk`**.

```
[root@serverX ~]# mkdir /finance/risk
```

3.4. Use **`vim`** para agregar la siguiente línea en la parte inferior de **`/etc/fstab`** en serverX:

```
/dev/finance/risk  /finance/risk  xfs  defaults  1 2
```

3.5. Use **`mount`** para verificar la entrada **`/etc/fstab`** y monte el nuevo dispositivo del LV **`risk`**.

```
[root@serverX ~]# mount -a
```

4. Cuando haya finalizado, reinicie su máquina **serverX**, y luego ejecute el comando **lab lvm grade** desde su máquina **serverX** para verificar su trabajo.

4.1.
```
[root@serverX ~]$ systemctl reboot
```

4.2.
```
[student@serverX ~]$ lab lvm grade
```

Resumen

Conceptos de la gestión de volúmenes lógicos

- Los componentes de la gestión de volúmenes lógicos incluyen dispositivos de almacenamiento, grupos de volúmenes para agrupar PV y alojar volúmenes lógicos, y un sistema de archivos adecuado agregado al LV; por ejemplo, **`xfs`** o **`ext4`**.

Gestión de volúmenes lógicos

- **`pvcreate`**, **`pvremove`** y **`pvdisplay`** crean, eliminan y detallan volúmenes físicos (PV).
- **`vgcreate`**, **`vgremove`** y **`vgdisplay`** crean, eliminan y detallan grupos de volúmenes (VG).
- **`lvcreate`**, **`lvremove`** y **`lvdisplay`** crean, eliminan y detallan volúmenes lógicos (LV).
- La adición de volúmenes lógicos se realiza en el orden PV, VG y LV.
- La eliminación de volúmenes lógicos se realiza en el orden LV, VG y PV.

Extensión de volúmenes lógicos

- Ampliar un grupo de volúmenes (VG) usando **`pvcreate`** y **`vgextend`**; usar **`vgdisplay`** para comprobar los resultados.
- Reducir un VG usando **`pvmove`** y **`vgreduce`**.
- Ampliar un volumen lógico (LV) usando **`lvextend`**.
- Usar **`xfs_growfs`** para cambiar el tamaño de sistemas de archivos **`xfs`**.
- Usar **`resize2fs`** para cambiar el tamaño de sistemas de archivos **`ext4`**.

redhat. TRAINING

CAPÍTULO 11

ACCESO A ALMACENAMIENTO DE RED CON EL SISTEMA DE ARCHIVOS DE RED (NFS)

Descripción general	
Meta	Usar autofs y línea de comandos para montar y desmontar almacenamiento de red con el NFS.
Objetivos	• Montar, acceder y desmontar almacenamiento de red con el NFS. • Automontado y acceso a almacenamiento de red con NFS.
Secciones	• Montaje de almacenamiento de red con el NFS (y práctica) • Automontaje de almacenamiento de red con el NFS (y práctica)
Trabajo de laboratorio	• Acceso a almacenamiento de red con el sistema de archivos de red (NFS)

Montaje de almacenamiento de red con NFS

Objetivos

Luego de finalizar esta sección, los estudiantes deberán poder montar, acceder y desmontar manualmente un recurso compartido de NFS.

Montaje y desmontaje manual de archivos compartidos de NFS

NFS, el *sistema de archivos de red*, es un protocolo estándar de Internet usado por Linux, UNIX y sistemas operativos similares como su sistema de archivos de red nativo. Es una extensión abierta y activa bajo un estándar que admite características nativas de sistemas de archivos y permisos de Linux.

Red Hat Enterprise Linux 7 admite NFSv4 (versión 4 del protocolo) de forma predeterminada y, si no está disponible, recurre automáticamente a NFSv3 y NFSv2. NFSv4 utiliza el protocolo TCP para comunicarse con el servidor, mientras las versiones anteriores de NFS pueden usar TCP o UDP.

Los servidores de NFS *exportan* recursos compartidos (directorios) y los clientes de NFS montan los recursos compartidos en un punto de montaje local (directorio). El punto de montaje local debe existir. Los recursos compartidos de NFS se pueden montar de diversas maneras:

- montar manualmente un recurso compartido de NFS usando el comando **`mount`**.
- montar automáticamente un recurso compartido de NFS en el arranque usando **`/etc/fstab`**.
- montar un recurso compartido de NFS a pedido a través de un proceso conocido como *automontaje*.

Protección del acceso a archivos con recursos compartidos de NFS

Los servidores NFS protegen el acceso a archivos usando varios métodos: **`none`**, **`sys`**, **`krb5`**, **`krb5i`** y **`krb5p`**. El servidor NFS puede elegir ofrecer un único método o varios métodos para cada recurso compartido exportado. Los clientes NFS deben conectarse al recurso compartido exportado usando uno de los métodos obligatorios para ese recurso compartido, especificado como una opción de montaje **`sec=`*`method`***.

Métodos de protección

- **`none`**: Acceso anónimo a los archivos, a las escrituras en el servidor (si está permitido) se les asignará UID y GID de **`nfsnobody`**.
- **`sys`**: Acceso a archivos basado en los permisos de archivos Linux estándares para valores de UID y GID. Si no se especifica, este es el valor predeterminado.
- **`krb5`**: los clientes deben probar su identidad mediante Kerberos, y luego se aplican los permisos de archivos de Linux estándares.
- **`krb5i`**: agrega criptográficamente una garantía sólida de que los datos de cada solicitud aún no han sido utilizados de forma indebida.

- **krb5p**: agrega un cifrado a todas las solicitudes entre el cliente y el servidor, lo que evita la exposición de los datos en la red. Esto tendrá un impacto en el rendimiento.

Importante

Las opciones de Kerberos requerirán, como mínimo, **/etc/krb5.keytab** y una configuración de autenticación adicional que no está cubierta en esta sección (que se una al dominio de Kerberos). Normalmente, **/etc/krb5.keytab** será proporcionado por el administrador de autenticación o de seguridad. Solicite una **keytab** que incluya un *director de host*, *director de nfs* o (idealmente) ambos.

NFS usa el servicio **nfs-secure** para ayudar a negociar y administrar la comunicación con el servidor al conectarse a recursos compartidos protegidos por Kerberos. Se debe ejecutar para usar los recursos compartidos de NFS protegidos; **inícielo** y **habilítelo** para asegurarse de que siempre esté disponible.

```
[student@desktopX ~]$ sudo systemctl enable nfs-secure
ln -s '/usr/lib/systemd/system/nfs-secure.service'  ...
[student@desktopX ~]$ sudo systemctl start nfs-secure
```

nota

El servicio **nfs-secure** es parte del paquete **nfs-utils**, que debe instalarse de forma predeterminada. Si no está instalado, use:

```
[student@desktopX ~]$ sudo yum -y install nfs-utils
```

Montar un recurso compartido de NFS
Son tres los pasos básicos para montar un recurso compartido de NFS:

1. **Identificar**: El administrador del servidor NFS puede proporcionar detalles de exportación, incluidos los requisitos de seguridad. De forma alternativa:

   Los recursos compartidos de NFSv4 se pueden identificar al montar la carpeta raíz del servidor NFS y al explorar los directorios exportados. Haga esto como **raíz**. El acceso a recursos compartidos que están usando Kerberos será denegado, pero el nombre del recurso compartido (directorio) estará visible. Otros directorios compartidos se podrán explorar.

   ```
   [student@desktopX ~]$ sudo mkdir /mountpoint
   [student@desktopX ~]$ sudo mount serverX:/ /mountpoint
   [student@desktopX ~]$ sudo ls /mountpoint
   ```

   Los recursos compartidos de NFSv2 y de NFSv3 se pueden descubrir mediante el uso de **showmount**.

   ```
   [student@desktopX ~]$ showmount -e serverX
   ```

2. **Punto de montaje**: Use **mkdir** para crear un punto de montaje en una ubicación adecuada.

```
[student@desktopX ~]$ mkdir -p /mountpoint
```

3. **Montaje**: Hay dos opciones aquí: hacerlo de forma manual o que esté incorporado en el archivo **/etc/fstab**. Cambie a *raíz* o use **sudo** para cualquiera de las dos operaciones.

   - *Manual*: Use el comando **mount**.

```
[student@desktopX ~]$ sudo mount -t nfs -o sync serverX:/share /mountpoint
```

     La opción **-t nfs** es el tipo de sistema de archivos para recursos compartidos de NFS (no es estrictamente obligatorio, se muestra para ofrecer una visión completa). La opción **-o sync** indica a **mount** sincronizar inmediatamente las operaciones de escritura con el servidor NFS (el valor predeterminado es asíncrono). Se usará el método de protección predeterminado (sec=sys) para intentar montar el recurso compartido de NFS, usando permisos de archivos Linux estándares.

   - */etc/fstab:* Use **vim** para editar el archivo **/etc/fstab** y agregar la entrada de montaje en la parte inferior del archivo. El recurso compartido de NFS se montará en cada arranque del sistema.

```
[student@desktopX ~]$ sudo vim /etc/fstab
...
serverX:/share  /mountpoint  nfs  sync  0 0
```

Use **umount**, usando los privilegios *raíz*, para desmontar manualmente el recurso compartido.

```
[student@desktopX ~]$ sudo umount /mountpoint
```

Referencias

Páginas del manual: **mount**(8), **umount**(8), **fstab**(5) y **mount.nfs**(8).

Práctica: Montaje y desmontaje de NFS

En este trabajo de laboratorio, montará manualmente un recurso compartido de NFS protegido por Kerberos, accederá a este y, opcionalmente, lo desmontará. Cree un montaje de recurso compartido persistente en /etc/fstab, móntelo y acceda a este. serverX es el host de NFSv4.

Recursos:	
Archivos:	**`nfs_ldapuserX.txt`** y **`nfs_student.txt`**
Máquinas:	desktopX y serverX

Resultados:

- El usuario **`ldapuserX`** podrá de forma satisfactoria iniciar sesión en el recurso compartido de NFS **`public`** montado de forma persistente en **`/mnt/public`**, y acceder a este.
- El recurso compartido de NFS **`manual`** puede ser montado por usuarios ad hoc en **`/mnt/manual`**.

Andes de comenzar

- Restablezca el sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

```
[student@serverX ~]$ lab nfsmount setup
```

- Restablezca el sistema desktopX.
- Inicie sesión en su sistema de escritorio y configúrelo.

```
[student@desktopX ~]$ lab nfsmount setup
```

- Abra una terminal.

Importante

La configuración de serverX se utiliza para los ejercicios prácticos de este capítulo. Solo debe ejecutarse una vez.

S.H.I.E.L.D. (Storage Hardware Incorporating Every Last Document, hardware de almacenamiento que incorpora cada último documento) usa un servidor central, serverX, para alojar varios directorios compartidos con documentos. El acceso a la mayoría de los directorios es mediante usuarios basados en LDAP, que se autentican con Kerberos; no obstante, varios directorios compartidos están usando seguridad para el acceso a archivos Linux estándar. Los usuarios deben poder iniciar sesión en el recurso compartido de NFS **`manual`** y montarlo, y deben tener el recurso compartido de NFS **`public`** disponible constantemente.

A continuación, se proporcionan los detalles que necesitará:

- Nombre de usuario: **ldapuserX**
- Contraseña: **kerberos**
- serverX comparte los dos directorios en **/shares**: **manual** y **public**.
- Punto de montaje de desktopX: **/mnt/public** y **/mnt/manual**
- El recurso compartido de NFS **public** requiere autenticación de **krb5p** para el acceso; **manual** usa la seguridad **sys**.
- **krb5.keytab** está disponible en **http://classroom.example.com/pub/keytabs/&dsk;.keytab**.
- Cada recurso compartido debe tener acceso de lectura y escritura.

1. Descargue e instale el archivo **krb5.keytab** para habilitar el acceso a Kerberos y su seguridad.

```
[student@desktopX ~]$ sudo wget -O /etc/krb5.keytab http://classroom.example.com/
pub/keytabs/desktopX.keytab
```

2. Habilite e inicie el servicio **nfs-secure**.

```
[student@desktopX ~]$ sudo systemctl enable nfs-secure
ln -s '/usr/lib/systemd/system/nfs-secure.service'  ...
[student@desktopX ~]$ sudo systemctl start nfs-secure
```

3. Use **mkdir** para crear ambos puntos de montaje: **/mnt/public** y **/mnt/manual**.

```
[student@desktopX ~]$ sudo mkdir -p /mnt/{public,manual}
```

4. Cree el montaje persistente. Este montaje solo será accesible para usuarios autenticados.

   4.1. Use **vim** para editar el archivo **/etc/fstab**.

```
[student@desktopX ~]$ sudo vim /etc/fstab
```

   Agregue esta línea al final del archivo:

```
serverX:/shares/public  /mnt/public  nfs  sec=krb5p,sync  0 0
```

   4.2. Use **mount** para montar el recurso compartido y comenzar a usarlo.

```
[student@desktopX ~]$ sudo mount -a
```

5. Use **mount** para montar manualmente **/shares/manual** en **/mnt/manual**. Debido a que ya tiene un montaje NFSv4 protegido por Kerberos del mismo servidor, deberá especificar la opción **sec=sys**.

```
[student@desktopX ~]$ sudo mount -o sync,sec=sys serverX:/shares/manual /mnt/manual
```

6. Use **ssh** para cambiar a **ldapuserX** en **localhost** y confirme los montajes, y el acceso de lectura/escritura.

   6.1. Use **ssh** para iniciar sesión como **ldapuserX**.

   ```
   [student@desktopX ~]$ ssh ldapuserX@localhost
   ```

   Si observa algo similar a lo siguiente, escriba **yes** (sí) para aceptar y continuar.

   ```
   The authenticity of host 'localhost (::1)' can't be established.
   ECDSA key fingerprint is d9:cc:73:82:3b:8a:74:e4:11:2f:f3:2b:03:a4:46:4d.
   Are you sure you want to continue connecting (yes/no)? yes
   ```

   Ingrese la contraseña: **kerberos**.

   ```
   ldapuserX@localhost's password: kerberos
   ```

   6.2. Verifique que puede cambiar a ambos directorios compartidos y confirme que tiene acceso de lectura/escritura.

   Use **cd** para cambiar directorios.

   ```
   [ldapuserX@desktopX ~]$ cd /mnt/manual
   ```

   Use **echo** y **cat** para verificar el acceso de lectura y escritura.

   ```
   [ldapuserX@desktopX manual]$ echo hello > test.txt
   [ldapuserX@desktopX manual]$ cat test.txt
   hello
   ```

   Repita este paso para evaluar **/mnt/public**.

   Use **exit** o **Ctrl**+**D** para cerrar sesión de **ldapuserX**.

   6.3. Repita el paso anterior como **student** en ambos directorios. Debe poder cambiar de directorio y detallar **/mnt/manual**, pero obtendrá un **permiso denegado** en **/mnt/public** porque **student** no puede autenticar mediante Kerberos.

   En lugar de **test.txt**, se recomienda que utilice algo como **test2.txt**, dado que **student** no tiene permiso para escribir archivos que son propiedad de **ldapuserX**.

nota

Cuando haya terminado de utilizar el almacenamiento de red, puede usar el comando **umount** para desmontar manualmente los archivos compartidos de NFS.

```
[student@desktopX ~]$ sudo umount /mnt/manual
```

Automontaje de almacenamiento de red con NFS

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Describir los beneficios de usar el servicio de automontaje.
- Automontar los recursos compartidos de NFS usando asignaciones directas e indirectas, incluidos comodines.

Montaje de recursos compartidos de NFS con el servicio de automontaje

El servicio de automontaje es un servicio (**`autofs`**) que puede montar automáticamente recursos compartidos de NFS "*a pedido*", y desmontará automáticamente recursos compartidos de NFS cuando ya no se usen.

Beneficios del servicio de automontaje

- Los usuarios no necesitan tener privilegios *raíz* para ejecutar los comandos **`mount`**/**`umount`**.
- Los recursos compartidos de NFS configurados en el servicio de automontaje están disponibles para todos los usuarios de la máquina, sujetos a los permisos de acceso.
- Los recursos compartidos de NFS no están conectados permanentemente como las entradas en **`/etc/fstab`**, lo que libera recursos de red y sistemas.
- El servicio de automontaje se configura completamente del lado del cliente; no se requiere configuración del lado del servidor.
- El servicio de automontaje usa las mismas opciones de montaje usadas por el comando **`mount`**, incluidas opciones de seguridad.
- Apoyo tanto para la asignación de puntos de montaje directos como indirectos, lo que proporciona flexibilidad en las ubicaciones de los puntos de montaje.
- Los puntos de montaje indirectos se crean y se eliminan mediante **`autofs`**, lo que alivia las necesidades de administrarlos manualmente.
- NFS es el sistema de archivos predeterminado para el servicio de automontaje, pero se puede usar para automontar un intervalo de diferentes sistemas de archivos.
- **`autofs`** es un servicio que se administra como otros servicios del sistema.

Crear un automontaje

La configuración de un automontaje es un proceso de varios pasos:

1. Instale el paquete **`autofs`**.

```
[student@desktopX ~]$ sudo yum -y install autofs
```

Este paquete contiene todo lo necesario para usar el servicio de automontaje para recursos compartidos de NFS.

2. Agregue un archivo de *asignación maestra* a **/etc/auto.master.d**; este archivo identifica el directorio base usado para puntos de montaje e identifica el archivo de asignación usado para crear los automontajes.

   Use **vim** para crear y editar el archivo de asignación maestra:

```
[student@desktopX ~]$ sudo vim /etc/auto.master.d/demo.autofs
```

   El nombre del archivo de asignación maestra no es importante; pero, normalmente, es algo útil. El único requisito es que debe tener una extensión de **.autofs**. El archivo de asignación maestra puede contener varias entradas de asignación, o usar múltiples archivos para datos de configuración independientes.

   Agregue la entrada de asignación maestra, en este caso, para montajes asignados indirectamente:

```
/shares  /etc/auto.demo
```

   Esta entrada usaría el directorio **/shares** como la base para futuros automontajes indirectos. El archivo **/etc/auto.demo** contiene los detalles de montaje; use un nombre de archivo absoluto. El archivo **auto.demo** debe crearse antes de comenzar el servicio **autofs**.

   Para usar directamente puntos de montajes asignados, agregue una entrada en el mismo archivo (o en un archivo por separado):

```
/-  /etc/auto.direct
```

   Todas las entradas de asignación directa usan "**/-**" como el directorio base. En este caso, el archivo de asignación que contiene los detalles de montaje es **/etc/auto.direct**.

3. Cree los archivos de asignación. El archivo de asignación identifica el punto de montaje, las opciones de montaje y la ubicación de origen que se montará.

   Use **vim** para crear y editar el archivo de asignación:

```
[student@desktopX ~]$ sudo vim /etc/auto.demo
```

   El nombre del archivo no es importante, pero por convención se ubica en **/etc** y se llama **auto.*name***, donde el *nombre* es significativo del contenido incluido.

```
work  -rw,sync  serverX:/shares/work
```

   El formato de una entrada es *punto de montaje*, *opciones de montaje* y *ubicación de origen*. En este ejemplo, se muestra una entrada de asignación indirecta básica. Las asignaciones directas y las asignaciones indirectas que usan comodines se tratarán más adelante en esta sección.

- Conocido como la "*clave*" en las páginas del manual, el *punto de montaje* será creado y eliminado automáticamente por el servicio **autofs**. En este caso, el punto de montaje totalmente calificado será **/shares/work**; consulte el archivo de asignación maestra. El directorio **/shares** y el directorio **work** se crearán y eliminarán según sea necesario mediante el servicio **autofs**.

  En este ejemplo, el punto de montaje local refleja la estructura del directorio del servidor. El punto de montaje local puede tener cualquier nombre. No hay requisitos relativos a la alineación de los nombres del punto de montaje local y la estructura del directorio del servidor.

- Las *opciones de montaje* comienzan con un "**-**" (guión) y están separadas por comas sin espacios en blanco. Las opciones de montaje disponibles son las mismas que las disponibles para el comando de montaje manual equivalente. En este ejemplo, el servicio de automontaje intentará y montará el recurso compartido usando el acceso de lectura/escritura, la seguridad se basará en permisos de archivos Linux estándares (el predeterminado: sec=sys) y el servidor será sincronizado inmediatamente durante las operaciones de escritura.

  Hay un par de opciones útiles específicas del servicio de automontaje: **-fstype=** y **-strict**. Use **fstype** para especificar el sistema de archivos si no es NFS y use **strict** para tratar errores, cuando monte sistemas de archivos, como graves.

- La *ubicación de origen* para los recursos compartidos de NFS sigue el patrón **host:/pathname**; en este ejemplo, **&srv;:/shares/work**. Este directorio deberá haber sido *exportado* en serverX con soporte de acceso de lectura/escritura y permisos de archivos Linux estándares para que el montaje sea exitoso.

  Si el sistema de archivos que se montará comienza con una "**/**" (barra), como entradas de dispositivos locales o recursos compartidos SMB, es necesario agregar delante "**:**" (dos puntos); por ejemplo, un recurso compartido SMB sería **://&srv;/share**.

4. Inicie y habilite el servicio de automontaje.

   Use **systemctl** tanto para iniciar como para habilitar el servicio **autofs**.

```
[student@desktopX ~]$ sudo systemctl enable autofs
ln -s '/usr/lib/systemd/system/autofs.service'  ...
[student@desktopX ~]$ sudo systemctl start autofs
```

El archivo de asignación: asignaciones directas

Como su nombre lo implica, las asignaciones directas se usan para asignar un recurso compartido de NFS a un punto de montaje existente. El servicio de automontaje no intentará crear el punto de montaje automáticamente; debe existir antes de que el servicio **autofs** se inicie.

Para continuar con el ejemplo anterior, el contenido del archivo **/etc/auto.direct** podría verse del siguiente modo:

```
/mnt/docs  -rw,sync  serverX:/shares/docs
```

El punto de montaje (o clave) siempre es una ruta absoluta, que comienza con una "**/**" (barra). El resto del archivo de asignación usa la misma estructura.

Sólo el directorio más a la derecha se coloca bajo el control del servicio de automontaje. Así, la estructura del directorio sobre el punto de montaje (**/mnt** en este ejemplo) no queda oculta por **autofs**.

El archivo de asignación: asignaciones indirectas de comodines
Cuando un servidor NFS exporta varios subdirectorios dentro de un directorio, el servicio de automontaje se puede configurar para acceder a cualquiera de esos subdirectorios usando una única entrada de asignación. Como ejemplo, esto puede ser realmente útil para montar automáticamente directorios de *inicio* para usuarios desde un servidor NFS.

Para continuar con el ejemplo anterior, si **&srv;:/shares** exporta dos o más subdirectorios y se puede acceder a estos usando las mismas opciones de montaje, el contenido del archivo **/etc/auto.demo** podría verse del siguiente modo:

```
*  -rw,sync  serverX:/shares/&
```

El punto de montaje (o clave) es un "*****" (asterisco) y el subdirectorio en la ubicación de origen es el símbolo "**&**". Todo lo demás en la entrada es igual.

Cuando un usuario intenta acceder a **/shares/work**, la clave ***** (que es **work** en este ejemplo) reemplazará el símbolo & en la ubicación de origen y **&srv;:/shares/work** se montará. Al igual que con el ejemplo indirecto, el servicio **autofs** creará y eliminará automáticamente el directorio **work**.

Referencias

Páginas del manual: **autofs**(5), **automount**(8), **auto.master**(5) y **mount.nfs**(8)

Práctica: Automontaje de NFS

En este trabajo de laboratorio, instalará un paquete para admitir el automontaje. Cree un automontaje de asignación directa y un automontaje de asignación indirecta usando comodines. serverX es el host NFSv4.

Recursos:	
Archivos:	**`nfs_ldapuserX.txt`**
Máquinas:	**`desktopX`** y **`serverX`**

Resultados:
El usuario **`ldapuserX`** podrá iniciar sesión satisfactoriamente y usará los tres directorios automontados.

Andes de comenzar

- Restablezca el sistema desktopX.
- Inicie sesión en su sistema de escritorio y configúrelo.

```
[student@desktopX ~]$ lab nfsmount setup
```

- Abra una terminal.

Importante

La configuración de serverX realizada al comienzo de "*Montaje y desmontaje de NFS*" también se utiliza para este ejercicio práctico. Si aún no ha realizado la configuración del servidor, ejecútelo ahora. Solo debe ejecutarse una vez para ambos ejercicios de práctica.

S.H.I.E.L.D. (Storage Hardware Incorporating Every Last Document, hardware de almacenamiento que incorpora cada último documento) usa un servidor central, serverX, para alojar varios directorios compartidos con documentos. El acceso a estos directorios es a través de usuarios basados en LDAP, y se autentica el uso de Kerberos con cifrado. Los usuarios deben poder iniciar sesión y que los directorios compartidos se automonten con acceso de lectura y escritura, listos para su uso.

A continuación, se proporcionan los detalles que necesitará:

- Nombre de usuario: **`ldapuserX`**
- Contraseña: **`kerberos`**
- serverX comparte tres directorios en **`/shares`**: **`docs`**, **`work`** y **`public`**.
- El acceso a los archivos está protegido mediante el uso de Kerberos con cifrado: **`krb5p`**.
- Punto de montaje de desktopX: **`/shares`** para **`docs`** y **`work`** y una asignación directa de **`public`** a **`/mnt/public`**.

- **krb5.keytab** está disponible en **http://classroom.example.com/pub/keytabs/&dsk;.keytab**.
- Cada recurso compartido debe tener acceso de lectura y escritura.

Cuando haya finalizado su trabajo, reinicie la máquina **desktopX**, luego ejecute el comando **lab nfsmount grade** desde la máquina **desktopX** para verificar el trabajo.

1. Descargue e instale el archivo **krb5.keytab** para habilitar el acceso a Kerberos y su seguridad.

```
[student@desktopX ~]$ sudo wget -O /etc/krb5.keytab http://classroom.example.com/
pub/keytabs/desktopX.keytab
```

2. Habilite e inicie el servicio **nfs-secure**.

```
[student@desktopX ~]$ sudo systemctl enable nfs-secure
ln -s '/usr/lib/systemd/system/nfs-secure.service'  ...
[student@desktopX ~]$ sudo systemctl start nfs-secure
```

3. Use **yum** para instalar **autofs**, necesario para automontar directorios.

```
[student@desktopX ~]$ sudo yum -y install autofs
Loaded plugins: langpacks
Resolving Dependencies
...
Complete!
```

4. Cree los archivos de configuración de automontaje para el automontaje de *asignación directa*.

   4.1. Use **vim** para crear y editar el archivo **/etc/auto.master.d/direct.autofs**.

```
[student@desktopX ~]$ sudo vim /etc/auto.master.d/direct.autofs
```

   Nota: La extensión de archivos debe ser **.autofs**.

   Agregue la línea de la siguiente manera:

```
/-  /etc/auto.direct
```

   4.2. Use **vim** para crear y editar el archivo de asignación **auto.direct**.

```
[student@desktopX ~]$ sudo vim /etc/auto.direct
```

   Agregue la línea de la siguiente manera:

```
/mnt/public  -rw,sync,sec=krb5p  serverX:/shares/public
```

   Nota: Los nombres de los archivos de arriba no son importantes; fueron elegidos de modo que sean significativos.

5. Cree los archivos de configuración de automontaje para los automontajes de *asignación indirecta*.

   5.1. Use **vim** para crear y editar el archivo **/etc/auto.master.d/shares.autofs**.

   ```
   [student@desktopX ~]$ sudo vim /etc/auto.master.d/shares.autofs
   ```

   Nota: La extensión de archivos debe ser **.autofs**.

   Agregue la línea de la siguiente manera:

   ```
   /shares  /etc/auto.shares
   ```

   5.2. Use **vim** para crear y editar el archivo de asignación **auto.shares**.

   ```
   [student@desktopX ~]$ sudo vim /etc/auto.shares
   ```

   Agregue la línea de la siguiente manera:

   ```
   *  -rw,sync,sec=krb5p  serverX:/shares/&
   ```

   Nota: Los nombres de los archivos de arriba no son importantes; fueron elegidos de modo que sean significativos.

6. Use **mkdir** para crear el punto de montaje **/mnt/public** para el automontaje de *asignación directa*.

   ```
   [student@desktopX ~]$ sudo mkdir -p /mnt/public
   ```

7. Habilite e inicie el servicio de automontaje.

   ```
   [student@desktopX ~]$ sudo systemctl enable autofs
   ln -s '/usr/lib/systemd/system/autofs.service'  ...
   [student@desktopX ~]$ sudo systemctl start autofs
   ```

8. Use **ssh** para cambiar a **ldapuserX** en **localhost** y confirme los montajes, y el acceso de lectura/escritura.

   8.1. Use **ssh** para iniciar sesión como **ldapuserX**.

   ```
   [student@desktopX ~]$ ssh ldapuserX@localhost
   ```

   Si observa algo similar a lo siguiente, escriba **yes** (sí) para aceptar y continuar.

   ```
   The authenticity of host 'localhost (::1)' can't be established.
   ECDSA key fingerprint is d9:cc:73:82:3b:8a:74:e4:11:2f:f3:2b:03:a4:46:4d.
   Are you sure you want to continue connecting (yes/no)? yes
   ```

   Ingrese la contraseña: **kerberos**.

```
ldapuserX@localhost's password: kerberos
```

8.2. Verifique que puede cambiar a los directorios compartidos automontados y confirme que tiene acceso de lectura/escritura.

Use **cd** para cambiar directorios.

```
[ldapuserX@desktopX ~]$ cd /shares/docs
```

Use **echo** y **cat** para verificar el acceso de lectura y escritura.

```
[ldapuserX@desktopX docs]$ echo hello > test.txt
[ldapuserX@desktopX docs]$ cat test.txt
hello
```

Repita este paso para evaluar **/shares/work** y **/mnt/public**.

Use **exit** o **Ctrl**+**D** para cerrar sesión de **ldapuserX**.

9. Reinicie la máquina **desktopX**, y luego, ejecute el comando **lab nfsmount grade** desde la máquina **desktopX** para verificar el trabajo.

9.1.
```
[student@desktopX ~]$ sudo systemctl reboot
```

9.2.
```
[student@desktopX ~]$ lab nfsmount grade
```

Trabajo de laboratorio: Acceso a almacenamiento de red con sistema de archivos de red (NFS)

En este trabajo de laboratorio, instalará un paquete para admitir el automontaje. Cree un automontaje para el directorio "de inicio" de ldapuserX desde classroom.example.com, un host NFSv4.

Recursos:	
Máquinas:	**desktopX** y **classroom.example.com**

Resultados:
El usuario **ldapuserX** podrá iniciar sesión de forma satisfactoria y usar el directorio de *inicio* montado en **/home/guests/ldapuserX**.

Andes de comenzar
- Restablezca el sistema desktopX.
- Inicie sesión en su sistema de escritorio y configúrelo.

```
[student@desktopX ~]$ lab nfs setup
```

- Abra una terminal.

Umbrella Corp usa un servidor central, **classroom**, para alojar los directorios de *inicio* de los usuarios basados en sus LDAP. Los usuarios deben poder iniciar sesión y que los directorios de *inicio* se automonten con acceso de lectura y escritura, listos para su uso.

A continuación, se proporcionan los detalles que necesitará:

- Nombre de usuario: **ldapuserX**
- Contraseña: **kerberos**
- **classroom.example.com** comparte **/home/guests**.
- desktopX punto de montaje: **/home/guests/ldapuserX**
- El directorio de *inicio* debe tener acceso de lectura y escritura.

Cuando haya finalizado su trabajo, reinicie la máquina **desktopX**, luego ejecute el comando **lab nfs grade** desde la máquina **desktopX** para verificar el trabajo.

1. Instale todos los paquetes necesarios para automontar el directorio de *inicio*.
2. Agregue un archivo de configuración **auto.master.d** que identifique el directorio base y el archivo de asignación asociado (use el nombre que desee para el archivo de configuración, pero debe finalizar con **.autofs**), y cree el archivo de asignación asociado (use el nombre que desee para el archivo de asignación).

3. Habilite e inicie el servicio de automontaje.

4. Use **ssh** para cambiar a **ldapuserX** en **localhost** y confirme el montaje, y el acceso de lectura/escritura.

5. Reinicie la máquina **desktopX**, y luego, ejecute el comando **lab nfs grade** desde la máquina **desktopX** para verificar el trabajo.

Solución

En este trabajo de laboratorio, instalará un paquete para admitir el automontaje. Cree un automontaje para el directorio "de inicio" de ldapuserX desde classroom.example.com, un host NFSv4.

Recursos:	
Máquinas:	**desktopX** y **classroom.example.com**

Resultados:
El usuario **ldapuserX** podrá iniciar sesión de forma satisfactoria y usar el directorio de *inicio* montado en **/home/guests/ldapuserX**.

Andes de comenzar
- Restablezca el sistema desktopX.
- Inicie sesión en su sistema de escritorio y configúrelo.

```
[student@desktopX ~]$ lab nfs setup
```

- Abra una terminal.

Umbrella Corp usa un servidor central, **classroom**, para alojar los directorios de *inicio* de los usuarios basados en sus LDAP. Los usuarios deben poder iniciar sesión y que los directorios de *inicio* se automonten con acceso de lectura y escritura, listos para su uso.

A continuación, se proporcionan los detalles que necesitará:

- Nombre de usuario: **ldapuserX**
- Contraseña: **kerberos**
- **classroom.example.com** comparte **/home/guests**.
- desktopX punto de montaje: **/home/guests/ldapuserX**
- El directorio de *inicio* debe tener acceso de lectura y escritura.

Cuando haya finalizado su trabajo, reinicie la máquina **desktopX**, luego ejecute el comando **lab nfs grade** desde la máquina **desktopX** para verificar el trabajo.

1. Instale todos los paquetes necesarios para automontar el directorio de *inicio*.

   Use **yum** para instalar **autofs**.

```
[student@desktopX ~]$ sudo yum -y install autofs
Loaded plugins: langpacks
Resolving Dependencies
...
Complete!
```

2. Agregue un archivo de configuración **auto.master.d** que identifique el directorio base y el archivo de asignación asociado (use el nombre que desee para el archivo de

configuración, pero debe finalizar con **.autofs**), y cree el archivo de asignación asociado (use el nombre que desee para el archivo de asignación).

2.1. Use **vim** para crear y editar el archivo **/etc/auto.master.d/home.autofs**.

```
[student@desktopX ~]$ sudo vim /etc/auto.master.d/home.autofs
```

Agregue la línea de la siguiente manera:

```
/home/guests  /etc/auto.home
```

nota

Esta solución utiliza **home.autofs** como el archivo de asignación maestra y **auto.home** como el archivo de asignación, pero los nombres de archivos no son importantes.

2.2. Use **vim** para crear y editar el archivo de asignación **auto.home**.

```
[student@desktopX ~]$ sudo vim /etc/auto.home
```

Agregue la línea de la siguiente manera:

```
*  -rw,sync  classroom.example.com:/home/guests/&
```

3. Habilite e inicie el servicio de automontaje.

```
[student@desktopX ~]$ sudo systemctl enable autofs
ln -s '/usr/lib/systemd/system/autofs.service'  ...
[student@desktopX ~]$ sudo systemctl start autofs
```

4. Use **ssh** para cambiar a **ldapuserX** en **localhost** y confirme el montaje, y el acceso de lectura/escritura.

4.1. Use **ssh** para iniciar sesión como **ldapuserX**.

```
[student@desktopX ~]$ ssh ldapuserX@localhost
```

Si observa algo similar a lo siguiente, escriba **yes** (sí) para aceptar y continuar.

```
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is d9:cc:73:82:3b:8a:74:e4:11:2f:f3:2b:03:a4:46:4d.
Are you sure you want to continue connecting (yes/no)? yes
```

Ingrese la contraseña: **kerberos**.

```
ldapuserX@localhost's password: kerberos
```

4.2. Verifique el directorio actual y el acceso de lectura/escritura.

Use **pwd** para verificar el directorio actual.

```
[ldapuserX@desktopX ~]$ pwd
/home/guests/ldapuserX
```

Use **echo** y **cat** para verificar el acceso de lectura y escritura.

```
[ldapuserX@desktopX ~]$ echo hello > test.txt
[ldapuserX@desktopX ~]$ cat test.txt
hello
```

Use **exit** o **Ctrl**+**D** para cerrar sesión de **ldapuserX**.

5. Reinicie la máquina **desktopX**, y luego, ejecute el comando **lab nfs grade** desde la máquina **desktopX** para verificar el trabajo.

5.1.
```
[student@desktopX ~]$ sudo systemctl reboot
```

5.2.
```
[student@desktopX ~]$ lab nfs grade
```

Resumen

Montaje de almacenamiento de red con NFS

- Identifique los detalles del recurso compartido de NFS; monte con NFSv4 la carpeta raíz del servidor de NFS.
- Cree un directorio de punto de montaje.
- Use **`mount`** o actualice **`/etc/fstab`** para montar el recurso compartido de NFS.
- Use **`umount`** para desmontar un recurso compartido de NFS.

Automontaje de almacenamiento de red con NFS

- Instale el paquete necesario: **`autofs`**.
- Cree un archivo de asignación maestra en **`/etc/auto.master.d/`*`file`*`.autofs`**.
- Cree un archivo de asignación para acceder al recurso compartido de NFS: **`/etc/auto.`*`name`***.
  - Asignaciones directas.
  - Asignaciones indirectas.
  - Asignaciones indirectas usando comodines.
- Inicie y habilite el servicio **`autofs`** mediante **`systemctl`**.

redhat. TRAINING

CAPÍTULO 12

ACCESO A ALMACENAMIENTO DE RED CON SMB

Descripción general	
Meta	Usar autofs y línea de comandos para montar y desmontar sistemas de archivos SMB.
Objetivos	• Montar, automontar y desmontar sistemas de archivos SMB.
Secciones	• Acceso a almacenamiento de red con SMB (y práctica)
Trabajo de laboratorio	• Acceso a almacenamiento de red con SMB

Acceso a almacenamiento de red con SMB

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder realizar lo siguiente:

- Montar y desmontar sistemas de archivos SMB usando la línea de comandos.
- Automontar sistemas de archivos SMB.

Montaje y desmontaje manual de sistemas de archivos SMB

Muchas organizaciones necesitan proporcionar almacenamiento de red e imprimir servicios para una variedad de sistemas operativos de escritorio. Red Hat Enterprise Linux usa el servidor Samba para proporcionar servicios que los clientes de Microsoft Windows pueden usar. Samba implementa el protocolo Server Message Block (SMB), y Common Internet File System (CIFS) es un dialecto de SMB. A menudo, los dos nombres se usan de forma intercambiable.

Conexión a recursos compartidos de SMB/CIFS

Los escritorios y servidores de Red Hat se pueden conectar a recursos compartidos ofrecidos a través de *cualquier* servidor que use el protocolo SMB.

Tres pasos básicos para acceder a un recurso compartido de SMB

1. *Identificar* el recurso compartido remoto al que se desea acceder.
2. *Determinar el punto de montaje* donde el recurso compartido debe montarse y crear el directorio vacío del punto de montaje.
3. *Montar* el sistema de archivos de red mediante un comando o cambio de configuración correspondiente.

Antes de comenzar, hay un paquete que se debe instalar para poder montar los recursos compartidos de SMB: **`cifs-utils`**. Tanto el comando **`mount`** como el servicio de automontaje de **`autofs`** requieren este paquete para montar los sistema de archivos de CIFS.

Un segundo paquete, **`samba-client`**, tiene algunas utilidades de línea de comando útiles (por ejemplo, **`smbclient`**) y a menudo vale la pena instalarlo también.

Montar un recurso compartido de SMB

1. **Identificación**: El administrador del host del servidor SMB puede proporcionar detalles del recurso compartido, como *nombre de usuario* y *contraseña*, nombres del *recurso compartido*, etc. Una alternativa es usar un cliente que puede navegar por los recursos compartidos, como **`smbclient`**.

   ```
   [student@desktopX ~]$ smbclient -L //serverX
   ```

   La opción **`-L`** pide a **`smbclient`** que detalle los recursos compartidos disponibles en serverX.

2. **Punto de montaje**: Use **mkdir** para crear un punto de montaje en una ubicación adecuada.

```
[student@desktopX ~]$ mkdir -p /mountpoint
```

3. **Montaje**: Hay dos opciones aquí: hacerlo de forma manual o que esté incorporado en el archivo **/etc/fstab**. Cambie a *raíz* o use **sudo** para cualquiera de las dos operaciones.

   - *Manual*: Use el comando **mount**.

```
[student@desktopX ~]$ sudo mount -t cifs -o guest //serverX/share /mountpoint
```

     La opción **-t cifs** es el tipo de sistemas de archivos para recursos compartidos de SMB y la opción **-o guest** indica a **mount** que intente y se autentique como una cuenta de *guest* sin una contraseña.

   - */etc/fstab*: Use **vim** para editar el archivo **/etc/fstab** y agregar la entrada de montaje en la parte inferior del archivo. El recurso compartido de SMB se montará en cada arranque del sistema.

```
[student@desktopX ~]$ sudo vim /etc/fstab
...
//serverX/share  /mountpoint  cifs  guest  0 0
```

Use **umount**, usando los privilegios de *raíz*, para desmontar manualmente el recurso compartido.

```
[student@desktopX ~]$ sudo umount /mountpoint
```

Autenticación de recursos compartidos de SMB

Los recursos compartidos de SMB se pueden marcar como no navegables, lo que significa que los clientes como **smbclient** no los mostrarán. Aún se puede acceder a los recursos compartidos de SMB al especificar explícitamente el nombre del recurso compartido durante la operación de montaje.

Generalmente, los servidores de SMB restringen el acceso a usuarios específicos o grupos de usuarios. El acceso a recursos compartidos requerirá la presentación de las credenciales adecuadas en el servidor SMB. Hay una variedad de métodos de autenticación que un servidor SMB puede elegir implementar, demasiados como para cubrirlos aquí.

Una opción común para la autenticación es el par **nombre de usuario** y **contraseña**. Estos se pueden agregar al comando **mount** (o la entrada **/etc/fstab**) o almacenar en un archivo de **credenciales** al que se deriva durante la operación de montaje. El comando **mount** solicitará una contraseña si no se la proporciona, pero debe ser proporcionada si se usa **/etc/fstab**. El acceso de guests puede solicitarse explícitamente con la opción **guest**.

Algunos ejemplos:

```
[student@desktopX ~]$ sudo mount -t cifs -o guest //serverX/docs /public/docs
```

Monte el recurso compartido de SMB **//&srv;/docs** en **/public/docs** e intente autenticarlo como *guest*.

```
[student@desktopX ~]$ sudo mount -t cifs -o username=watson //serverX/cases /bakerst/
cases
```

Monte el recurso compartido de SMB **//&srv;/cases** en **/bakerst/cases** e intente autenticarlo como *watson*. El comando **mount** solicitará la contraseña en este ejemplo.

El archivo de **credenciales** ofrece una mejor seguridad porque la contraseña se almacena en un archivo más seguro, mientras que el archivo **/etc/fstab** se examina fácilmente.

```
[student@desktopX ~]$ sudo mount -t cifs -o credentials=/secure/sherlock //serverX/
sherlock /home/sherlock/work
```

Monte el recurso compartido de SMB **//&srv;/sherlock** en **/home/sherlock/work** e intente autenticar con las credenciales almacenadas en **/secure/sherlock**.

El formato para el archivo de **credenciales** es:

```
username=username
password=password
domain=domain
```

Debe colocarse en alguna parte segura con solo acceso *raíz* (por ejemplo, **chmod** 600).

Durante las operaciones de archivos, el servidor SMB supervisará el acceso de archivos con las credenciales usadas para montar el recurso compartido. El cliente revisará el acceso de archivos con el UID/GID de los archivos enviados desde el servidor. Esto significa que el cliente deberá tener el mismo UID/GID y, si es necesario, la misma membresía de grupo complementaria que los archivos del servidor SMB.

Hay una cantidad de opciones de montaje que manejan métodos de autenticación alternativos y de comprobación del acceso local, como multiusuario (y cifscreds) y opciones basadas en Kerberos. No se cubrirán aquí; para obtener más información, consulte las páginas de **man** y los artículos disponibles en **access.redhat.com**.

Montaje de sistemas de archivos de SMB con el servicio de automontaje

El uso del comando **mount** requiere privilegios de *raíz* para la conexión con los recursos compartidos de SMB. De forma alternativa, se pueden agregar entradas a **/etc/fstab**, pero las conexiones a los servidores SMB estarían activas todo el tiempo.

El servicio de automontaje, o **autofs**, se puede configurar para montar recursos compartidos de SMB "a pedido", cuando un proceso intenta acceder a un archivo en el recurso compartido de SMB. El servicio de automontaje luego desmontará el recurso compartido cuando ya no se encuentre en uso, después de un determinado período de inactividad.

El proceso para configurar un automontaje en un recurso compartido de SMB usando **autofs** es básicamente el mismo que otros automontajes:

- Agregue un archivo de configuración **auto.master.d** que identifique el directorio base para recursos compartidos y el archivo de asignación asociado.
- Cree o edite el archivo de asignación para incluir los detalles de montaje para el recurso compartido de SMB.

- Habilite e inicie el servicio **autofs**.

nota

Si aún no está instalado, instale el paquete **autofs**. Al igual que **mount**, el servicio de automontaje también depende del paquete **cifs-utils** para montar los recursos compartidos de SMB.

El archivo de asignación
Se debe especificar el tipo de sistema de archivos con la opción **-fstype=cifs** y luego una lista de opciones de montaje separadas por comas, las mismas opciones de montaje usadas por el comando **mount**. Delante de la dirección URI del servidor deben agregarse dos puntos ":".

Un ejemplo:

Lo siguiente crea un automontaje en **/bakerst/cases** para el recurso compartido de SMB **//&srv;/cases**, y autentica conforme al archivo de credenciales **/secure/sherlock**.

- **/etc/auto.master.d/bakerst.autofs** Contenido:

```
/bakerst   /etc/auto.bakerst
```

- **/etc/auto.bakerst** Contenido:

```
cases  -fstype=cifs,credentials=/secure/sherlock  ://serverX/cases
```

- Contenido de **/secure/sherlock** (propiedad de **raíz**, perms **600**):

```
username=sherlock
password=violin221B
domain=BAKERST
```

- Habilitación e inicio de **autofs**:

```
[student@desktopX ~]$ sudo systemctl enable autofs
[student@desktopX ~]$ sudo systemctl start autofs
```

Referencias

Páginas del manual: **mount**(8), **umount**(8), **fstab**(5), **mount.cifs**(8), **smbclient**(1), **autofs**(5), **automount**(8) y **auto.master**(5)

Práctica: Montaje de un sistema de archivos de SMB

En este trabajo de laboratorio, creará una entrada de montaje en **/etc/fstab** y la montará.

Recursos:	
Archivos:	**samba.txt** en el directorio del servidor, para pruebas.
Máquinas:	**desktopX** y **serverX**

Resultados:

- Paquete **cifs-utils** instalado.
- La carpeta de inicio de estudiante de serverX montada en **/home/student/work**.
- El archivo **/etc/fstab** incluye la entrada de montaje.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

```
[student@serverX ~]$ lab samba setup
```

- Restablezca su sistema desktopX.
- Inicie sesión en desktopX y abra una terminal.

Tiene un directorio de inicio en serverX que se utiliza para almacenar documentos relativos al trabajo. El directorio se comparte vía Samba para admitir todos los sistemas operativos de escritorio de la empresa.

El administrador de serverX ha confirmado que el nombre del recurso compartido es **student** y que los **uid/gid** son los mismos que los de su instancia desktopX; la contraseña compartida es *student*.

1. **Instale el paquete**
   Use **yum** para instalar **cifs-utils**.

   ```
   [student@desktopX ~]$ sudo yum -y install cifs-utils
   Loaded plugins: langpacks
   Resolving Dependencies
   ...
   Complete!
   ```

   Este paquete proporciona apoyo para montar sistemas de archivos CIFS y es usado por el comando **mount**.

2. **Crear el punto de montaje**
   Use **mkdir** para crear el punto de montaje del directorio **work**.

```
[student@desktopX ~]$ mkdir ~/work
```

3. **Crear el archivo de credenciales**
   3.1. Use **mkdir** para crear el directorio **secure**.

```
[student@desktopX ~]$ sudo mkdir /secure
```

   3.2. Use **vim** para crear el archivo de credenciales **student.smb** y complételo.

```
[student@desktopX ~]$ sudo vim /secure/student.smb
```

   Agregue las siguientes líneas:

```
username=student
password=student
domain=MYGROUP
```

   3.3. Use **chmod** para proteger el directorio **secure** y el archivo de credenciales **student.smb**.

```
[student@desktopX ~]$ sudo chmod 770 /secure
[student@desktopX ~]$ sudo chmod 600 /secure/student.smb
```

4. **Actualizar /etc/fstab y montarlo**
   4.1. Use **vim** para agregar la configuración de montaje al final de **/etc/fstab**.

```
[student@desktopX ~]$ sudo vim /etc/fstab
...
//serverX/student  /home/student/work  cifs  credentials=/secure/student.smb  0
 0
```

   4.2. Use **mount** para verificar la configuración y montar el sistema de archivos.

```
[student@desktopX ~]$ sudo mount -a
```

   Este comando no debe informar errores. Si lo hace, verifique su configuración en **/etc/fstab**.

5. **Verificar su acceso**
   5.1. Use **cat** para generar el archivo **samba.txt**.

```
[student@desktopX ~]$ cat ~/work/samba.txt
Success
```

   5.2. Use **echo** para escribir el punto de montaje **work**.

```
[student@desktopX ~]$ echo testing > ~/work/test.txt
```

Trabajo de laboratorio: Acceso a almacenamiento de red con SMB

En este trabajo de laboratorio, instalará paquetes para admitir el automontaje de recursos compartidos de CIFS y crear tres automontajes.

Recursos:	
Archivos:	**`samba.txt`** en cada directorio compartido, para pruebas.
Máquinas:	**`desktopX`** y **`serverX`**

Resultados:

- Instalación de al menos dos paquetes para admitir el automontaje de recursos compartidos de Samba.
- Automonte **`/shares/work`** con acceso **`RW`** autenticado a su directorio de inicio en serverX.
- Automonte **`/shares/docs`** con acceso **`RO`** de guest al recurso compartido **`public`**.
- Automonte **`/shares/cases`** con acceso **`RW`** autenticado al recurso compartido de equipo restringido **`bakerst`**.
- Disponible persistentemente luego de un *reinicio*.

Andes de comenzar

Si aún no lo ha hecho al inicio del ejercicio anterior:

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

```
[student@serverX ~]$ lab samba setup
```

Siempre realice este paso:

- Restablezca su sistema desktopX.
- Inicie sesión en desktopX y abra una terminal.

Su empresa ejecuta un servicio de Samba en serverX para proporcionar el intercambio de documentos tanto para clientes de Red Hat Enterprise Linux como de Microsoft Windows. El servidor contiene un directorio para que cada usuario almacene sus documentos personales, un directorio de solo lectura públicamente disponible para documentos comunes y varios directorios de equipo para alojar documentos de colaboración.

Es posible que deba llevar a cabo una administración de usuarios y grupos básica en desktopX para garantizar que **`student`** pueda acceder a archivos en todos los recursos compartidos.

A continuación, se proporcionan los detalles clave de serverX que necesitará:

- Nombre de usuario: **`student`**
- Contraseña: **`student`**
- Membresía de grupo: **`bakerst`**, **`GID=10221`**
- Dominio: **`MYGROUP`**
- Los recursos compartidos están habilitados y se pueden escribir.

  desktopX punto de montaje: **`/shares/work`**
- Hay un recurso compartido denominado **`public`** que solo requiere privilegios de guest para acceder.

  desktopX punto de montaje: **`/shares/docs`**
- Su equipo tiene un recurso compartido privado, que se puede escribir, denominado **`bakerst`** que solo es accesible para miembros del grupo **`bakerst`**.

  desktopX punto de montaje: **`/shares/cases`**

Cuando haya finalizado, reinicie su máquina **`desktopX`**, y luego ejecute el comando **`lab samba grade`** desde su máquina **`desktopX`** para verificar su trabajo.

1. Instale los dos paquetes necesarios para automontar un sistema de archivos CIFS.
2. Agregue un archivo de configuración **`auto.master.d`** que identifique el directorio base y el archivo de asignación asociado (use el nombre que desee para el archivo de configuración, pero debe finalizar con **`.autofs`**) y cree el archivo de asignación asociado (use el nombre que desee para el archivo de asignación), y asegúrese de que cada montaje tenga la autenticación adecuada. Según sea necesario, puede crear otros archivos de configuración para admitir la configuración de asignación de automontajes.
3. Asegúrese de que el nombre de usuario **`student`** tenga los UID y GID correctos para acceder a cada uno de los recursos compartidos (*Sugerencia*: **`bakerst`**). En caso de ser necesario, agregue los grupos nuevos que sean necesarios, modifique la membresía del grupo del estudiante, o realice ambas acciones.

   Nota: Si agrega un nuevo grupo a los grupos complementarios del estudiante, necesitará salir de la shell e iniciar una nueva shell, o usar **`newgrp`** ***`groupname`*** para cambiar al grupo agregado recientemente. Esto es necesario porque el entorno con el cual se inicia Bash no se actualiza con los nuevos detalles del estudiante.
4. Habilite e inicie el servicio de automontaje.
5. Compruebe que puede acceder a cada recurso compartido y escribir en los recursos compartidos para los cuales tiene privilegios de escritura: **`work`** y **`cases`**.

   Hay un archivo denominado **`samba.txt`** que contiene el mensaje "*Success*" (Correcto) en cada una de las ubicaciones de recursos compartidos. Use **`cat samba.txt`**.

   Use **`echo testing > my.txt`** para evaluar si puede escribir en un directorio.

6. Cuando haya finalizado, reinicie su máquina **desktopX**, y luego ejecute el comando **lab samba grade** desde su máquina **desktopX** para verificar su trabajo.

Solución

En este trabajo de laboratorio, instalará paquetes para admitir el automontaje de recursos compartidos de CIFS y crear tres automontajes.

Recursos:	
Archivos:	**samba.txt** en cada directorio compartido, para pruebas.
Máquinas:	**desktopX** y **serverX**

Resultados:

- Instalación de al menos dos paquetes para admitir el automontaje de recursos compartidos de Samba.
- Automonte **/shares/work** con acceso **RW** autenticado a su directorio de inicio en serverX.
- Automonte **/shares/docs** con acceso **RO** de guest al recurso compartido **public**.
- Automonte **/shares/cases** con acceso **RW** autenticado al recurso compartido de equipo restringido **bakerst**.
- Disponible persistentemente luego de un *reinicio*.

Andes de comenzar

Si aún no lo ha hecho al inicio del ejercicio anterior:

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

```
[student@serverX ~]$ lab samba setup
```

Siempre realice este paso:

- Restablezca su sistema desktopX.
- Inicie sesión en desktopX y abra una terminal.

Su empresa ejecuta un servicio de Samba en serverX para proporcionar el intercambio de documentos tanto para clientes de Red Hat Enterprise Linux como de Microsoft Windows. El servidor contiene un directorio para que cada usuario almacene sus documentos personales, un directorio de solo lectura públicamente disponible para documentos comunes y varios directorios de equipo para alojar documentos de colaboración.

Es posible que deba llevar a cabo una administración de usuarios y grupos básica en desktopX para garantizar que **student** pueda acceder a archivos en todos los recursos compartidos.

A continuación, se proporcionan los detalles clave de serverX que necesitará:

- Nombre de usuario: **student**
- Contraseña: **student**

- Membresía de grupo: **bakerst**, **GID=10221**
- Dominio: **MYGROUP**
- Los recursos compartidos están habilitados y se pueden escribir.

  desktopX punto de montaje: **/shares/work**
- Hay un recurso compartido denominado **public** que solo requiere privilegios de guest para acceder.

  desktopX punto de montaje: **/shares/docs**
- Su equipo tiene un recurso compartido privado, que se puede escribir, denominado **bakerst** que solo es accesible para miembros del grupo **bakerst**.

  desktopX punto de montaje: **/shares/cases**

Cuando haya finalizado, reinicie su máquina **desktopX**, y luego ejecute el comando **lab samba grade** desde su máquina **desktopX** para verificar su trabajo.

1. Instale los dos paquetes necesarios para automontar un sistema de archivos CIFS.

```
[student@desktopX ~]$ sudo yum -y install cifs-utils autofs
Loaded plugins: langpacks
Resolving Dependencies
...
Complete!
```

2. Agregue un archivo de configuración **auto.master.d** que identifique el directorio base y el archivo de asignación asociado (use el nombre que desee para el archivo de configuración, pero debe finalizar con **.autofs**) y cree el archivo de asignación asociado (use el nombre que desee para el archivo de asignación), y asegúrese de que cada montaje tenga la autenticación adecuada. Según sea necesario, puede crear otros archivos de configuración para admitir la configuración de asignación de automontajes.

   2.1. Use **vim** para crear y editar el archivo **/etc/auto.master.d/shares.autofs**.

```
[student@desktopX ~]$ sudo vim /etc/auto.master.d/shares.autofs
```

   Agregue la siguiente línea:

```
/shares  /etc/auto.shares
```

nota

Esta solución utiliza **shares.autofs** como el archivo de asignación maestra y **auto.shares** como el archivo de asignación, pero los nombres de archivos no son importantes.

   2.2. Use **vim** para crear el archivo de asignación **auto.shares**.

```
[student@desktopX ~]$ sudo vim /etc/auto.shares
```

Agregue las siguientes líneas:

```
work   -fstype=cifs,credentials=/etc/me.cred  ://serverX/student
docs   -fstype=cifs,guest                     ://serverX/public
cases  -fstype=cifs,credentials=/etc/me.cred  ://serverX/bakerst
```

nota

Una alternativa al archivo de credenciales (y los pasos mostrados aquí para crearlo y editarlo) sería sustituir la entrada **credentials=/etc/me.cred** en el archivo **auto.shares** con dos entradas, **username=student,password=student**, pero sería menos seguro.

2.3. Use **vim** para crear el archivo de credenciales.

```
[student@desktopX ~]$ sudo vim /etc/me.cred
```

Agregue las siguientes líneas:

```
username=student
password=student
domain=MYGROUP
```

2.4. Use **chmod** para proteger el archivo de credenciales.

```
[student@desktopX ~]$ sudo chmod 600 /etc/me.cred
```

nota

Este paso no es fundamental para este trabajo de laboratorio, pero se muestra para ofrecer una visión completa.

3. Asegúrese de que el nombre de usuario **student** tenga los UID y GID correctos para acceder a cada uno de los recursos compartidos (*Sugerencia*: **bakerst**). En caso de ser necesario, agregue los grupos nuevos que sean necesarios, modifique la membresía del grupo del estudiante, o realice ambas acciones.

   Nota: Si agrega un nuevo grupo a los grupos complementarios del estudiante, necesitará salir de la shell e iniciar una nueva shell, o usar **newgrp *groupname*** para cambiar al grupo agregado recientemente. Esto es necesario porque el entorno con el cual se inicia Bash no se actualiza con los nuevos detalles del estudiante.

   3.1. Use el comando **groups** para verificar las membresías del grupo actual correspondientes al usuario **student**.

```
[student@desktopX ~]$ groups
student
```

La cuenta **student** no pertenece al grupo **bakerst** (GID **10221**) y deberá agregarse.

3.2. Compruebe si el grupo **bakerst** existe en desktopX. Use **grep** para comprobar el archivo **/etc/group**.

```
[student@desktopX ~]$ grep -e bakerst -e 10221 /etc/group
```

El grupo **bakerst** tampoco existe; deberá agregarse primero.

3.3. Use **groupadd** para agregar el grupo **bakerst** con GID **10221**.

```
[student@desktopX ~]$ sudo groupadd -g 10221 bakerst
```

3.4. Use **usermod** para agregar el grupo **bakerst** a **student** como un grupo complementario.

```
[student@desktopX ~]$ sudo usermod -aG bakerst student
```

nota

Generalmente, este método no es la mejor solución para alinear valores de UID y GID, dado que hay opciones de montaje que pueden manejar esto. Sin embargo, es una solución adecuada para este trabajo de laboratorio, y usted practica algunas habilidades de administración de usuarios y grupos.

3.5. Use **newgrp** para cambiar a **bakerst**.

```
[student@desktopX ~]$ newgrp bakerst
```

4. Habilite e inicie el servicio de automontaje.

```
[student@desktopX ~]$ sudo systemctl enable autofs
ln -s '/usr/lib/systemd/system/autofs.service'  ...
[student@desktopX ~]$ sudo systemctl start autofs
```

5. Compruebe que puede acceder a cada recurso compartido y escribir en los recursos compartidos para los cuales tiene privilegios de escritura: **work** y **cases**.

Hay un archivo denominado **samba.txt** que contiene el mensaje "*Success*" (Correcto) en cada una de las ubicaciones de recursos compartidos. Use **cat samba.txt**.

Use **echo testing > my.txt** para evaluar si puede escribir en un directorio.

5.1. Compruebe que puede leer y escribir en **work**:

```
[student@desktopX ~]$ cd /shares/work
[student@desktopX work]$ cat samba.txt
Success
[student@desktopX work]$ echo testing > my.txt
```

5.2. Compruebe que puede leer, pero no escribir en **docs**:

```
[student@desktopX work]$ cd ../docs
[student@desktopX docs]$ cat samba.txt
Success
[student@desktopX docs]$ echo testing > my.txt
bash: my.txt: Permission denied
```

5.3. Compruebe que puede leer y escribir en **cases**:

```
[student@desktopX docs]$ cd ../cases
[student@desktopX cases]$ cat samba.txt
Success
[student@desktopX cases]$ echo testing > my.txt
```

6. Cuando haya finalizado, reinicie su máquina **desktopX**, y luego ejecute el comando **lab samba grade** desde su máquina **desktopX** para verificar su trabajo.

6.1.
```
[student@desktopX ~]$ sudo systemctl reboot
```

6.2.
```
[student@desktopX ~]$ lab samba grade
```

Resumen

Acceso a almacenamiento de red con SMB

- Identifique los detalles del recurso compartido; por ejemplo, **`smbclient -L // server`**.
- Cree un directorio de punto de montaje.
- Use **`mount`** o actualice **`/etc/fstab`** para montar el recurso compartido de SMB.
- Use **`umount`** para desmontar un recurso compartido.
- Use el servicio **`autofs`** para el automontaje, usando las mismas opciones de montaje que **`mount`**.
  - **`enable`**, para habilitar el servicio de modo que se inicie en el arranque.
  - **`start`**, para iniciar el servicio.
- Use **`-fstype=cifs`** coloque "**`:`**" delante de la URI.

redhat. TRAINING

CAPÍTULO 13

CONTROL Y SOLUCIÓN DE PROBLEMAS DEL PROCESO DE ARRANQUE DE RED HAT ENTERPRISE LINUX

Descripción general	
Meta	Solucionar problemas del proceso de arranque de Red Hat Enterprise Linux.
Objetivos	• Describir el proceso de arranque de Red Hat Enterprise Linux. • Reparar problemas de arranque comunes. • Reparar problemas de archivos en el arranque. • Reparar problemas del cargador de arranque.
Secciones	• Proceso de arranque de Red Hat Enterprise Linux (y práctica) • Reparación de problemas de arranque comunes (y práctica) • Reparación de problemas de sistemas de archivos en el arranque (y práctica) • Reparación de problemas del cargador de arranque (y práctica)
Trabajo de laboratorio	• Control y solución de problemas del proceso de arranque de Red Hat Enterprise Linux

El proceso de arranque de Red Hat Enterprise Linux

Objetivos

Luego de completar esta sección, los estudiantes deberían poder describir e influenciar el proceso de arranque de Red Hat Enterprise Linux.

El proceso de arranque de Red Hat Enterprise Linux 7

Los sistemas de computación modernos son combinaciones complejas de hardware y software. Desde un estado de apagado no definido hasta un sistema de ejecución con un prompt de inicio de sesión (gráfico), se requiere una gran cantidad de piezas de hardware y software que funcionen en conjunto. La siguiente lista proporciona una descripción general de alto nivel de las tareas de arranque de un sistema físico **x86_64** a Red Hat Enterprise Linux 7. La lista de máquinas virtuales **x86_64** es prácticamente la misma, pero algunos de los pasos específicos del hardware son manejados por el hipervisor en el software.

1. La máquina se enciende. El firmware del sistema (UEFI moderno o BIOS más antiguo) ejecuta una *prueba automática de encendido (Power On Self Test, POST),* y comienza a inicializar parte del hardware.

   Configurado mediante lo siguiente: Las pantallas de configuración de BIOS/UEFI del sistema, a las cuales se llega típicamente al presionar una determinada combinación de teclas (p. ej., **F2**) al principio del proceso de arranque.

2. El firmware del sistema busca un dispositivo de arranque, ya sea configurado en el firmware de arranque UEFI o al buscar un *registro de arranque maestro (Master Boot Record,* MBR) en todos los discos, en el orden configurado en el BIOS.

   Configurado mediante lo siguiente: Las pantallas de configuración de BIOS/UEFI del sistema, a las cuales se llega típicamente al presionar una determinada combinación de teclas (p. ej., **F2**) al principio del proceso de arranque.

3. El firmware del sistema lee un *cargador de arranque* desde el disco, luego pasa el control del sistema al cargador de arranque. En un sistema Red Hat Enterprise Linux 7, este será típicamente **grub2**.

   Configurado mediante lo siguiente: **grub2-install**

4. El cargador de arranque carga su configuración desde el disco, y presenta al usuario un menú de posibles configuraciones para arrancar.

   Configurado mediante lo siguiente: **/etc/grub.d/**, **/etc/default/grub** y (no manualmente) **/boot/grub2/grub.cfg**.

5. Luego de que el usuario haya hecho una elección (o se haya agotado el tiempo de espera automático), el cargador de arranque carga el kernel *y el initramfs configurados* desde el disco y los coloca en la memoria. Un **initramfs** es un archivo **gzip**-ed **cpio** que contiene módulos del kernel para todo el hardware necesario en el arranque,

scripts de inicio y más. En Red Hat Enterprise Linux 7, **initramfs** contiene un sistema totalmente utilizable por sí solo.

Configurado mediante lo siguiente: **/etc/dracut.conf**

6. El cargador de arranque pasa el control del sistema al kernel, y detalla todas las opciones especificadas en la línea de comandos del kernel en el cargador de arranque, y la ubicación del **initramfs** en la memoria.

   Configurado mediante lo siguiente: **/etc/grub.d/**, **/etc/default/grub** y (no manualmente) **/boot/grub2/grub.cfg**.

7. El kernel inicializa todo el hardware para el cual puede encontrar un controlador en el **initramfs**, y luego ejecuta **/sbin/init** desde **initramfs** como **PID 1**. En Red Hat Enterprise Linux 7, **initramfs** contiene una copia de trabajo de **systemd** como **/sbin/init**, al igual que un daemon de **udev**.

   Configurado mediante lo siguiente: parámetro de línea de comandos **init=**.

8. La instancia **systemd** desde **initramfs** ejecuta todas las unidades para el objetivo **initrd.target**. Esto incluye el montaje del sistema de archivos raíz real en **/sysroot**.

   Configurado mediante lo siguiente: **/etc/fstab**

9. El sistema de archivos raíz del kernel se cambia (articula) desde el sistema de archivos raíz de **initramfs** al sistema de archivos raíz del sistema que se montó anteriormente en **/sysroot**. Luego, vuelve a ejecutarse **systemd** usando la copia de **systemd** instalado en el sistema.

10. **systemd** busca un objetivo predeterminado, ya sea especificado desde la línea de comandos del kernel o configurado en el sistema, luego inicia (y detiene) unidades para cumplir con la configuración para ese objetivo, y resuelve dependencias entre unidades automáticamente. En su esencia, un objetivo **systemd** es un conjunto de unidades que debe activarse para alcanzar un estado de sistema deseado. Estos objetivos incluirán típicamente al menos una pantalla de inicio de sesión basado en texto o inicio de sesión gráfico que se generará.

    Configurado mediante lo siguiente: **/etc/systemd/system/default.target**, **/etc/systemd/system/**

Arrancar, reiniciar y apagar

Para apagar o reiniciar un sistema en ejecución desde la línea de comandos, los administradores pueden usar el comando **systemctl**.

systemctl poweroff detendrá todos los servicios en ejecución, desmontará todos los sistemas de archivos (o volverá a montarlos como solo lectura cuando no se puedan desmontar) y luego apagará el sistema.

systemctl reboot detendrá todos los servicios en ejecución, desmontará todos los sistemas de archivos y luego reiniciará el sistema.

Para facilitar la compatibilidad con sistemas anteriores, los comandos **poweroff** y **reboot** aún existen, pero en Red Hat Enterprise Linux 7 son enlaces simbólicos a la herramienta **systemctl**.

Importante

`systemctl halt` y **`halt`** también están disponibles para detener el sistema, pero a diferencia de sus equivalentes de **`poweroff`**, estos comandos *no* apagan el sistema, sino que lo llevan hasta un punto donde es seguro apagarlo manualmente.

Selección de un objetivo de systemd

Un objetivo de **`systemd`** es un conjunto de unidades de **`systemd`** que deben iniciarse para alcanzar un estado deseado. Los más importantes de estos objetivos están detallados en la siguiente tabla.

Objetivo	Propósito
`graphical.target`	El sistema admite varios usuarios, e inicios de sesión gráficos y basados en texto.
`multi-user.target`	El sistema admite varios usuarios y solo inicios de sesión basados en texto.
`rescue.target`	Prompt **`sulogin`**, inicialización del sistema básico finalizada.
`emergency.target`	Prompt **`sulogin`**, cambio de **`initramfs`** completo y raíz del sistema montado en **`/`** solo lectura.

Es posible que un objetivo sea parte de otro objetivo; por ejemplo, **`graphical.target`** incluye **`multi-user.target`**, que a su vez depende de **`basic.target`** y otros. Estas dependencias se pueden visualizar desde la línea de comandos con el siguiente comando:

```
[root@serverX ~]# systemctl list-dependencies graphical.target | grep target
```

Una descripción general de todos los objetivos disponibles se puede visualizar con:

```
[root@serverX ~]# systemctl list-units --type=target --all
```

Una descripción general de todos los objetivos instalados en el disco se puede visualizar con:

```
[root@serverX ~]# systemctl list-unit-files --type=target --all
```

Selección de un objetivo en el tiempo de ejecución

En un sistema en ejecución, los administradores pueden elegir cambiar a un objetivo diferente usando el comando **`systemctl isolate`**; por ejemplo:

```
[root@serverX ~]# systemctl isolate multi-user.target
```

Aislar un objetivo detendrá todos los servicios no requeridos por ese objetivo (y sus dependencias), e iniciará todos los servicios requeridos que aún no se hayan iniciado.

nota

No todos los objetivos se pueden aislar. Solo los objetivos que tienen establecido **AllowIsolate=yes** en sus archivos de unidad se pueden aislar; por ejemplo, el objetivo **graphical.target** se puede aislar, pero el objetivo **cryptsetup.target** no.

Configuración de un objetivo predeterminado
Cuando el sistema se inicia, y el control se pasa a **systemd** desde **initramfs**, **systemd** intentará activar el objetivo **default.target**. Normalmente, el objetivo **default.target** será un enlace simbólico (en **/etc/systemd/system/**) a **graphical.target** o **multi-user.target**.

En lugar de editar este enlace simbólico manualmente, la herramienta **systemctl** viene con dos comandos para administrar este enlace: **get-default** y **set-default**.

```
[root@serverX ~]# systemctl get-default
multi-user.target
[root@serverX ~]# systemctl set-default graphical.target
rm '/etc/systemd/system/default.target'
ln -s '/usr/lib/systemd/system/graphical.target' '/etc/systemd/system/default.target'
[root@serverX ~]# systemctl get-default
graphical.target
```

Selección de un objetivo diferente en el momento del arranque
Para seleccionar un objetivo diferente al momento del arranque, se puede agregar una opción especial a la línea de comandos del kernel desde el cargador de arranque: **systemd.unit=**.

Por ejemplo, para arrancar el sistema en una shell de rescate donde se pueden hacer cambios de configuración (casi) sin ningún servicio en ejecución, se puede agregar lo siguiente desde el menú del cargador de arranque interactivo antes del inicio:

```
systemd.unit=rescue.target
```

Este cambio de configuración solo afectará a un único arranque, lo que hace que sea una herramienta útil para la solución de problemas en el proceso de arranque.

Para usar este método de selección de un objetivo diferente, use el siguiente procedimiento para sistemas Red Hat Enterprise Linux 7:

1. (Re)inicie el sistema.
2. Interrumpa la cuenta regresiva del menú del cargador de arranque presionando cualquier tecla.
3. Mueva el cursor hasta la entrada que debe iniciarse.
4. Presione **e** para editar la entrada actual.
5. Mueva el cursor hasta la línea que comienza con **linux16**. Esta es la línea de comandos del kernel.

6. Agregue **`systemd.unit=`*`desired.target`***.

7. Presione **`Ctrl`**+**`x`** para realizar el arranque con estos cambios.

Referencias

Páginas del manual: **`bootup`**(7), **`dracut.bootup`**(7), **`systemd.target`**(5), **`systemd.special`**(7), **`sulogin`**(8) y **`systemctl`**(1).

`info grub2` (*Manual GNU GRUB*)

Práctica: Selección de un objetivo de arranque

En este trabajo de laboratorio, configurará su sistema **serverX** para arrancar en diferentes objetivos.

Recursos:	
Máquinas:	**serverX**

Resultados:
Un sistema arrancado en diferentes destinos.

Andes de comenzar
- Restablezca su sistema **serverX**.

1. En su sistema **serverX**, cambie al objetivo **multi-user** manualmente sin reiniciar.

   1.1.
   ```
   [student@serverX ~]$ sudo systemctl isolate multi-user.target
   ```

2. Inicie sesión en una consola basada en texto como **raíz**.

3. Configure su **serverX** para que arranque automáticamente en el objetivo **multi-user** después de un nuevo arranque; luego reinicie su sistema **serverX** para verificar.

   3.1.
   ```
   [root@serverX ~]# systemctl set-default multi-user.target
   rm '/etc/systemd/system/default.target'
   ln -s '/usr/lib/systemd/system/multi-user.target' '/etc/systemd/system/
   default.target'
   ```

   3.2.
   ```
   [root@serverX ~]# systemctl reboot
   ```

4. Reinicie su sistema **serverX**, luego, desde el menú del cargador de arranque, arranque en el objetivo **rescue**.

   4.1. Reinicie su máquina **serverX**.

   ```
   [root@serverX ~]# systemctl reboot
   ```

   4.2. Presione cualquier tecla para interrumpir el cargador de arranque cuando aparezca el menú.

   4.3. Mueva la selección a la entrada predeterminada (la primera) usando las teclas de dirección.

   4.4. Presione **e** para editar la entrada actual.

   4.5. Mueva el cursor hasta la línea que comienza con **linux16**.

4.6. Mueva el cursor hasta el final de la línea (usando la tecla **End** (Fin)), y agregue el siguiente texto:

```
systemd.unit=rescue.target
```

4.7. Presione **Ctrl**+**x** para realizar el arranque con la configuración modificada.

4.8. Cuando se le solicite la contraseña **raíz**, ingrese **redhat**.

5. Configure el objetivo **systemd** predeterminado nuevamente al objetivo gráfico.

```
[root@serverX ~]# systemctl set-default graphical.target
```

6. Presione **Ctrl**+**d** para continuar arrancando en el objetivo predeterminado (nuevo).

Reparación de problemas de arranque comunes

Objetivos

Luego de completar esta sección, los estudiantes deberían poder reparar problemas de arranque comunes.

Recuperación de la contraseña raíz

Una tarea que todos los administradores de sistemas deben poder realizar es recuperar una contraseña **raíz** perdida. Si el administrador aún tiene la sesión iniciada, ya sea como usuario sin privilegios, pero con acceso **sudo** completo, o como **raíz**, esta tarea es sencilla. Cuando el administrador no ha iniciado sesión, esta tarea es un poco más complicada.

Existen varios métodos para establecer una nueva contraseña **raíz**. Un administrador de sistemas podría, por ejemplo, arrancar el sistema usando un CD Live, montar el sistema de archivos raíz desde allí y editar **/etc/shadow**. En esta sección, exploraremos un método que no requiere el uso de medios externos.

nota

En Red Hat Enterprise Linux 6 y versiones anteriores, un administrador podía arrancar el sistema en *nivel de ejecución 1,*y se le presentaba un prompt raíz. Los análogos más cercanos al nivel de ejecución 1 en una máquina Red Hat Enterprise Linux 7 son los objetivos **rescue.target** y **emergency.target**, ambos requieren la contraseña **raíz** para iniciar sesión.

En Red Hat Enterprise Linux 7, es posible tener scripts que se ejecuten desde la pausa de **initramfs** en ciertos puntos, proporcionar una **root** shell y luego continuar cuando esa shell se cierre. Si bien esto se realiza principalmente para depuraciones, también se puede usar para recuperar una contraseña de root perdida:

1. Reinicie el sistema.
2. Interrumpa la cuenta regresiva del cargador de arranque presionando cualquier tecla.
3. Mueva el cursor a la entrada que debe arrancarse.
4. Presione **e** para editar la entrada seleccionada.
5. Mueva el cursor hasta la línea de comandos del kernel (la línea que empieza con **linux16**).
6. Agregue **rd.break** (esto hará que se produzca un quiebre antes de que el control se entregue de **initramfs** al sistema real).

nota

La solicitud de **initramfs** se mostrará en todas las consolas que se especifiquen *últimas* en la línea de comandos del kernel.

7. Presione **Ctrl**+**x** para realizar el arranque con los cambios.

nota

Es posible que las imágenes creadas previamente coloquen múltiples argumentos de consola en el kernel para respaldar una amplia variedad de situaciones de implementación. La advertencia con rd.break es que mientras muchos de los mensajes del kernel se enviarán a todas las consolas, el prompt usará en última instancia la última consola. Si no recibe el prompt, se recomienda que vuelva a ordenar temporalmente los argumentos de la consola=.

En este punto, se presentará una **root** shell, con el sistema de archivos raíz para el sistema real montado para solo lectura en **/sysroot**.

Importante

SELinux aún no está habilitado en este punto, de modo que cualquier archivo nuevo que se cree no tendrá un contexto de SELinux asignado. Tenga en cuenta que algunas herramientas (como **passwd**) primero crean un archivo nuevo, y luego lo trasladan al lugar del archivo que intentan editar; y se crea así de manera efectiva un nuevo archivo sin un contexto SELinux.

Para recuperar la contraseña **raíz** desde este punto, realice el siguiente procedimiento:

1. Vuelva a montar **/sysroot** como lectura-escritura.

```
switch_root:/# mount -o remount,rw /sysroot
```

2. Cambie a jail **chroot**, donde **/sysroot** se trata como la raíz de un árbol de sistemas de archivos.

```
switch_root:/# chroot /sysroot
```

3. Establezca una nueva contraseña raíz:

```
sh-4.2# passwd root
```

4. Asegúrese de que todos los archivos no etiquetados (incluido **/etc/shadow** en este punto) obtengan una nueva etiqueta durante el arranque.

```
sh-4.2# touch /.autorelabel
```

5. Ingrese **exit** dos veces. El primero saldrá del jail de **chroot** y el segundo saldrá de la shell de depuración de **initramfs**.

En este punto, el sistema continuará con el arranque, realizará un nuevo etiquetado de SELinux completo, y luego realizará el arranque nuevamente.

Uso de journalctl

Puede ser útil mirar los registros de arranques anteriores (que fallaron). Si el registro de **journald** se ha hecho persistente, esto se puede hacer con la herramienta **journalctl**.

Primero asegúrese de tener habilitado el registro de **journald** persistente:

```
[root@serverX ~]# mkdir -p -m2755 /var/log/journal
[root@serverX ~]# chown :systemd-journal /var/log/journal
[root@serverX ~]# killall -USR1 systemd-journald
```

Para inspeccionar los archivos de registro para un arranque anterior, use la opción **-b** para **journalctl**. Sin argumentos, la opción **-b** filtrará el resultado solo con mensajes que pertenecen a este arranque, pero con un número negativo como argumento, filtrará arranques anteriores. Por ejemplo:

```
[root@serverX ~]# journalctl -b-1 -p err
```

Este comando mostrará todos los mensajes calificados como error o peor del arranque anterior.

Diagnosticar y reparar problemas de arranque de systemd

Si hay problemas durante el inicio de servicios, existe un par de herramientas disponibles para los administradores de sistemas que pueden ayudar con la depuración o la resolución de problemas:

Shell de depuración temprana
Al ejecutar **systemctl enable debug-shell.service**, una **root** shell se iniciará en **TTY9** (**Ctrl**+**Alt**+**F9**) al principio de la secuencia de arranque. Este shell inicia sesión automáticamente como raíz, de modo que un administrador puede usar alguna de las otras herramientas de depuración mientras el sistema aún está arrancando.

Advertencia

No olvide deshabilitar el servicio **debug-shell.service** cuando haya finalizado la depuración, dado que deja una shell raíz no autenticada abierta a cualquier usuario con acceso a la consola local.

Objetivos de emergencia y recuperación
Al agregar **`systemd.unit=rescue.target`** o **`systemd.unit=emergency.target`** delante de la línea de comandos del kernel desde el cargador de arranque, el sistema iniciará una shell de emergencia o recuperación especial en lugar de iniciarse normalmente. Estas dos shells requieren la contraseña **`raíz`**. El objetivo de **`emergencia`** mantiene el sistema de archivos raíz montado con solo lectura; mientras que **`rescue.target`** espera que **`sysinit.target`** se complete primero para que una mayor parte del sistema se inicie (p. ej., registros, sistemas de archivos, etc.).

Estas shells se pueden usar para arreglar problemas que impiden que el sistema arranque normalmente; por ejemplo, un bucle de dependencia entre servicios o una entrada incorrecta en **`/etc/fstab`**. Cuando se sale de estas shells, continúa el proceso de arranque regular.

Trabajos atascados
Durante el inicio, **`systemd`** inicia varios trabajos. Si alguno de estos trabajos no se puede completar, impedirán que otros trabajos se ejecuten. Para inspeccionar la lista de trabajos actual, un administrador puede usar el comando **`systemctl list-jobs`**. Todos los trabajos detallados como **`en ejecución`** deben completarse para que los trabajos detallados como **`en espera`** puedan continuar.

Referencias

Páginas del manual: **`dracut.cmdline`**(7), **`systemd-journald`**(8), **`journalctl`**(1), **`sushell`**(8) y **`systemctl`**(1)

`/usr/lib/systemd/system/debug-shell.service`

Práctica: restablecimiento de una contraseña raíz perdida

En este trabajo de laboratorio, recuperará una contraseña raíz perdida.

Recursos:	
Máquinas:	**serverX**

Resultados:
Contraseña raíz recuperada.

Andes de comenzar
- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo:

```
[student@serverX ~]$ lab rootpw setup
```

El script **lab rootpw setup** acaba de restablecer su contraseña raíz a una secuencia de comandos aleatoria y reinició el sistema. Sin usar **sudo**, entre en su propio sistema y restablezca la contraseña **raíz** nuevamente a **redhat**.

1. Vuelva a arrancar su sistema e interrumpa la cuenta regresiva en el menú del cargador de arranque.

   1.1. Envíe **Ctrl**+**Alt**+**Del** a su sistema usando la entrada del menú o el botón relevantes.

   1.2. Cuando el menú del cargador de arranque aparece, presione cualquier tecla para interrumpir la cuenta regresiva.

2. Edite la entrada del cargador de arranque predeterminada (en la memoria) para anular el proceso de arranque luego de que todos los sistemas de archivos hayan sido montados, pero antes de que el control se entregue a **systemd**, luego arranque.

   2.1. Use las teclas de dirección para destacar la entrada del cargador de arranque predeterminada.

   2.2. Presione **e** para editar la entrada actual.

   2.3. Con las teclas de dirección, navegue hacia la línea que comienza con **linux16**.

   2.4. Presione **End** (Fin) para mover el cursor hasta el final de la línea.

   2.5. Agregue **rd.break** en el final de la línea.

   2.6. Presione **Ctrl**+**x** para realizar el arranque con la configuración modificada.

3. En el prompt **switch_root**, vuelva a montar la lectura-escritura de systemd del archivo **/sysroot** y, luego, use **chroot** para ir a un jail **chroot** en **/sysroot**.

   3.1.
```
switch_root:/# mount -o remount,rw /sysroot
```

```
switch_root:/# chroot /sysroot
```

4. Cambie la contraseña **raíz** nuevamente a **redhat**.

4.1.
```
sh-4.2# echo redhat | passwd --stdin root
```

5. Configure el sistema para que realice automáticamente un etiquetado nuevo de SELinux completo luego del arranque. Esto es necesario dado que la herramienta **passwd** recreó el archivo **/etc/shadow** sin un contexto SELinux.

5.1.
```
sh-4.2# touch /.autorelabel
```

6. Escriba **exit** dos veces para continuar arrancando su sistema de forma normal. El sistema ejecutará un nuevo etiquetado SELinux, luego volverá a arrancar nuevamente por sí solo.

7. Verifique su trabajo al ejecutar el siguiente comando:

```
[student@serverX ~]$ lab rootpw grade
```

Reparación de problemas de archivos en el arranque

Objetivos

Luego de completar esta sección, los estudiantes deberían poder reparar problemas de sistemas de archivos durante el arranque.

Los errores en sistemas de archivos dañados y en **/etc/fstab** pueden impedir que un sistema arranque. En la mayoría de los casos, **systemd** continuará con el arranque luego de un tiempo de espera, o caerá en una shell de reparación de emergencia que requiere la contraseña **raíz**.

En la siguiente tabla, se detallan algunos errores comunes y sus resultados.

Problema	Resultado
Sistema de archivos dañado	**systemd** intentará un **fsck**. Si el problema es demasiado grave para un arreglo automático, se le solicitará al usuario que ejecute **fsck** manualmente desde una shell de emergencia.
Dispositivo no existente/ UUID mencionado en **/etc/fstab**	**systemd** esperará un tiempo establecido a que el dispositivo esté disponible. Si el dispositivo no aparece como disponible, el usuario cae en una shell de emergencia luego del tiempo de espera.
Punto de montaje no existente en **/etc/fstab**	**systemd** crea el punto de montaje si es posible; de lo contrario, cae en una shell de emergencia.
Opción de montaje incorrecta especificada en **/etc/fstab**	El usuario cae en una shell de emergencia.

En todos los casos, un administrador también puede utilizar el objetivo **emergency.target** para diagnosticar y arreglar el problema, dado que ningún sistema de archivos se montará antes de que se muestre la shell de emergencia.

nota

Al usar la shell de recuperación automática durante problemas de sistemas de archivos, no olvide emitir un **systemctl daemon-reload** luego de editar **/etc/fstab**. Sin esta recarga, **systemd** continuará usando la versión anterior.

Referencias

Páginas del manual: **systemd-fsck**(8), **systemd-fstab-generator**(3), **systemd.mount**(5)

Práctica: Reparación de problemas en el arranque

En este trabajo de laboratorio, recuperará el sistema de un error en **/etc/fstab**.

Recursos:	
Máquinas:	**serverX**

Resultados:
Luego de completar este ejercicio, su máquina debería arrancar nuevamente de forma normal, sin intervención del usuario.

Andes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo:

```
[student@serverX ~]$ lab bootbreakfs setup
```

Usted *tenía* un nuevo administrador en su equipo, pero se decidió que sería mejor para todos si ese administrador buscara otra profesión.

Ahora que el problema de su personal ha sido resuelto, hay un par de problemas restantes. Uno de ellos es una máquina que ha sido "arreglada" por este administrador.

1. Mire bien la consola de su máquina **serverX**. Parece que se atascó antes.

   Tómese un minuto para especular sobre una posible causa de este comportamiento, luego vuelva a arrancar la máquina e interrumpa la cuenta regresiva del menú del cargador de arranque. (Si espera el tiempo suficiente, el sistema finalmente iniciará una shell de rescate por sí solo, pero eso puede tardar un tiempo).

   1.1. Generalmente, enviaría **Ctrl**+**Alt**+**Del** a su sistema para que se reinicie. Este problema de arranque particular hace que esa secuencia de teclas reintente la secuencia de arranque nuevamente sin reiniciarse. En este caso, espere a que la tarea termine o use el interruptor de encendido para forzar un reinicio.

   1.2. Cuando el menú del cargador de arranque aparezca luego de la prueba automática del BIOS, presione cualquier tecla para interrumpir la cuenta regresiva.

2. Si observa el error que tuvo durante el arranque anterior, parece que al menos ciertas partes del sistema aún están funcionando. Dado que sabe la contraseña **raíz** (**redhat**), intente un arranque de **emergencia**.

   2.1. Use las teclas de dirección para destacar la entrada del cargador de arranque predeterminada.

   2.2. Presione **e** para editar la entrada actual.

   2.3. Con las teclas de dirección, navegue hacia la línea que comienza con **linux16**.

2.4. Presione **End** (Fin) para mover el cursor hasta el final de la línea.

2.5. Agregue **systemd.unit=emergency.target** en el final de la línea.

2.6. Presione **Ctrl**+**x** para realizar el arranque con la configuración modificada.

3. Inicie sesión en el modo de emergencia. Preste atención a los errores que pueda recibir.

3.1. En el prompt **Give root password for maintenance** (Proporcione la contraseña raíz para mantenimiento), ingrese **redhat**.

4. Inspeccione qué sistemas de archivos se montan actualmente.

4.1.
```
[root@localhost ~]# mount
...
/dev/vda1 on / type xfs (ro,relatime,seclabel,attr2,inode64,noquota)
```

5. Parece que el sistema de archivos raíz está montado como solo lectura; móntelo como lectura-escritura.

5.1.
```
[root@localhost ~]# mount -o remount,rw /
```

6. Intente montar todos los demás sistemas de archivos:

6.1.
```
[root@localhost ~]# mount -a
mount: mount point /RemoveMe does not exist
```

7. Abra **/etc/fstab** en un editor y arregle el problema.

7.1.
```
[root@localhost ~]# vi /etc/fstab
```

7.2. Elimine la línea no válida (la que tiene **RemoveMe**).

7.3. Guarde los cambios, luego salga del editor.

8. Intente montar todas las entradas para verificar que su **/etc/fstab** ahora sea correcto.

8.1.
```
[root@localhost ~]# mount -a
```

9. Salga de su shell de **emergencia** y reinicie el sistema; para ello, escriba **reboot**. Ahora su sistema debería arrancar normalmente.

Reparación de problemas del cargador de arranque

Objetivos

Luego de completar esta sección, los estudiantes deberían poder reparar problemas del cargador de arranque.

El cargador de arranque utilizado de forma predeterminada en Red Hat Enterprise Linux 7 es **grub2**, la segunda versión importante del *Gran gestor de arranque unificado*.

grub2 se puede usar para arrancar tanto en sistemas BIOS como UEFI, y admite el arranque de casi cualquier sistema de operaciones que se ejecute en hardware moderno.

El archivo de configuración principal de **grub2** es **/boot/grub2/grub.cfg**, pero se supone que los administradores no editan este archivo directamente. En cambio, se utiliza una herramienta denominada **grub2-mkconfig** para generar esa configuración usando un conjunto de archivos de configuración diferente, y la lista de kernels instalados.

grub2-mkconfig observará a **/etc/default/grub** en busca de opciones, como el tiempo de espera del menú predeterminado y la línea de comandos del kernel que se usará, y luego usa un conjunto de scripts en **/etc/grub.d/** para generar un archivo de configuración.

Para hacer cambios permanentes en la configuración del cargador de arranque, un administrador debe editar los archivos de configuración detallados anteriormente, y luego ejecutar el siguiente comando:

```
[root@serverX ~]# grub2-mkconfig > /boot/grub2/grub.cfg
```

En aquellos casos en los que se hayan hecho cambios importantes, se recomienda que el administrador ejecute ese comando sin la redirección, de modo que los resultados se puedan inspeccionar primero.

Directivas importantes

Para resolver una configuración de **grub2** rota, un administrador primero deberá comprender la sintaxis de **/boot/grub2/grub.cfg**. Las entradas reales que se pueden utilizar para el arranque están codificadas dentro de bloques de **menuentry**. En estos bloques, las líneas **linux16** y **initrd16** apuntan al kernel que se cargará desde el disco (junto con la línea de comandos del kernel) y a las **initramfs** que se cargarán. Durante la edición interactiva en el arranque, la finalización de la **pestaña** está disponible para encontrar estos archivos.

Las líneas de **set root** dentro de esos bloques no apuntan al sistema de archivos raíz para el sistema Red Hat Enterprise Linux 7; en cambio, apuntan al sistema de archivos desde el cual **grub2** debería cargar los archivos de initramfs y el kernel. La sintaxis es ***harddrive, partition***, donde **hd0** es el primer disco duro en el sistema, **hd1** es el segundo, etc. Las particiones se indican como **msdos1** para la primera partición de MBR, o **gpt1** para la primera partición de GPT en esa unidad.

Reinstalación del cargador de arranque

En aquellos casos donde el mismo cargador de arranque se ha dañado, se puede volver a instalar usando el comando **grub2-install**. En sistemas BIOS, el disco donde **grub2** debe

instalarse en el MBR debe proporcionarse como un argumento. En sistemas UEFI, no es necesario ningún argumento cuando la partición del sistema EFI se monta en **`/boot/efi`**.

Referencias

`info grub2` (*Manual GNU GRUB*)

`info grub2-install` (*Manual GNU GRUB*)
- Capítulo 28: "Cómo invocar **`grub2-install`**"

Práctica: Reparación de un problema del cargador de arranque

En este trabajo de laboratorio, reparará un problema con la configuración del cargador de arranque en una de sus máquinas.

Recursos:	
Máquinas:	**serverX**

Resultados:
Una máquina que arranca normalmente sin la intervención del usuario.

Andes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo:

```
[student@serverX ~]$ lab bootbreakgrub setup
```

Uno de sus *anteriores* compañeros de trabajo estaba experimentando con la aceleración del proceso de arranque en una de sus máquinas. Luego de varios intentos fallidos, se le ha asignado a usted la tarea de reparar el daño provocado.

1. Observe la consola de su máquina **serverX**, luego reiníciela e interrumpa el reloj de la cuenta regresiva del cargador de arranque.

   1.1. Envíe **Ctrl**+**Alt**+**Del** a su sistema usando la entrada del menú o el botón relevantes.

   1.2. Cuando el menú del cargador de arranque aparezca, presione cualquier tecla para interrumpir la cuenta regresiva.

2. Mueva el cursor hasta la entrada de arranque predeterminada, luego presione **e** para editar esa entrada. Inspeccione la configuración detenidamente, en busca de cualquier cosa que parezca fuera de lo común.

3. Encuentre la línea que bloquea el proceso de arranque, modifíquela, y luego arranque con esos cambios.

   3.1. **os16** no es una directiva **grub** válida. Cámbiela a **linux16**.

   3.2. Presione **Ctrl**+**x** para arrancar el sistema con la configuración modificada.

4. Espere a que el sistema arranque, inicie sesión como **student**, eleve sus privilegios a **raíz**, y luego genere una nueva configuración de **grub2**. No sobrescriba inmediatamente la configuración existente; inspeccione la nueva configuración primero.

   4.1.
   ```
   [student@serverX ~]$ sudo -i
   [root@serverX ~]# grub2-mkconfig
   ```

   4.2. Desplácese por el resultado para ver si parece una configuración de **grub2** válida.

4.3. Grabe la configuración a disco.

```
[root@serverX ~]# grub2-mkconfig > /boot/grub2/grub.cfg
```

5. Vuelva a arrancar la máquina y compruebe si arranca normalmente de nuevo sin la intervención del usuario.

5.1.

```
[root@serverX ~]# systemctl reboot
```

Prueba del capítulo: Control y solución de problemas del proceso de arranque Red Hat Enterprise Linux

Los siguientes pasos se realizan durante el proceso de arranque de un sistema Red Hat Enterprise Linux 7. Reordénelos de modo que indiquen el orden en que ocurren.

__ a. El kernel e initramfs se cargan desde el disco.

__ b. Todas las unidades para el objetivo **`predeterminado`** están iniciadas.

__ c. El cargador de arranque presenta un menú al usuario.

__ d. El kernel inicializa e inicia **`/sbin/init`** desde initramfs.

__ e. El firmware del sistema carga el cargador de arranque.

__ f. El sistema de archivos raíz del sistema se monta como solo lectura en **`/sysroot`**.

__ g. Se produce la inicialización del hardware básico.

__ h. El sistema de archivos raíz se cambia, y el control se pasa a una nueva instancia de **`systemd`**.

__ i. El cargador de arranque carga su configuración desde el disco.

Solución

Los siguientes pasos se realizan durante el proceso de arranque de un sistema Red Hat Enterprise Linux 7. Reordénelos de modo que indiquen el orden en que ocurren.

4 a. El kernel e initramfs se cargan desde el disco.

9 b. Todas las unidades para el objetivo **`predeterminado`** están iniciadas.

3 c. El cargador de arranque presenta un menú al usuario.

5 d. El kernel inicializa e inicia **`/sbin/init`** desde initramfs.

1 e. El firmware del sistema carga el cargador de arranque.

7 f. El sistema de archivos raíz del sistema se monta como solo lectura en **`/sysroot`**.

6 g. Se produce la inicialización del hardware básico.

8 h. El sistema de archivos raíz se cambia, y el control se pasa a una nueva instancia de **`systemd`**.

2 i. El cargador de arranque carga su configuración desde el disco.

Resumen

El proceso de arranque de Red Hat Enterprise Linux

- El proceso de arranque de Red Hat Enterprise Linux 7 se puede dividir en cuatro pasos:
  1. Hardware (BIOS/UEFI)
  2. Cargador de arranque (**grub2**)
  3. **kernel** e **initramfs**
  4. **systemd**
- **systemctl reboot** y **systemctl poweroff** reinician y apagan el sistema, respectivamente.
- **systemctl isolate *desired.target*** cambia a un nuevo objetivo en tiempo de ejecución.
- **systemctl get-default** y **systemctl set-default** se pueden usar para consultar y establecer el objetivo predeterminado.
- **systemd.unit=** en la línea de comandos del kernel selecciona un objetivo diferente en el arranque.

Reparación de problemas de arranque comunes

- Use **rd.break** en la línea de comandos del kernel para interrumpir el proceso de arranque antes de que se entregue el control desde el **initramfs**. El sistema se montará (solo lectura) bajo **/sysroot**.
- Se puede usar **journalctl** para filtrar para arranques específicos con la opción **-b**.
- El servicio **debug-shell.service** se puede utilizar para obtener una **root** shell automática durante el arranque.

Reparación de problemas de archivos en el arranque

- **systemd** mostrará una shell de emergencia en la mayoría de los casos en que lidie con problemas de sistemas de archivo.
- El objetivo **emergency.target** también puede utilizarse para diagnosticar y arreglar problemas de sistemas de archivos.

Reparación de problemas del cargador de arranque

- Use **e** y **Ctrl**+**x** para editar las entradas del cargador de arranque en la memoria, y luego realice el arranque.
- Use **grub2-mkconfig > /boot/grub2/grub.cfg** para volver a generar la configuración del cargador de arranque.
- **grub2-install** se utiliza para reinstalar el cargador de arranque.

redhat. TRAINING

CAPÍTULO 14

LIMITACIÓN DE LA COMUNICACIÓN DE RED CON FIREWALLD

Descripción general	
Meta	Configurar un firewall básico.
Objetivos	• Configurar un firewall básico usando `firewalld`, `firewall-config` y `firewall-cmd`.
Secciones	• Limitación de la comunicación de red (y práctica)
Trabajo de laboratorio	• Limitación de la comunicación de red con firewalld

Limitación de la comunicación de red

Objetivos

Luego de completar esta sección, los estudiantes deberían poder configurar un firewall básico.

Conceptos netfilter y firewalld

El kernel Linux incluye un potente subsistema de filtrado de red, **netfilter**. El subsistema **netfilter** permite a los módulos del kernel inspeccionar cada paquete que atraviese el sistema. Esto significa que cualquier paquete de red entrante, saliente o que se reenvíe se puede inspeccionar, modificar, soltar o rechazar de una manera programática, antes de llegar a los componentes en el espacio del usuario. Este es el principal componente para crear un firewall en una máquina Red Hat Enterprise Linux 7.

Interacción con netfilter

Si bien es teóricamente posible para los administradores del sistema escribir sus propios módulos del kernel para interactuar con **netfilter**, esto típicamente no sucede. En cambio, se usan otros programas para interactuar con **netfilter**. Uno de los más comunes y conocidos de estos programas es **`iptables`**. En versiones anteriores de Red Hat Enterprise Linux, **`iptables`** fue el principal método de interacción con el subsistema de **netfilter** del kernel.

El comando **`iptables`** es una herramienta de bajo nivel, y administrar correctamente los firewall con esta herramienta puede presentar un desafío. Además, solo se ajusta a las reglas de firewall IPv4. Para una cobertura de firewall más completa, se deben usar otras utilidades, como **`ip6tables`** para IPv6 y **`ebtables`**.

Presentación de firewalld

En Red Hat Enterprise Linux 7, se ha presentado un nuevo método de interacción con **netfilter**: **`firewalld`**. **`firewalld`** es un daemon del sistema que puede configurar y supervisar las reglas del firewall del sistema. Las aplicaciones pueden hablar con **`firewalld`** para solicitar que se abran puertos usando el sistema de mensajería **DBus**, una función que se puede desactivar o bloquear. Cubre tanto IPv4 como IPv6, y potencialmente la configuración **`ebtables`**. El daemon **`firewalld`** se instala desde el paquete *firewalld*. Este paquete es parte de una instalación **`base`**, pero no parte de una instalación **`minimal`**.

`firewalld` simplifica la administración de firewall al clasificar todo el tráfico de la red en *zonas*. En función de los criterios como la dirección IP de la fuente de un paquete o la interfaz de red entrante, el tráfico luego se desvía a las reglas de firewall para la zona adecuada. Cada zona tiene su propia lista de puertos y servicios para abrir o cerrar.

nota

En el caso de equipos portátiles u otras máquinas que cambian regularmente las redes, **NetworkManager** se puede usar para configurar automáticamente la zona de firewall para una conexión. Las zonas se pueden personalizar con reglas adecuadas para conexiones particulares.

Esto es especialmente útil en el traslado entre el *hogar*, el *trabajo* y las redes inalámbricas *públicas*. Un usuario podría desear llegar al servicio **sshd** de su sistema cuando se conecta a las redes de su hogar y corporativas, pero no cuando se conecta a la red inalámbrica pública en la tienda de café local.

Cada paquete que viene en el sistema se revisará primero para determinar la *dirección de origen*. Si esa dirección de origen está conectada a una zona específica, las reglas de esa zona se analizarán. Si la dirección de origen no está conectada a una zona, se usará la zona de la interfaz de red *entrante*.

Si la interfaz de red no está asociada con una zona por algún motivo, se usará la zona *predeterminada*. La zona predeterminada no es una zona por separado en sí; es una de las otras zonas. De forma predeterminada, se usa la zona **public** (pública), pero el administrador del sistema puede cambiarla.

La mayoría de las zonas permitirá el tráfico a través del firewall que relaciona una lista de puertos y protocolos ("631/udp") o servicios predefinidos ("ssh"). Si el tráfico no relaciona un puerto/protocolo o servicio permitidos, generalmente será rechazado. (La zona trusted [de confianza], que permite todo el tráfico de forma predeterminada, es una excepción a esto).

Zonas predefinidas

firewalld incluye un número de zonas predefinidas, aptas para varios propósitos. La zona predeterminada está configurada en *public* y las interfaces se asignan a *public* si no se hacen cambios. La interfaz **lo** se trata como si estuviera en la zona *trusted* (de confianza). En la siguiente tabla, se detalla la configuración de estas zonas en la instalación, pero el administrador del sistema puede luego personalizar estas zonas para que tengan diferentes configuraciones. De forma predeterminada, todas las zonas permiten todo el tráfico entrante que sea parte de una comunicación iniciada por el sistema y todo el tráfico saliente.

Configuración predeterminada de zonas `firewalld`

Nombre de la zona	Configuración predeterminada
trusted (de confianza)	Permite todo el tráfico entrante.
inicio	Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos **ssh**, **mdns**, **ipp-client**, **samba-client** o **dhcpv6-client**.
internal (interna)	Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos s**sh**, **mdns**, **ipp-client**, **samba-client**, or **dhcpv6-client** (lo mismo que la zona **home** para empezar).
work (trabajo)	Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos **ssh**, **ipp-client** o **dhcpv6-client**.

Nombre de la zona	Configuración predeterminada
public (pública)	Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos **ssh** o **dhcpv6-client**. *Zona predeterminada para interfaces de red recientemente agregadas.*
external (externa)	Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione el servicio predefinido **ssh**. El tráfico IPv4 saliente reenviado a través de esta zona *se enmascara* para que luzca como que se originó desde la dirección IPv4 de la interfaz de red saliente.
dmz	Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione el servicio predefinido **ssh**.
block (bloqueo)	Rechaza todo el tráfico entrante, a menos que esté relacionado con tráfico saliente.
drop (caída)	Deja caer todo el tráfico entrante a menos que esté relacionado con tráfico saliente (ni siquiera responde con errores ICMP).

Para conocer una lista de todas las zonas predefinidas y sus usos previstos, consulte la página del manual **firewalld.zones**(5).

Servicios predefinidos

firewalld también incluye un número de servicios predefinidos. Estas definiciones de servicios se pueden usar para permitir fácilmente que el tráfico de servicios de red particulares pase a través del firewall. En la siguiente tabla, se detalla la configuración de los servicios predefinidos usados en la configuración predeterminada de las zonas de firewall.

Servicios firewalld predefinidos seleccionados

Nombre del servicio	Configuración
ssh	Servidor SSH local. Tráfico a 22/tcp
dhcpv6-client	Cliente DHCPv6 local. Tráfico a 546/udp en la red fe80::/64 IPv6
ipp-client	Impresión IPP local. Tráfico a 631/udp.
samba-client	Archivo Windows local y cliente de intercambio de impresión. Tráfico a 137/udp y 138/udp.
mdns	Resolución del nombre del enlace local DNS (mDNS) multidifusión (multicast). Tráfico a 5353/udp a las direcciones de multidifusión (multicast) 224.0.0.251 (IPv4) o ff02::fb (IPv6).

nota

Existen muchos otros servicios predefinidos. El comando **`firewall-cmd --get-services`** los mostrará. Los archivos de configuración que definen los incluidos en el paquete *firewalld* se pueden encontrar en el directorio **`/usr/lib/firewalld/services`**, en un formato definido por **`firewalld.zone`**(5). No analizaremos en más detalle estos archivos en este capítulo.

Para los fines de este capítulo, las opciones más simples para un administrador de sistemas nuevo en **`firewalld`** es usar servicios predefinidos, o bien especificar explícitamente el puerto/protocolo que desean permitir. La herramienta gráfica **`firewall-config`** también se puede usar para revisar los servicios predefinidos y para definir servicios adicionales.

Configurar parámetros de firewall

Hay tres formas principales de que los administradores de sistemas interactúen con **`firewalld`**:

- Al editar directamente archivos de configuración en **`/etc/firewalld/`** (no analizado en este capítulo)
- Al usar la herramienta gráfica **`firewall-config`**
- Al usar **`firewall-cmd`** desde la línea de comandos

Configurar parámetros de firewall con firewall-config

`firewall-config` es una herramienta gráfica que se puede usar para alterar e inspeccionar tanto la configuración en ejecución en memoria para **`firewalld`**, así como la configuración persistente en disco. La herramienta **`firewall-config`** se puede instalar desde el paquete *firewall-config*.

Una vez instalado, **`firewall-config`** se puede iniciar desde la línea de comandos como **`firewall-config`**, o desde el menú Applications (Aplicaciones) bajo **Applications** > **Sundry** > **Firewall**. Si un usuario sin privilegios inicia **`firewall-config`**, se le solicitará la contraseña **`raíz`** para continuar.

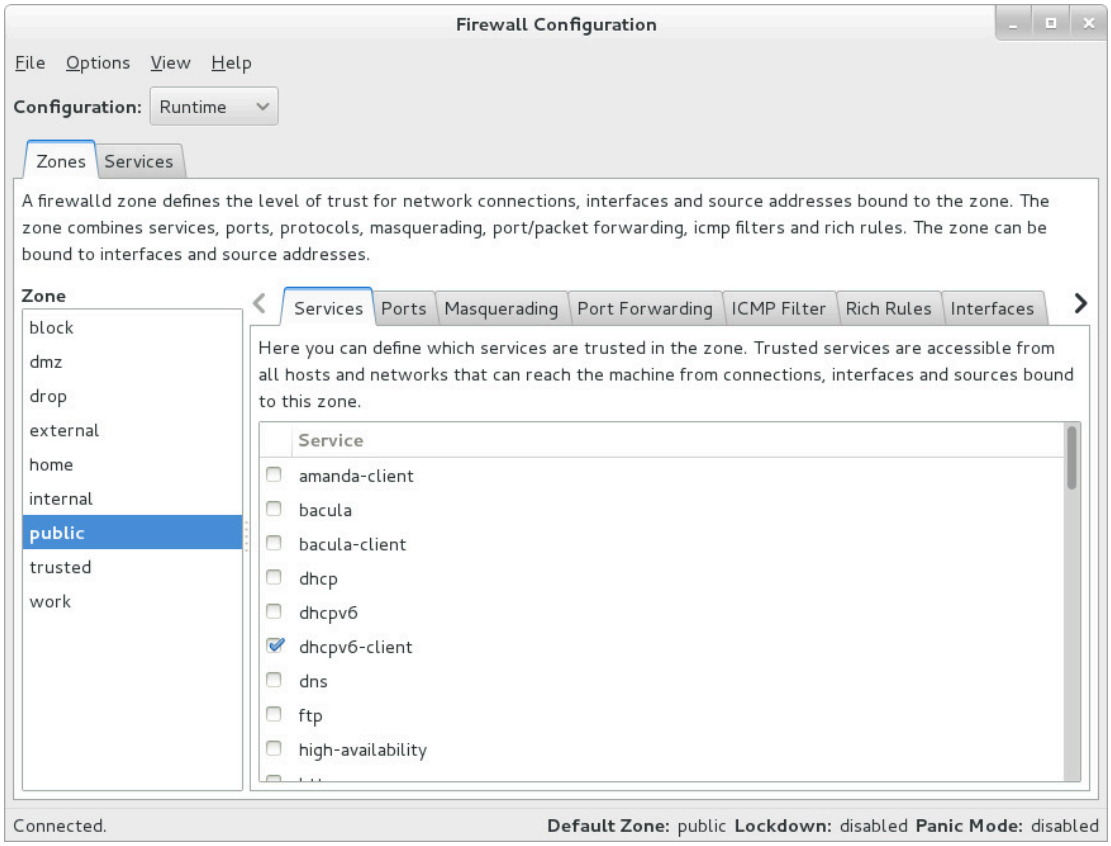

Figura 14.1: Pantalla de configuración de firewall principal

En la pantalla principal de **`firewall-config`**, un administrador de sistemas puede elegir entre modificar la configuración en memoria actual o la configuración en disco persistente que se usará luego de un nuevo inicio/nueva recarga de **`firewalld`**. Esto se logra con el menú desplegable **Configuration** (Configuración). En la mayoría de los casos, los administradores de sistemas desearán ajustar la configuración persistente (**Permanent** [Permanente]) y luego usar la entrada de menú **Options (Opciones)** > **Reload Firewalld (Volver a cargar firewalld)** para activar sus cambios.

Para modificar una zona, seleccione la zona en el menú **Zone** (Zona) a la izquierda. Interfaces de red e intervalos/direcciones IP de origen se pueden asignar en las pestañas **Interfaces** (Interfaces) y **Sources** (Orígenes) a la derecha, respectivamente.

Se pueden abrir puertos al poner una marca de verificación adelante de estos en la pestaña **Services** (Servicios) o al agregar un nuevo puerto en la pestaña **Ports** (Puertos) de esa zona.

Si un conjunto de puertos específicos tiene que abrirse en múltiples zonas, un administrador del sistema también puede definir un servicio para esos puertos. Esto se puede hacer en la pestaña **Services** (Servicios) en la parte superior de la ventana.

La zona *predeterminada* para conexiones especificadas de otro modo se puede cambiar en **Options (Opciones)** > **Change Default Zone (Cambiar zona predeterminada)**.

Importante

Todos los cambios hechos en la configuración **Permanent** (Permanente) no estarán activos hasta la próxima vez que la unidad de servicio **`firewalld`** se reinicie o se recargue. Del mismo modo, los cambios realizados en la configuración de **Runtime** (Tiempo de ejecución) no sobrevivirán una recarga o un reinicio del servicio **`firewalld`**.

Configurar parámetros del firewall con firewall-cmd

Para aquellos administradores de sistemas que prefieren trabajar en la línea de comandos o que no pueden usar un entorno gráfico por algún motivo, también hay un cliente de línea de comandos para interactuar con **`firewalld`**, **`firewall-cmd`**.

`firewall-cmd` se instala como parte del paquete principal *firewalld*. **`firewall-cmd`** puede realizar las mismas acciones que **`firewall-config`**.

En la siguiente tabla, se detallan varios comandos de **`firewall-cmd`** usados frecuentemente, junto con una explicación. Observe que, a menos que se especifique de otro modo, casi todos los comandos funcionarán en la configuración de *tiempo de ejecución*, a menos que se especifique la opción **`--permanent`**. Muchos de los comandos detallados toman la opción **`--zone=<ZONE>`** para determinar qué zona afectan.

Comandos `firewall-cmd`	Explicación
`--get-default-zone`	Consultar la zona predeterminada actual.
`--set-default-zone=<ZONE>`	Configurar la zona predeterminada. Esto cambia tanto la configuración del tiempo de ejecución como la permanente.
`--get-zones`	Mostrar todas las zonas disponibles.
`--get-active-zones`	Mostrar todas las zonas que están actualmente en uso (tienen una interfaz u origen conectado a esta), junto con la información de su interfaz y origen.
`--add-source=<CIDR> [--zone=<ZONE>]`	Enrutar todo el tráfico que proviene de la dirección IP o red/máscara de red **`<CIDR>`** a la zona especificada. Si no se proporciona ninguna opción **`--zone=`**, se usará la zona predeterminada.
`--remove-source=<CIDR> [--zone=<ZONE>]`	Eliminar la regla que enruta todo el tráfico que proviene de la dirección IP o red/máscara de red **`<CIDR>`** de la zona especificada. Si no se proporciona ninguna

Comandos `firewall-cmd`	Explicación
	opción **--zone=**, se usará la zona predeterminada.
--add-interface=<*INTERFACE*> [--zone=<*ZONE*>]	Enrutar todo el tráfico que proviene de **<*INTERFACE*>** a la zona especificada. Si no se proporciona ninguna opción **--zone=**, se usará la zona predeterminada.
--change-interface=<*INTERFACE*> [--zone=<*ZONE*>]	Asociar la interfaz con **<*ZONE*>** en lugar de su zona actual. Si no se proporciona ninguna opción **--zone=**, se usará la zona predeterminada.
--list-all [--zone=<*ZONE*>]	Mostrar todas las interfaces, fuentes, servicios y puertos configurados para **<*ZONE*>**. Si no se proporciona ninguna opción **--zone=**, se usará la zona predeterminada.
--list-all-zones	Recuperar toda la información para todas las zonas. (Interfaces, orígenes, puertos, servicios, etc.)
--add-service=<*SERVICE*> [--zone=<*ZONE*>]	Permitir el tráfico a **<*SERVICE*>**. Si no se proporciona ninguna opción **--zone=**, se usará la zona predeterminada.
--add-port=<*PORT/PROTOCOL*> [--zone=<*ZONE*>]	Permitir el tráfico a los puertos **<*PORT/PROTOCOL*>**. Si no se proporciona ninguna opción **--zone=**, se usará la zona predeterminada.
--remove-service=<*SERVICE*> [--zone=<*ZONE*>]	Eliminar **<*SERVICE*>** de la lista permitida para la zona. Si no se proporciona ninguna opción **--zone=**, se usará la zona predeterminada.
--remove-port=<*PORT/PROTOCOL*> [--zone=<*ZONE*>]	Eliminar los puertos **<*PORT/PROTOCOL*>** de la lista permitida para la zona. Si no se proporciona ninguna opción **--zone=**, se usará la zona predeterminada.
--reload	Dejar caer la configuración del tiempo de ejecución y aplicar la configuración persistente.

Ejemplo de firewall-cmd
Los siguientes ejemplos muestran la zona predeterminada que se configura en **dmz**, todo el tráfico proveniente de la red **192.168.0.0/24** que se asigna a la zona **internal** (interna) y los puertos de red para **mysql** que se abren en la zona **internal** (interna).

```
[root@serverX ~]# firewall-cmd --set-default-zone=dmz
[root@serverX ~]# firewall-cmd --permanent --zone=internal --add-source=192.168.0.0/24
[root@serverX ~]# firewall-cmd --permanent --zone=internal --add-service=mysql
[root@serverX ~]# firewall-cmd --reload
```

nota

En situaciones donde la sintaxis básica de **firewalld** no es suficiente, los administradores de sistemas también pueden agregar *rich-rules (reglas enriquecidas)*, una sintaxis más expresiva, para escribir reglas más complejas. Si aun así la sintaxis de las reglas enriquecidas no es suficiente, los administradores de sistemas también pueden usar *reglas de Direct Configuration (Configuración directa),* básicamente la sintaxis de **iptables** sin formato que se mezclará con las reglas de **firewalld**.

Estos modos avanzados no están incluidos en el alcance de este capítulo.

Referencias

Páginas del manual: **firewall-cmd**(1), **firewall-config**(1), **firewalld**(1), **firewalld.zone**(5) y **firewalld.zones**(5)

Práctica: Limitación de la comunicación de red

En este trabajo de laboratorio, configurará un firewall básico.

Recursos	
Máquinas:	**serverX** y **desktopX**

Resultados:
Luego de finalizar este ejercicio, su máquina **serverX** debe tener un servidor web en ejecución que escuche en el puerto sin cifrar **80/TCP** y el puerto encapsulado SSL **443/TCP**. La configuración de firewall en **serverX** solo debe permitir conexiones al puerto encapsulado SSL.

El firewall debe permitir el acceso a **sshd** y **vnc** desde todos los hosts.

Andes de comenzar
- Restablezca su sistema **serverX**.

1. En su sistema **serverX**, asegúrese de que tanto el paquete *httpd* como el paquete *mod_ssl* estén instalados. Estos paquetes proporcionan el servidor web *Apache* que usted protegerá con un firewall, y las extensiones necesarias para el servidor web para servir contenido mediante SSL.

   1.1.
   ```
   [student@serverX ~]$ sudo yum -y install httpd mod_ssl
   ```

2. En su sistema **serverX**, cree un nuevo archivo denominado **/var/www/html/index.html**, con el siguiente contenido:

   ```
   I am alive
   ```

   2.1.
   ```
   [student@serverX ~]$ sudo bash -c "echo 'I am alive' > /var/www/html/index.html"
   ```

3. Inicie y habilite el servicio **httpd** en su sistema **serverX**.

   3.1.
   ```
   [student@serverX ~]$ sudo systemctl start httpd
   ```

   3.2.
   ```
   [student@serverX ~]$ sudo systemctl enable httpd
   ```

4. En su sistema **serverX**, asegúrese de que tanto el servicio **iptables** como el **ip6tables** estén *enmascarados*, y de que el servicio **firewalld** esté habilitado y en ejecución.

   4.1.
   ```
   [student@serverX ~]$ sudo systemctl mask iptables
   [student@serverX ~]$ sudo systemctl mask ip6tables
   [student@serverX ~]$ sudo systemctl status firewalld
   ```

5. En su sistema **serverX**, inicie la aplicación **firewall-config**. Cuando se le solicite la contraseña de **student**, ingrese **student**.

   5.1.
   ```
   [student@serverX ~]$ firewall-config
   ```

   o

   Seleccione **Applications (Aplicaciones)** > **Sundry** > **Firewall** del menú del sistema.

6. En el menú desplegable **Configuration** (Configuración), seleccione **Permanent** (Permanente) para cambiar a la edición de la configuración permanente.

7. Agregue el servicio **https** a la lista de servicios permitidos en la zona **public** (pública).

   7.1. En la lista **Zone** (Zona), seleccione **public** (pública). Dado que esta zona es también la zona predeterminada, se destaca en negrita.

   7.2. En la pestaña **Services** (Servicios), agregue una marca de verificación delante del servicio **https**.

   7.3. **Importante**: También agregue una marca de verificación delante del servicio **vnc-server**. Si no lo hace, se bloqueará la interfaz gráfica cuando active el firewall. Si accidentalmente se bloquea, recupere el acceso con **ssh -X &srv; firewall-config** desde su máquina **desktopX**.

8. Active la configuración de su firewall seleccionando **Options (Opciones)** > **Reload Firewalld (Recargar firewalld)** desde el menú.

9. Verifique su trabajo al intentar ver el contenido de su servidor web desde **desktopX**.

   9.1. Este comando debería fallar:

   ```
   [student@desktopX ~]$ curl -k http://serverX.example.com
   ```

   9.2. Este comando debe arrojar resultados satisfactorios:

   ```
   [student@desktopX ~]$ curl -k https://serverX.example.com
   ```

nota

Si usa **firefox** para conectarse al servidor web, le solicitará la verificación del certificado del host si pasa el firewall satisfactoriamente.

Trabajo de laboratorio: Limitación de la comunicación de red

En este trabajo de laboratorio, configurará un firewall en su sistema **serverX** para bloquear todo acceso a los servicios que no sean **ssh** y un servidor web que se ejecuta en un puerto **8080/TCP**.

Recursos	
Máquinas:	**serverX** y **desktopX**

Resultados:
Un firewall configurado en **serverX** que bloquea el acceso a servicios que no sean **ssh** y **8080/TCP**.

Andes de comenzar
- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo.

```
[student@serverX ~]$ lab firewall setup
```

- Restablezca su sistema **desktopX**.

Su empresa ha decidio ejecutar una nueva aplicación. Esta aplicación escucha en puertos **80/TCP** y **8080/TCP**. Debido a consideraciones de seguridad, solo se debe poder llegar al puerto **8080/TCP** desde el mundo exterior. Se entiende que **ssh** (puerto **22/TCP**) también debe estar disponible. Todos los cambios que hace deben persistir en un reinicio.

Importante: La interfaz gráfica usada en el entorno Aprendizaje en línea de Red Hat necesita el puerto **5900/TCP** para permanecer disponible también. Este puerto también es conocido bajo el nombre del servicio **vnc-server**. Si accidentalmente se bloquea a usted mismo fuera de su **serverX**, puede intentar recuperar el acceso al usar **ssh** para su máquina **serverX** desde su máquina **desktopX** o restablecer su máquina **serverX**. Si elige restablecer su máquina **serverX**, tendrá que ejecutar los scripts de configuración para este trabajo de laboratorio nuevamente. La configuración de sus máquinas ya incluye una zona personalizada denominada **ROL** que abre estos puertos.

Cuando haya finalizado su trabajo, vuelva a arrancar su máquina **serverX**, y luego, ejecute el comando **lab firewall grade** desde su máquina **desktopX** para verificar su trabajo.

1. Configure su sistema de modo que los servicios **iptables** y **ip6tables** no sean iniciados accidentalmente por un administrador.
2. Verifique si el servicio **firewalld** se está ejecutando. Si no, inícielo.
3. Verifique que la zona de firewall predeterminada esté configurada en **public** (pública).
4. Verifique que no haya puertos no deseados abiertos en la configuración permanente para la zona **public** (pública).

5. Agregue el puerto **8080/TCP** a la configuración permanente para la zona **public** (pública). Verifique su configuración.

6. Reinicie su máquina **serverX**. (Para realizar una evaluación rápida, también puede usar **sudo firewall-cmd --reload**).

7. Desde su máquina **desktopX**, ejecute **lab firewall grade** para verificar su trabajo.

Solución

En este trabajo de laboratorio, configurará un firewall en su sistema **serverX** para bloquear todo acceso a los servicios que no sean **ssh** y un servidor web que se ejecuta en un puerto **8080/TCP**.

Recursos	
Máquinas:	**serverX** y **desktopX**

Resultados:
Un firewall configurado en **serverX** que bloquea el acceso a servicios que no sean **ssh** y **8080/TCP**.

Andes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo.

```
[student@serverX ~]$ lab firewall setup
```

- Restablezca su sistema **desktopX**.

Su empresa ha decidio ejecutar una nueva aplicación. Esta aplicación escucha en puertos **80/TCP** y **8080/TCP**. Debido a consideraciones de seguridad, solo se debe poder llegar al puerto **8080/TCP** desde el mundo exterior. Se entiende que **ssh** (puerto **22/TCP**) también debe estar disponible. Todos los cambios que hace deben persistir en un reinicio.

Importante: La interfaz gráfica usada en el entorno Aprendizaje en línea de Red Hat necesita el puerto **5900/TCP** para permanecer disponible también. Este puerto también es conocido bajo el nombre del servicio **vnc-server**. Si accidentalmente se bloquea a usted mismo fuera de su **serverX**, puede intentar recuperar el acceso al usar **ssh** para su máquina **serverX** desde su máquina **desktopX** o restablecer su máquina **serverX**. Si elige restablecer su máquina **serverX**, tendrá que ejecutar los scripts de configuración para este trabajo de laboratorio nuevamente. La configuración de sus máquinas ya incluye una zona personalizada denominada **ROL** que abre estos puertos.

Cuando haya finalizado su trabajo, vuelva a arrancar su máquina **serverX**, y luego, ejecute el comando **lab firewall grade** desde su máquina **desktopX** para verificar su trabajo.

1. Configure su sistema de modo que los servicios **iptables** y **ip6tables** no sean iniciados accidentalmente por un administrador.

   1.1.
   ```
   [student@serverX ~]$ sudo systemctl mask iptables
   [student@serverX ~]$ sudo systemctl mask ip6tables
   ```

2. Verifique si el servicio **firewalld** se está ejecutando. Si no, inícielo.

   2.1.
   ```
   [student@serverX ~]$ sudo systemctl status firewalld
   ```

   2.2. Si el paso anterior indicó que **firewalld** no estaba habilitado ni ejecutándose:

```
[student@serverX ~]$ sudo systemctl enable firewalld
[student@serverX ~]$ sudo systemctl start firewalld
```

3. Verifique que la zona de firewall predeterminada esté configurada en **public** (pública).

3.1.
```
[student@serverX ~]$ sudo firewall-cmd --get-default-zone
public
```

3.2. Si el paso anterior arrojó otra zona:

```
[student@serverX ~]$ sudo firewall-cmd --set-default-zone public
```

4. Verifique que no haya puertos no deseados abiertos en la configuración permanente para la zona **public** (pública).

4.1.
```
[student@serverX ~]$ sudo firewall-cmd --permanent --zone=public --list-all
public (default)
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

5. Agregue el puerto **8080/TCP** a la configuración permanente para la zona **public** (pública). Verifique su configuración.

5.1.
```
[student@serverX ~]$ sudo firewall-cmd --permanent --zone=public --add-port
 8080/tcp
```

5.2.
```
[student@serverX ~]$ sudo firewall-cmd --permanent --zone=public --list-all
public (default)
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports: 8080/tcp
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

6. Reinicie su máquina **serverX**. (Para realizar una evaluación rápida, también puede usar **sudo firewall-cmd --reload**).

7. Desde su máquina **desktopX**, ejecute **lab firewall grade** para verificar su trabajo.

7.1.
```
[student@desktopX ~]$ lab firewall grade
```

Resumen

Limitación de la comunicación de red

- El kernel Linux tiene un subsistema llamado **`netfilter`** para filtrar el tráfico de red.
- **`firewalld`** es el componente de espacio del usuario que administra las reglas del firewall.
- **`firewalld`** divide el tráfico en zonas basadas en la dirección de origen y la interfaz de red a la que llega, y cada zona tiene sus propias reglas de firewall.
- **`firewall-config`** y **`firewall-cmd`** se pueden usar para controlar las reglas de firewall.

CAPÍTULO 15

REVISIÓN COMPLETA DE SYSTEM ADMINISTRATION II

Descripción general	
Meta	Practicar y demostrar conocimientos y habilidades aprendidas en Red Hat System Administration II.
Objetivos	• Revisar los capítulos del curso para reforzar conocimientos y habilidades.
Secciones	• Revisión completa de Red Hat System Administration II
Trabajo de laboratorio	• Revisión completa de Red Hat System Administration II

Revisión integral de Red Hat System Administration II

Objetivos

Después de completar esta sección, los estudiantes deben poder demostrar sus conocimientos y habilidades respecto del tema cubierto en cada capítulo.

Revisión de Red Hat System Administration II

Antes de comenzar la revisión integral de este curso, los estudiantes deberían sentirse cómodos con los temas que se explicaron en cada capítulo.

Los estudiantes pueden consultar las secciones anteriores en el libro de textos para lecturas complementarias.

Capítulo 1, Automatización de la instalación con Kickstart
Automatizar la instalación de sistemas Red Hat Enterprise Linux con Kickstart.
- Explicar los conceptos y la arquitectura de Kickstart.
- Crear un archivo de configuración kickstart.

Capítulo 2, Uso de expresiones regulares con grep
Escribir expresiones regulares mediante el uso de **`grep`** para aislar o localizar contenido en archivos de texto.
- Crear expresiones regulares que coincidan con patrones de texto.
- Usar **`grep`** para localizar contenido en archivos.

Capítulo 3, Creación y edición de archivos de texto con vim
Presentar el editor de textos **`vim`**.
- Explicar los tres modos principales de **`vim`**.
- Abrir, editar y guardar archivos de texto.
- Usar atajos del editor.

Capítulo 4, Programación de tareas futuras de Linux
Programar tareas para que se ejecuten automáticamente en el futuro.
- Programar tareas únicas con at.
- Programar trabajos recurrentes con cron.
- Programar trabajos de sistemas recurrentes.
- Administrar archivos temporales.

Capítulo 5, Administración de la prioridad de los procesos de Linux
Influir en las prioridades relativas según las cuales se ejecutan los procesos de Linux.
- Describir niveles de nice.
- Establecer niveles de nice sobre procesos nuevos y existentes.

Capítulo 6, Control de acceso a archivos con listas de control de acceso (ACL)
Administrar la seguridad de los archivos utilizando listas de control de acceso (ACL) POSIX.
- Describir listas de control de acceso POSIX.
- Administrar listas de control de acceso POSIX.

Capítulo 7, Administración de seguridad de SELinux
Administrar el comportamiento de Security Enhanced Linux (SELinux) de un sistema para mantenerlo seguro en caso de un riesgo del servicio de red.
- Explicar los conceptos básicos de los permisos de SELinux.
- Cambiar modos de SELinux con setenforce.
- Cambiar contextos de archivos con semanage y restorecon.
- Administrar booleanos de SELinux con setsebool.
- Examinar registros y usar sealert para solucionar problemas de violaciones de SELinux.

Capítulo 8, Conexión de usuarios y grupos definidos por la red
Configurar sistemas para usar servicios de administración de identidades centrales.
- Usar servicios de administración de identidades centralizados.

Capítulo 9, Adición de discos, particiones y sistemas de archivos a un sistema Linux
Crear y administrar discos, particiones y sistemas de archivos desde la línea de comandos.
- Gestionar particiones y sistemas de archivos sencillos.
- Administrar espacio swap (intercambio).

Capítulo 10, Administración del almacenamiento de gestión de volúmenes lógicos (LVM)
Gestionar volúmenes lógicos desde la línea de comandos.
- Describir los componentes y conceptos de la gestión de volúmenes lógicos.
- Gestionar volúmenes lógicos.
- Extender volúmenes lógicos.

Capítulo 11, Acceso a almacenamiento de red con el sistema de archivos de red (NFS)
Usar autofs y línea de comandos para montar y desmontar almacenamiento de red con el NFS.
- Montar, acceder y desmontar almacenamiento de red con el NFS.
- Automontado y acceso a almacenamiento de red con NFS.

Capítulo 12, Acceso a almacenamiento de red con SMB
Usar autofs y línea de comandos para montar y desmontar sistemas de archivos SMB.
- Montar, automontar y desmontar sistemas de archivos SMB.

Capítulo 13, Control y solución de problemas del proceso de arranque de Red Hat Enterprise Linux
Solucionar problemas del proceso de arranque de Red Hat Enterprise Linux.
- Describir el proceso de arranque de Red Hat Enterprise Linux.
- Reparar problemas de arranque comunes.

- Reparar problemas de archivos en el arranque.
- Reparar problemas del cargador de arranque.

Capítulo 14, Limitación de la comunicación de red con firewalld
Configurar un firewall básico.
- Configurar un firewall básico usando **`firewalld`**, **`firewall-config`** y **`firewall-cmd`**.

Referencias

Obtenga información acerca de más clases disponibles de Red Hat en
http://www.redhat.com/training/

Trabajo de laboratorio: Revisión integral de Red Hat System Administration II

En este trabajo de laboratorio, el estudiante configurará un sistema usando las habilidades enseñadas en el curso.

Recursos:	
Archivos:	**http://&srvfqdn;/logfile**
Máquinas:	**serverX** y **desktopX**

Resultados:
Dos sistemas configurados según los requisitos especificados a continuación.

Andes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo.

```
[student@serverX ~]$ lab sa2-review setup
```

- Restablezca su sistema **desktopX**.

Se le ha asignado la tarea de configurar un nuevo sistema para su empresa: **desktopX**. El sistema debe configurarse según los siguientes requisitos.

- El sistema debe autenticar a los usuarios usando **LDAP** y **Kerberos** usando la siguiente configuración:

Nombre	Valor
Servidor LDAP	**classroom.example.com**
Base de búsqueda	**dc=example,dc=com**
Usar TLS	Sí
Cert TLS CA	**http://classroom.example.com/pub/example-ca.crt**
Dominio Kerberos	**EXAMPLE.COM**
KDC de Kerberos	**classroom.example.com**
Servidor de administración Kerberos	**classroom.example.com**

  Con fines de evaluación, puede usar el usuario **ldapuser*X***, con la contraseña **kerberos**.

- Los directorios de inicio para sus usuarios de LDAP deben montarse automáticamente en el acceso. Estos directorios de inicio reciben el servicio del recurso compartido de NFS **classroom.example.com:/home/guests**.
- **serverX** exporta un recurso compartido CIFS denominado **westeros**. Este recurso compartido debe montarse automáticamente en el arranque en el punto de montaje **/**

mnt/westeros. Para montar este recurso compartido, deberá usar el nombre de usuario **tyrion** con la contraseña **slapjoffreyslap**. Esta contraseña no debe almacenarse en ninguna parte en donde un usuario sin privilegios pueda leerla.

- **serverX** exporta un recurso compartido de NFSv4 denominado **/essos**. Este recurso compartido debe montarse como lectura-escritura en el arranque en **/mnt/essos** usando la autenticación, el cifrado y la revisión de integridad de Kerberos.

  Puede descargar una keytab para su sistema desde **http://&clrmfqdn;/pub/keytabs/desktop*X*.keytab**.

- Configure un nuevo volumen lógico de 512 MiB denominado **arya** en un nuevo grupo de volúmenes de 2 GiB denominado **stark**.

  Este nuevo volumen lógico debe formatearse con un sistema de archivos XFS y montarse persistentemente en **/mnt/underfoot**.

- Su sistema debe estar equipado con una nueva partición swap (intercambio) de 512 MiB, activada automáticamente en el arranque.

- Cree un nuevo grupo denominado **kings** y cuatro nuevo usuarios que pertenezcan a ese grupo: **stannis**, **joffrey**, **renly** y **robb**.

- Cree un nuevo directorio **/ironthrone**, que sea propiedad de **root:root** con permisos **700**.

  Configure este directorio de modo que los usuarios en el grupo **kings** tengan privilegios tanto de lectura como de escritura, con la excepción del usuario **joffrey**, a quien solo deben otorgarse privilegios de lectura.

  Estas restricciones también se deben aplicar a todos los archivos y directorios nuevos creados en el directorio **/ironthrone**.

- Instale los paquetes *httpd* y *mod_ssl*, luego habilite e inicie el servicio **httpd.service**.

- Abra un puerto **12345/tcp** en la zona predeterminada para el firewall que se ejecuta en su sistema.

- Cree un nuevo directorio denominado **/docroot**. Asegúrese de que el contexto SELinux para este directorio esté establecido en **public_content_t** y que este contexto sobrevivirá una operación de nuevo etiquetado.

- **http://server*X*.example.com/logfile** contiene los registros para un proyecto reciente. Descargue este archivo, luego extraiga todas las líneas que finalicen en **ERROR** o **FALLO** para el archivo **/home/student/errors.txt**. Todas las líneas deben mantenerse en el orden en el cual aparecen en el archivo de registro.

- Su sistema debe tener un nuevo directorio usado para almacenar archivos temporales denominados **/run/veryveryvolatile**. Siempre que se ejecute **systemd-tmpfiles --clean**, cualquier archivo con una antigüedad mayor que **5** segundos debe eliminarse de ese directorio.

  Este directorio debe tener permisos **1777**, y ser propiedad de **root:root**.

Todos los cambios deben sobrevivir un nuevo arranque. Cuando haya terminado de configurar su sistema, puede evaluar su trabajo reiniciando su máquina **desktopX** y ejecutando el siguiente comando:

```
[student@desktopX ~]$ lab sa2-review grade
```

Solución

En este trabajo de laboratorio, el estudiante configurará un sistema usando las habilidades enseñadas en el curso.

Recursos:	
Archivos:	**http://&srvfqdn;/logfile**
Máquinas:	**serverX** y **desktopX**

Resultados:
Dos sistemas configurados según los requisitos especificados a continuación.

Andes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo.

```
[student@serverX ~]$ lab sa2-review setup
```

- Restablezca su sistema **desktopX**.

Se le ha asignado la tarea de configurar un nuevo sistema para su empresa: **desktopX**. El sistema debe configurarse según los siguientes requisitos.

- El sistema debe autenticar a los usuarios usando **LDAP** y **Kerberos** usando la siguiente configuración:

Nombre	Valor
Servidor LDAP	**classroom.example.com**
Base de búsqueda	**dc=example,dc=com**
Usar TLS	Sí
Cert TLS CA	**http://classroom.example.com/pub/example-ca.crt**
Dominio Kerberos	**EXAMPLE.COM**
KDC de Kerberos	**classroom.example.com**
Servidor de administración Kerberos	**classroom.example.com**

  Con fines de evaluación, puede usar el usuario **ldapuser*X***, con la contraseña **kerberos**.

- Los directorios de inicio para sus usuarios de LDAP deben montarse automáticamente en el acceso. Estos directorios de inicio reciben el servicio del recurso compartido de NFS **classroom.example.com:/home/guests**.
- **serverX** exporta un recurso compartido CIFS denominado **westeros**. Este recurso compartido debe montarse automáticamente en el arranque en el punto de montaje **/mnt/westeros**. Para montar este recurso compartido, deberá usar el nombre de usuario **tyrion** con la contraseña **slapjoffreyslap**. Esta contraseña no debe almacenarse en ninguna parte en donde un usuario sin privilegios pueda leerla.

- **serverX** exporta un recurso compartido de NFSv4 denominado **/essos**. Este recurso compartido debe montarse como lectura-escritura en el arranque en **/mnt/essos** usando la autenticación, el cifrado y la revisión de integridad de Kerberos.

  Puede descargar una keytab para su sistema desde **http://&clrmfqdn;/pub/keytabs/desktopX.keytab**.

- Configure un nuevo volumen lógico de 512 MiB denominado **arya** en un nuevo grupo de volúmenes de 2 GiB denominado **stark**.

  Este nuevo volumen lógico debe formatearse con un sistema de archivos XFS y montarse persistentemente en **/mnt/underfoot**.

- Su sistema debe estar equipado con una nueva partición swap (intercambio) de 512 MiB, activada automáticamente en el arranque.

- Cree un nuevo grupo denominado **kings** y cuatro nuevo usuarios que pertenezcan a ese grupo: **stannis**, **joffrey**, **renly** y **robb**.

- Cree un nuevo directorio **/ironthrone**, que sea propiedad de **root:root** con permisos **700**.

  Configure este directorio de modo que los usuarios en el grupo **kings** tengan privilegios tanto de lectura como de escritura, con la excepción del usuario **joffrey**, a quien solo deben otorgarse privilegios de lectura.

  Estas restricciones también se deben aplicar a todos los archivos y directorios nuevos creados en el directorio **/ironthrone**.

- Instale los paquetes *httpd* y *mod_ssl*, luego habilite e inicie el servicio **httpd.service**.

- Abra un puerto **12345/tcp** en la zona predeterminada para el firewall que se ejecuta en su sistema.

- Cree un nuevo directorio denominado **/docroot**. Asegúrese de que el contexto SELinux para este directorio esté establecido en **public_content_t** y que este contexto sobrevivirá una operación de nuevo etiquetado.

- **http://serverX.example.com/logfile** contiene los registros para un proyecto reciente. Descargue este archivo, luego extraiga todas las líneas que finalicen en **ERROR** o **FALLO** para el archivo **/home/student/errors.txt**. Todas las líneas deben mantenerse en el orden en el cual aparecen en el archivo de registro.

- Su sistema debe tener un nuevo directorio usado para almacenar archivos temporales denominados **/run/veryveryvolatile**. Siempre que se ejecute **systemd-tmpfiles --clean**, cualquier archivo con una antigüedad mayor que **5** segundos debe eliminarse de ese directorio.

  Este directorio debe tener permisos **1777**, y ser propiedad de **root:root**.

Todos los cambios deben sobrevivir un nuevo arranque. Cuando haya terminado de configurar su sistema, puede evaluar su trabajo reiniciando su máquina **desktopX** y ejecutando el siguiente comando:

```
[student@desktopX ~]$ lab sa2-review grade
```

1. El sistema debe autenticar a los usuarios usando **LDAP** y **Kerberos** con la siguiente configuración:

Nombre	Valor
Servidor LDAP	**classroom.example.com**
Base de búsqueda	**dc=example,dc=com**
Usar TLS	Sí
Cert TLS CA	**http://classroom.example.com/pub/example-ca.crt**
Dominio Kerberos	**EXAMPLE.COM**
KDC de Kerberos	**classroom.example.com**
Servidor de administración Kerberos	**classroom.example.com**

Con fines de evaluación, puede usar el usuario **ldapuser*X***, con la contraseña **kerberos**.

1.1. Instale los paquetes *authconfig-gtk* y *sssd*.

```
[student@desktopX ~]$ sudo yum install authconfig-gtk sssd
```

1.2. Ejecute **authconfig-gtk** e ingrese la información proporcionada. No olvide desmarcar la opción **Use DNS to locate KDCs for realms** (Usar DNS para ubicar KDC para dominios).

```
[student@desktopX ~]$ sudo authconfig-gtk
```

2. Los directorios de inicio para sus usuarios de LDAP deben montarse automáticamente en el acceso. Estos directorios de inicio reciben el servicio del recurso compartido de NFS **classroom.example.com:/home/guests**.

2.1. Instale el paquete *autofs*.

```
[student@desktopX ~]$ sudo yum install autofs
```

2.2. Cree un nuevo archivo denominado **/etc/auto.master.d/guests.autofs** con el siguiente contenido:

```
/home/guests  /etc/auto.guests
```

2.3. Cree un nuevo archivo denominado **/etc/auto.guests** con el siguiente contenido:

```
* -rw,sync  classroom.example.com:/home/guests/&
```

2.4. Inicie y habilite el servicio **autofs.service**.

```
[student@desktopX ~]$ sudo systemctl enable autofs.service
[student@desktopX ~]$ sudo systemctl start autofs.service
```

3. **serverX** exporta un recurso compartido CIFS denominado **westeros**. Este recurso compartido debe montarse automáticamente en el arranque en el punto de montaje **/mnt/westeros**. Para montar este recurso compartido, deberá usar el nombre de usuario **tyrion** con la contraseña **slapjoffreyslap**. Esta contraseña no debe almacenarse en ninguna parte en donde un usuario sin privilegios pueda leerla.

   3.1. Instale el paquete *cifs-utils*.

   ```
   [student@desktopX ~]$ sudo yum install cifs-utils
   ```

   3.2. Cree el punto de montaje.

   ```
   [student@desktopX ~]$ sudo mkdir -p /mnt/westeros
   ```

   3.3. Cree un archivo de credenciales denominado **/root/tyrion.creds** con el siguiente contenido, luego establezca los permisos en ese archivo en **0600**:

   ```
   username=tyrion
   password=slapjoffreyslap
   ```

   ```
   [student@desktopX ~]$ sudo chmod 0600 /root/tyrion.creds
   ```

   3.4. Agregue la siguiente línea a **/etc/fstab**:

   ```
   //serverX.example.com/westeros /mnt/westeros cifs creds=/root/tyrion.creds 0 0
   ```

   3.5. Monte todos los sistemas de archivos e inspeccione el sistema de archivos montado.

   ```
   [student@desktopX ~]$ sudo mount -a
   [student@desktopX ~]$ cat /mnt/westeros/README.txt
   ```

4. **serverX** exporta un recurso compartido de NFSv4 denominado **/essos**. Este recurso compartido debe montarse como lectura-escritura en el arranque en **/mnt/essos** usando la autenticación, cifrado y revisión de integridad de Kerberos.

   Puede descargar una keytab para su sistema desde **http://&clrmfqdn;/pub/keytabs/desktopX.keytab**.

   4.1. Cree el punto de montaje.

   ```
   [student@desktopX ~]$ sudo mkdir -p /mnt/essos
   ```

   4.2. Descargue la keytab para su sistema.

```
[student@desktopX ~]$ sudo wget -O /etc/krb5.keytab http://
classroom.example.com/pub/keytabs/desktopX.keytab
```

4.3. Agregue la siguiente línea en **/etc/fstab**:

```
serverX.example.com:/essos /mnt/essos nfs sec=krb5p,rw 0 0
```

4.4. Inicie y habilite el servicio **nfs-secure.service**.

```
[student@desktopX ~]$ sudo systemctl enable nfs-secure.service
[student@desktopX ~]$ sudo systemctl start nfs-secure.service
```

4.5. Monte todos los sistemas de archivos.

```
[student@desktopX ~]$ sudo mount -a
```

5. Configure un nuevo volumen lógico de 512 MiB denominado **arya** en un nuevo grupo de volúmenes de 2 GiB denominado **stark**.

   Este nuevo volumen lógico debe formatearse con un sistema de archivos XFS y montarse persistentemente en **/mnt/underfoot**.

   5.1. Cree una partición de 2 GiB en un disco secundario.

```
[student@desktopX ~]$ sudo fdisk /dev/vdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0xcade6cae.

Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): Enter
First sector (2048-20971519, default 2048): Enter
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519): +2G
Partition 1 of type Linux and of size 2 GiB is set

Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

5.2. Cambie la nueva partición a un volumen físico.

```
[student@desktopX ~]$ sudo pvcreate /dev/vdb1
```

5.3. Cree un nuevo grupo de volúmenes con el nuevo volumen físico.

```
[student@desktopX ~]$ sudo vgcreate stark /dev/vdb1
```

5.4. Cree un nuevo volumen lógico (LV) de 512 MiB en el nuevo grupo de volúmenes.

```
[student@desktopX ~]$ sudo lvcreate -n arya -L 512M stark
```

5.5. Formatee el nuevo LV con un sistema de archivos XFS.

```
[student@desktopX ~]$ sudo mkfs -t xfs /dev/stark/arya
```

5.6. Cree el punto de montaje.

```
[student@desktopX ~]$ sudo mkdir -p /mnt/underfoot
```

5.7. Agregue la siguiente línea a **`/etc/fstab`**:

```
/dev/stark/arya /mnt/underfoot xfs defaults 1 2
```

5.8. Monte todos los sistemas de archivos.

```
[student@desktopX ~]$ sudo mount -a
```

6. Su sistema debe estar equipado con una nueva partición swap (intercambio) de 512 MiB, activada automáticamente en el arranque.

6.1. Cree una nueva partición de 512 MiB en su disco secundario y establezca el tipo de partición en **82**.

```
[student@desktopX ~]$ sudo fdisk /dev/vdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): n
Partition type:
   p   primary (1 primary, 0 extended, 3 free)
   e   extended
Select (default p): p
Partition number (2-4, default 2): Enter
First sector (4196352-20971519, default 4196352): Enter
Using default value 4196352
Last sector, +sectors or +size{K,M,G} (4196352-20971519, default
 20971519): +512M
```

```
Partition 2 of type Linux and of size 512 MiB is set

Command (m for help): t
Partition number (1,2, default 2): Enter
Hex code (type L to list all codes): 82
Changed type of partition 'Linux' to 'Linux swap / Solaris'

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource
 busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
[student@desktopX ~]$ sudo partprobe
```

6.2. Formatee la nueva partición como swap (intercambio).

```
[student@desktopX ~]$ sudo mkswap /dev/vdb2
```

6.3. Recupere el UUID para su nueva partición swap (intercambio).

```
[student@desktopX ~]$ sudo blkid /dev/vdb2
```

6.4. Agregue la siguiente línea a **`/etc/fstab`**; asegúrese de usar el UUID que halló en el paso anterior.

```
UUID="xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx" swap swap defaults 0 0
```

6.5. Active todos los swaps (intercambios).

```
[student@desktopX ~]$ sudo swapon -a
```

7. Cree un nuevo grupo denominado **`kings`** y cuatro nuevo usuarios que pertenezcan a ese grupo: **`stannis`**, **`joffrey`**, **`renly`** y **`robb`**.

7.1. Cree el grupo **`kings`**.

```
[student@desktopX ~]$ sudo groupadd kings
```

7.2. Cree los cuatro usuarios y agréguelos al grupo **`kings`**.

```
[student@desktopX ~]$ for NEWUSER in stannis joffrey renly robb; do
>  sudo useradd -G kings ${NEWUSER}
> done
```

8. Cree un nuevo directorio **`/ironthrone`**, que sea propiedad de **`root:root`** con permisos **`0700`**.

Configure este directorio de modo que los usuarios en el grupo **kings** tengan privilegios tanto de lectura como de escritura, con la excepción del usuario **joffrey**, a quien solo deben otorgarse privilegios de lectura.

Estas restricciones también se deben aplicar a todos los archivos y directorios nuevos creados en el directorio **/ironthrone**.

8.1. Cree el directorio con los permisos correctos.

```
[student@desktopX ~]$ sudo mkdir -m 0700 /ironthrone
```

8.2. Agregue una ACL en **/ironthrone** otorgando a los usuarios del grupo **kings** privilegios de lectura y escritura. No olvide agregar también permisos de ejecución, dado que este es un directorio.

```
[student@desktopX ~]$ sudo setfacl -m g:kings:rwX /ironthrone
```

8.3. Agregue una ACL para el usuario **joffrey**, con permisos de solo lectura y ejecución.

```
[student@desktopX ~]$ sudo setfacl -m u:joffrey:r-x /ironthrone
```

8.4. Agregue también las dos ACL anteriores como ACL predeterminadas.

```
[student@desktopX ~]$ sudo setfacl -m d:g:kings:rwx /ironthrone
[student@desktopX ~]$ sudo setfacl -m d:u:joffrey:r-x /ironthrone
```

9. Instale los paquetes *httpd* y *mod_ssl*, luego habilite e inicie el servicio **httpd.service**.

9.1. Instale los paquetes *httpd* y *mod_ssl*.

```
[student@desktopX ~]$ sudo yum install httpd mod_ssl
```

9.2. Inicie y habilite el servicio **httpd.service**.

```
[student@desktopX ~]$ sudo systemctl start httpd.service
[student@desktopX ~]$ sudo systemctl enable httpd.service
```

10. Abra un puerto **12345/tcp** en la zona predeterminada para el firewall que se ejecuta en su sistema.

10.1 Abra el puerto **12345/tcp** en la configuración permanente de la zona predeterminada para su firewall.

```
[student@desktopX ~]$ sudo firewall-cmd --permanent --add-port=12345/tcp
```

10.2 Vuelva a cargar su firewall para activar sus cambios.

```
[student@desktopX ~]$ sudo firewall-cmd --reload
```

11. Cree un nuevo directorio denominado **/docroot**. Asegúrese de que el contexto SELinux para este directorio esté establecido en **public_content_t** y que este contexto sobrevivirá una operación de nuevo etiquetado.

    11.1 Cree el directorio **/docroot**.

    ```
    [student@desktopX ~]$ sudo mkdir /docroot
    ```

    11.2 Agregue un nuevo contexto de archivos predeterminado para el directorio **/docroot** y todos sus descendientes.

    ```
    [student@desktopX ~]$ sudo semanage fcontext -a -t public_content_t '/
    docroot(/.*)?'
    ```

    11.3 Vuelva a etiquetar el directorio **/docroot**.

    ```
    [student@desktopX ~]$ sudo restorecon -RvF /docroot
    ```

12. **http://server*X*.example.com/logfile** contiene los registros para un proyecto reciente. Descargue este archivo, luego extraiga todas las líneas que finalicen en **ERROR** o **FALLO** para el archivo **/home/student/errors.txt**. Todas las líneas deben mantenerse en el orden en el cual aparecen en el archivo de registro.

    12.1 Descargue el archivo de registros.

    ```
    [student@desktopX ~]$ wget http://server X.example.com/logfile
    ```

    12.2 Extraiga cada línea que termine en **ERROR** o **FALLO** en el archivo **/home/student/errors.txt**, mientras mantiene intacto el orden de las líneas.

    ```
    [student@desktopX ~]$ grep -e 'ERROR$' -e 'FAIL$' logfile > /home/student/
    errors.txt
    ```

13. Su sistema debe tener un nuevo directorio usado para almacenar archivos temporales denominados **/run/veryveryvolatile**. Siempre que se ejecute **systemd-tmpfiles --clean**, cualquier archivo con una antigüedad mayor que **5** segundos debe eliminarse de ese directorio.

    Este directorio debe tener permisos **1777**, y ser propiedad de **root:root**.

    13.1 Cree un nuevo archivo denominado **/etc/tmpfiles.d/veryveryvolatile.conf** con el siguiente contenido:

    ```
    d /run/veryveryvolatile 1777 root root 5s
    ```

    13.2 Haga que **systemd-tmpfiles** cree el directorio.

    ```
    [student@desktopX ~]$ sudo systemd-tmpfiles --create
    ```

14. Compruebe su trabajo al volver a arrancar su máquina **desktopX** y ejecute el siguiente comando en su sistema **desktopX**:

```
[student@desktopX ~]$ lab sa2-review grade
```

Si algún requisito se presenta como “FALLO”, vuelva a revisar ese requisito, y luego vuelva a arrancar y a corregir nuevamente.

Resumen

Revisión integral de Red Hat System Administration II

- Revise los capítulos para validar el nivel de conocimientos.
- Revise los ejercicios de práctica para validar el nivel de habilidades.