



**RED HAT®
TRAINING**



Capacitación integral y práctica que resuelve los problemas del mundo real

Red Hat System Administration I

Manual del alumno (ROLE)

RED HAT SYSTEM ADMINISTRATION I

Red Hat Enterprise Linux 7 RH124
Red Hat System Administration I
Edición 3 20170803

Autores: Susan Lauber, Philip Sweany, Rudolf Kastl, George Hacker
Editor: Steven Bonneville

Copyright © 2015 Red Hat, Inc.

The contents of this course and all its modules and related materials, including handouts to audience members, are Copyright © 2015 Red Hat, Inc.

No part of this publication may be stored in a retrieval system, transmitted or reproduced in any way, including, but not limited to, photocopy, photograph, magnetic, electronic or other record, without the prior written permission of Red Hat, Inc.

This instructional program, including all material provided herein, is supplied without any guarantees from Red Hat, Inc. Red Hat, Inc. assumes no liability for damages or legal action arising from the use or misuse of contents or details contained herein.

If you believe Red Hat training materials are being used, copied, or otherwise improperly distributed please e-mail training@redhat.com or phone toll-free (USA) +1 (866) 626-2994 or +1 (919) 754-3700.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, Hibernate, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a registered trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

The OpenStack® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Colaboradores: Rob Locke, Bowe Strickland, Scott McBrien, Wander Boessenkool, Forrest Taylor

Revisores: Michael Phillips, David Bucknell, Aaron Hicks, Jay Ramsurrun

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

Convenciones del documento	xii
Notas y advertencias	xii
Introducción	xiii
Red Hat System Administration I	xiii
Orientación sobre el entorno del trabajo de laboratorio en el aula	xiv
Internacionalización	xvi
1. Acceso a la línea de comandos	1
Acceso a la línea de comandos a través de la consola local	2
Práctica: Terminales de acceso a la consola local	5
Acceso a la línea de comandos con el escritorio	8
Práctica: Entorno de escritorio GNOME 3	13
Ejecución de comandos con la shell Bash	15
Práctica: comandos bash y atajos del teclado	19
Trabajo de laboratorio: Acceso a la línea de comandos	22
2. Administración de archivos desde la línea de comandos	29
Jerarquía del sistema de archivos Linux	30
Práctica: Jerarquía de sistemas de archivos	33
Ubicación de archivos por nombre	36
Práctica: Ubicación de archivos y directorios	41
Administración de archivos con las herramientas de línea de comandos	44
Práctica: Administración de archivo de línea de comandos	49
Coincidencia de nombres de archivo mediante el uso de expansión de nombre de ruta	52
Práctica: Expansión del nombre de ruta	56
Ejercicio de laboratorio: Administración de archivos con expansión de shell	58
3. Obtención de ayuda en Red Hat Enterprise Linux	65
Lectura de la documentación utilizando el comando man	66
Práctica: Uso del comando del man	69
Lectura de la documentación utilizando el comando pinfo	71
Práctica: uso del comando pinfo	74
Lectura de documentación en /usr/share/doc	76
Práctica: Visualización de la documentación del paquete	78
Obtención de ayuda de Red Hat	80
Práctica: Crear y visualizar un SoS Report	86
Ejercicio de laboratorio: Visualización e impresión de la documentación de ayuda	88
4. Creación, visualización y edición de archivos de texto	95
Redirecciónamiento de la salida a un archivo o programa	96
Práctica: Redirección y canalizaciones de E/S	103
Edición de archivos de texto desde el aviso de shell	105
Práctica: Edición de archivos con Vim	108
Edición de archivos de texto con un editor gráfico	110
Práctica: Copiado de texto entre ventanas	113
Ejercicio de laboratorio: Crear, visualizar y editar archivos de texto	116
5. Administración de usuarios y grupos de Linux local	125
Usuarios y Grupos	126
Práctica: Conceptos de usuario y grupo	129
Obtención de acceso de superusuario	131
Práctica: Ejecución de comandos como usuario root	135

Red Hat System Administration I

Administración de cuentas de usuarios locales	138
Práctica: Creación de usuarios usando herramientas de la línea de comandos	141
Administración de cuentas de grupos locales	143
Práctica: Administración de grupos utilizando herramientas de línea de comandos	145
Administración de contraseñas de usuarios	147
Práctica: Administración de la antigüedad de la contraseña de usuario	151
Ejercicio de laboratorio: Administración de usuarios y grupos locales de Linux	153
6. Control de acceso a archivos con permisos del sistema de archivos Linux	157
Permisos del sistema de archivos Linux	158
Práctica: Interpretación de permisos de archivos y directorios	162
Administración de permisos del sistema de archivos desde la línea de comandos	164
Práctica: Administrar la seguridad de los archivos desde la línea de comandos	168
Administración de permisos predeterminados y acceso a archivos	170
Práctica: Control de permisos y propiedad de archivos nuevos	175
Ejercicio de laboratorio: Control de acceso a archivos con permisos del sistema de archivos Linux	177
7. Administración y control de procesos Linux	181
Procesos	182
Práctica: Procesos	187
Control de trabajos	189
Práctica: Procesos de primer y segundo plano	192
Finalización de procesos	195
Práctica: Finalización de procesos	200
Monitoreo de la actividad de procesos	202
Práctica: Control de la actividad de proceso	206
Ejercicio de laboratorio: Monitoreo y administración de procesos de Linux	208
8. Control de servicios y demonios	215
Identificación de procesos del sistema comenzados en forma automática	216
Práctica: Identificar el estado de unidades systemd	220
Control de servicios del sistema	222
Práctica: Uso de systemctl para administrar servicios	226
Ejercicio de laboratorio: Control de servicios y demonios	228
9. Configuración y protección del servicio OpenSSH	231
Acceso a la línea de comandos remota con SSH	232
Práctica: Acceso remoto a la línea de comandos	235
Configuración de autenticación basada en llaves SSH	237
Práctica: Uso de la autenticación mediante claves SSH	239
Personalización de la configuración del servicio SSH	240
Práctica: Restricción de inicios de sesión en SSH	242
Ejercicio de laboratorio: Configuración y protección del servicio OpenSSH	245
10. Análisis y almacenamiento de registros	249
Arquitectura de registro del sistema	250
Práctica: Componentes de registro de sistema	252
Revisión de archivos Syslog	255
Práctica: Encontrar entradas de registro	259
Revisión de las entradas del journal de systemd	261
Práctica: búsqueda de eventos con journalctl	264
Preservando el journal de systemd	265

Práctica: Configuración del journal de systemd constante	267
Mantenimiento de la hora correcta	268
Práctica: Ajuste de la hora del sistema	272
Ejercicio de laboratorio: Análisis y almacenamiento de registros	275
11. Administración de la red de Red Hat Enterprise Linux	279
Conceptos de red	280
Práctica: Conceptos de red	286
Validación de la configuración de red	289
Práctica: Cómo examinar la configuración de red	292
Configuración de red con nmcli	294
Práctica: Configuración de red con nmcli	299
Edición de archivos de configuración de red	302
Práctica: Edición de archivos de configuración de red	304
Configuración de nombres de host y resolución de nombre	306
Práctica: Configuración de nombres de hosts y resolución de nombres	309
Ejercicio de laboratorio: Administración de la red de Red Hat Enterprise Linux	312
12. Archivar y copiar archivos entre sistemas	317
Administración de archivos tar comprimidos	318
Práctica: Copia de seguridad y restauración de archivos a partir de un archivo tar	323
Copia segura de archivos entre sistemas	324
Práctica: Copia de archivos por medio de la red con scp	326
Sincronización de archivos entre sistemas en forma segura	327
Práctica: Sincronización segura de dos directorios con rsync	330
Trabajo de laboratorio: Archivado y copia de archivos entre sistemas	332
13. Instalación y actualización de paquetes de software	337
Adjuntar sistemas a las suscripciones para actualizaciones de software	338
Práctica: Administración de suscripciones de Red Hat	344
Paquetes de software RPM y yum	346
Práctica: Paquetes de software RPM	349
Administración de actualizaciones de software con yum	351
Práctica: Instalación y actualización de software con yum	358
Habilitación de repositorios de software yum	362
Práctica: Habilitar repositorios de software	365
Análisis de los archivos del paquete RPM	367
Práctica: Trabajar con los archivos de paquete del RPM	371
Ejercicio de laboratorio: Instalación y actualización de paquetes de software	373
14. Acceso a los sistemas de archivos de Linux	377
Identificación de dispositivos y sistemas de archivos	378
Práctica: Identificación de los dispositivos y sistemas de archivos	381
Montaje y desmontaje de sistemas de archivos	383
Práctica: Montar y desmontar sistemas de archivos	386
Creación de enlaces entre archivos	388
Práctica: Creación de enlaces entre archivos	390
Localización de archivos en el sistema	391
Práctica: Búsqueda de archivos en el sistema	398
Ejercicio de laboratorio: Acceso a los sistemas de archivos de Linux	400
15. Uso de sistemas virtualizados	405
Administración de un host de virtualización local	406
Práctica: Administración de un host de virtualización local	412

Red Hat System Administration I

Instalación de una máquina virtual nueva	414
Práctica: Instalación de una máquina virtual nueva	424
Prueba del capítulo: Uso de sistemas virtualizados	426
16. Revisión completa	431
Revisión integral de Red Hat System Administration I	432
Trabajo de laboratorio: Revisión integral	436

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.



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.



Referencias

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

Introducción

Red Hat System Administration I

Red Hat System Administration I (RH124) se diseñó para profesionales de TI sin experiencia previa en la administración de sistemas Linux. El curso tiene como objetivo proporcionar a los estudiantes "habilidades de supervivencia" para la administración de Linux y, para ello, se centra en tareas de administración básicas. En *Red Hat System Administration I* también se presentan los conceptos clave de línea de comandos y las herramientas de nivel empresarial a fin de ofrecerles una base a los estudiantes que planifiquen convertirse en administradores de sistemas Linux de tiempo completo. Estos conceptos se ampliarán en el siguiente curso: *Red Hat System Administration II* (RH134).

Objetivos del curso

- Obtener la habilidad suficiente para realizar las tareas principales de administración de sistemas en Red Hat Enterprise Linux.
- Desarrollar las habilidades necesarias para un administrador de sistemas Red Hat Enterprise Linux con certificación RHCSA.

Destinatarios

- Profesionales de TI que se dedican a diversas disciplinas y que necesitan realizar tareas de administración de Linux esenciales; entre ellas, instalación, establecimiento de conectividad de red, administración de almacenamiento físico y administración de seguridad básica.

Requisitos previos

- No hay requisitos previos formales para este curso; sin embargo, sería muy beneficioso contar con experiencia previa en administración de sistemas en otros sistemas operativos.

Introducción

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 desktopX.example.com y serverX.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
desktopX.example.com	172.25.X.10	Computadora "cliente" del estudiante
serverX.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 presionando **Super+Space** (en ocasiones denominado **Windows+Space**). También aparecerá un *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 "Bloq Mayús secundaria" y tecla de activación de teclas muertas para escribir caracteres adicionales. Asimismo, 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, presionando **Ctrl+Shift+U**, seguido por el código. Después de presionar **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 presionando **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



CAPÍTULO 1

ACCESO A LA LÍNEA DE COMANDOS

Descripción general	
Meta	Iniciar sesión en el sistema Linux y ejecutar comandos simples usando la shell.
Objetivos	<ul style="list-style-type: none">Utilizar la sintaxis de la shell Bash para ingresar comandos en una consola Linux.Iniciar aplicaciones en un entorno de escritorio GNOME.Utilizar funciones de Bash para ejecutar comandos desde un aviso de shell con menos pulsaciones de tecla.
Secciones	<ul style="list-style-type: none">Acceso a la línea de comandos a través de la consola local (y práctica)Acceso a la línea de comandos a través del escritorio (y práctica)Ejecución de comandos mediante la shell Bash (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">Acceso a la línea de comandos

Acceso a la línea de comandos a través de la consola local

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder iniciar sesión en un sistema Linux en una consola de texto local y ejecutar comandos simples a través de la shell.

La shell bash

Una *línea de comandos* es una interfaz basada en texto que puede utilizarse para introducir instrucciones en un sistema informático. Un programa denominado shell proporciona la línea de comandos de *Linux*. Durante la larga historia de los sistemas tipo UNIX, se han desarrollado muchos intérpretes de comandos. La shell predeterminada para los usuarios en Red Hat Enterprise Linux es **GNU Bourne-Again Shell (bash)**. Bash es una versión mejorada de uno de los shells más exitosos que se utiliza en los sistemas tipo UNIX: la **Bourne Shell (sh)**.

Si una shell se utiliza de manera interactiva, muestra una cadena cuando espera un comando del usuario. Esto se denomina *aviso de shell*. Cuando un usuario regular inicia una shell, el aviso predeterminado finaliza con un carácter \$.

```
[student@desktopX ~]$
```

El carácter \$ reemplaza el carácter # si la shell se está ejecutando como el superusuario **root**. Con esto, resulta más evidente que se trata de una shell de superusuario, lo que permite evitar accidentes y errores en la cuenta con privilegios.

```
[root@desktopX ~]#
```

El uso de **bash** para ejecutar comandos puede ser eficaz. La shell **bash** proporciona un lenguaje de secuencia de comandos capaz de admitir la automatización de tareas. La shell tiene capacidades adicionales que pueden simplificar operaciones o posibilitar aquellas que son difíciles de realizar con herramientas gráficas.



nota

La shell **bash** es similar en concepto al intérprete de la línea de comandos disponible en versiones recientes de Microsoft Windows **cmd .exe**, pero **bash** posee un lenguaje de secuencia de comando más sofisticado. También es similar a Windows PowerShell en Windows 7 y Windows Server 2008 R2. A los administradores de Mac OS X que utilizan la utilidad **Terminal** de Macintosh les agradará saber que **bash** es la shell predeterminada en Mac OS X.

Consolas virtuales

Los usuarios acceden a la shell **bash** a través de una *terminal*. Un terminal proporciona un teclado para las entradas del usuario y una pantalla para las salidas. En instalaciones basadas

en texto, esta puede ser la *consola física* del equipo Linux, el teclado de hardware y la pantalla. El acceso al terminal también puede configurarse a través de puertos en serie.

Otra forma de acceder a una shell es desde una *consola virtual*. La consola física de una máquina con Linux admite múltiples consolas virtuales que funcionan como terminales independientes. Cada consola virtual admite un inicio de sesión independiente.

Si el entorno gráfico se encuentra activado, se ejecutará en la *primera* consola virtual en Red Hat Enterprise Linux 7. Se dispone de cinco avisos de inicio de sesión de texto adicionales en las consolas de la dos a la seis (o de la consola uno a la cinco si el entorno gráfico está desactivado). Cuando se esté ejecutando un entorno gráfico, presione **Ctrl+Alt** y presione una tecla de función (de **F2** a **F6**) para acceder a un aviso de inicio de sesión de texto en una consola virtual. Presione **Ctrl+Alt+F1** para regresar a la primera consola virtual y al escritorio gráfico.



Importante

En las imágenes virtuales preconfiguradas proporcionadas por Red Hat, se han deshabilitado los avisos de inicio de sesión en las consolas virtuales.



nota

En Red Hat Enterprise Linux 5 y en versiones anteriores, las primeras *seis* consolas virtuales proporcionaron siempre avisos de inicio de sesión de texto. Cuando se inició el entorno gráfico, se ejecutó en la consola virtual siete (a la que se accede a través **Ctrl+Alt+F7**).

Conceptos básicos de la shell

Los comandos ingresados en el aviso de shell están compuestos por tres partes básicas:

- *Comando* para ejecutar
- *Opciones* para ajustar el comportamiento del comando
- *Argumentos*, que generalmente son destinos del comando

El *comando* es el nombre del programa que se ejecuta. Puede estar seguido de una o más *opciones*, que ajustan el comportamiento del comando o lo que hará. Las opciones generalmente comienzan con uno o dos guiones (**-a** o **--all**, por ejemplo) para que se distingan de los argumentos. Los comandos también pueden estar seguidos de uno o más *argumentos*, que a menudo indican un objetivo en el cual el comando debe funcionar.

Por ejemplo, la línea de comandos **usermod -L morgan** tiene un comando (**usermod**), una opción (**-L**) y un argumento (**morgan**). El efecto de este comando es bloquear la contraseña de la cuenta del usuario morgan.

Para usar un comando de manera eficiente, el usuario debe conocer las opciones y los argumentos que acepta, así como el orden en el que espera que se introduzcan (la *sintaxis* del comando). La mayoría de los comandos tiene una opción **--help**. Esto hace que el comando imprima una descripción de su función, es decir, una "declaración de uso" que detalla la sintaxis del comando y una lista de las opciones que acepta y sus funciones.

Capítulo 1. Acceso a la línea de comandos

Es posible que la lectura de las declaraciones de uso sea una tarea complicada. Se tornan mucho más simples de comprender una vez que el usuario está familiarizado con algunas convenciones básicas:

- Los corchetes, [], comprenden elementos opcionales.
- Todo lo que vaya seguido de . . . representa una lista con longitud arbitraria de elementos de ese tipo.
- Cuando hay múltiples elementos separados por tuberías, |, solo *uno* de ellos puede especificarse.
- El texto incluido entre corchetes angulares, <>, representa datos variables. Por ejemplo, <filename> significa “inserte aquí el nombre de archivo que desee usar”. En ocasiones, estas variables simplemente se escriben con mayúsculas (por ejemplo, FILENAME).

Tenga en cuenta la primera declaración de uso para el comando **date**:

```
[student@desktopX ~]$ date --help
date [OPTION]... [+FORMAT]
```

Indica que **date** puede aceptar una lista opcional de opciones ([OPTION] . . .), seguida de una cadena de formato opcional y precedida por el signo "más", +, que describe cómo debe mostrarse la fecha actual ([+FORMAT]). Puesto que ambas elecciones son opcionales, **date** funcionará aunque no se hayan especificado las opciones o los argumentos (imprimirá la fecha y hora actuales con su formato predeterminado).



nota

La página **man** para un comando tiene una sección SINOPSIS que proporciona información sobre la sintaxis del comando. La página de manual **man-pages(7)** describe cómo interpretar los corchetes, las barras verticales, etc. que los usuarios ven en la SINOPSIS o en un mensaje de uso.

Cuando un usuario termina de usar la shell y desea salir, la sesión puede finalizarse de distintas maneras. El comando **exit** finaliza la sesión de la shell actual. Otra forma de finalizar una sesión es presionando **Ctrl+d**.



Referencias

Páginas del manual **intro(1)**, **bash(1)**, **consola(4)**, **pts(4)** y **man-pages(7)**

Nota: Algunos detalles de la página de manual de la consola(4) que incluyen init(8) e inittab(5) son obsoletos.

Práctica: Terminales de acceso a la consola local

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

Argumento	Comando	Consola física	Consola virtual
Opción	Petición	Shell	Terminal

Descripción	Término
El intérprete que ejecuta los comandos escritos como secuencias.	
La indicación visual que muestra que una shell interactiva todavía espera a que el usuario escriba un comando.	
El nombre de un programa que se ejecutará.	
La parte de la línea de comandos que modifica el comportamiento de un comando.	
La parte de la línea de comando que especifica el destino donde debe operar el comando.	
El teclado y la pantalla de hardware que se usan para interactuar con un sistema.	

Descripción	Término
Cada una de las distintas consolas lógicas que puede admitir un inicio de sesión independiente.	
Una interfaz que proporciona una pantalla de salida y un teclado para ingresar en una sesión de shell.	

Solución

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

Descripción	Término
El intérprete que ejecuta los comandos escritos como secuencias.	Shell
La indicación visual que muestra que una shell interactiva todavía espera a que el usuario escriba un comando.	Petición
El nombre de un programa que se ejecutará.	Comando
La parte de la línea de comandos que modifica el comportamiento de un comando.	Opción
La parte de la línea de comando que especifica el destino donde debe operar el comando.	Argumento
El teclado y la pantalla de hardware que se usan para interactuar con un sistema.	Consola física
Cada una de las distintas consolas lógicas que puede admitir un inicio de sesión independiente.	Consola virtual
Una interfaz que proporciona una pantalla de salida y un teclado para ingresar en una sesión de shell.	Terminal

Acceso a la línea de comandos con el escritorio

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder iniciar sesión en el sistema Linux usando el entorno de escritorio GNOME 3 para ejecutar comandos desde un aviso de shell en un programa de terminal.

Entorno de escritorio de GNOME

El *entorno de escritorio* es la interfaz de usuario gráfica en un sistema Linux. El entorno de escritorio predeterminado en Red Hat Enterprise Linux 7 se proporciona mediante **GNOME 3**. Este proporciona un escritorio integrado para usuarios y una plataforma de desarrollo unificada en la parte superior de una estructura gráfica proporcionada por el **Sistema X Window**.

GNOME Shell proporciona las funciones principales de la interfaz de usuario para el entorno de escritorio GNOME. La aplicación **gnome-shell** es muy personalizable. De forma predeterminada, los usuarios de RHEL 7 usan el tema "GNOME Classic" para **gnome-shell**, que es similar al entorno de escritorio GNOME 2. Otra opción disponible es el tema "moderno" GNOME 3 usado por el proyecto de base GNOME. Cualquier tema se puede seleccionar persistentemente en el inicio de sesión al seleccionar el ícono de engranaje junto al botón **Sign In** cuando se ingresa la contraseña del usuario.

La primera vez que un usuario inicia sesión, se ejecuta un programa de configuración inicial para ayudar a configurar parámetros de cuenta básicos. Luego, se inicia la aplicación **GNOME Help** en la pantalla **Getting Started with GNOME**. En esta pantalla, se incluyen videos y documentación para ayudar a orientar a nuevos usuarios en el entorno de GNOME 3.

GNOME Help se puede iniciar rápidamente al presionar **F1** en **gnome-shell**, al seleccionar **Applications > Documentation > Help**, o al ejecutar el comando **yelp**.

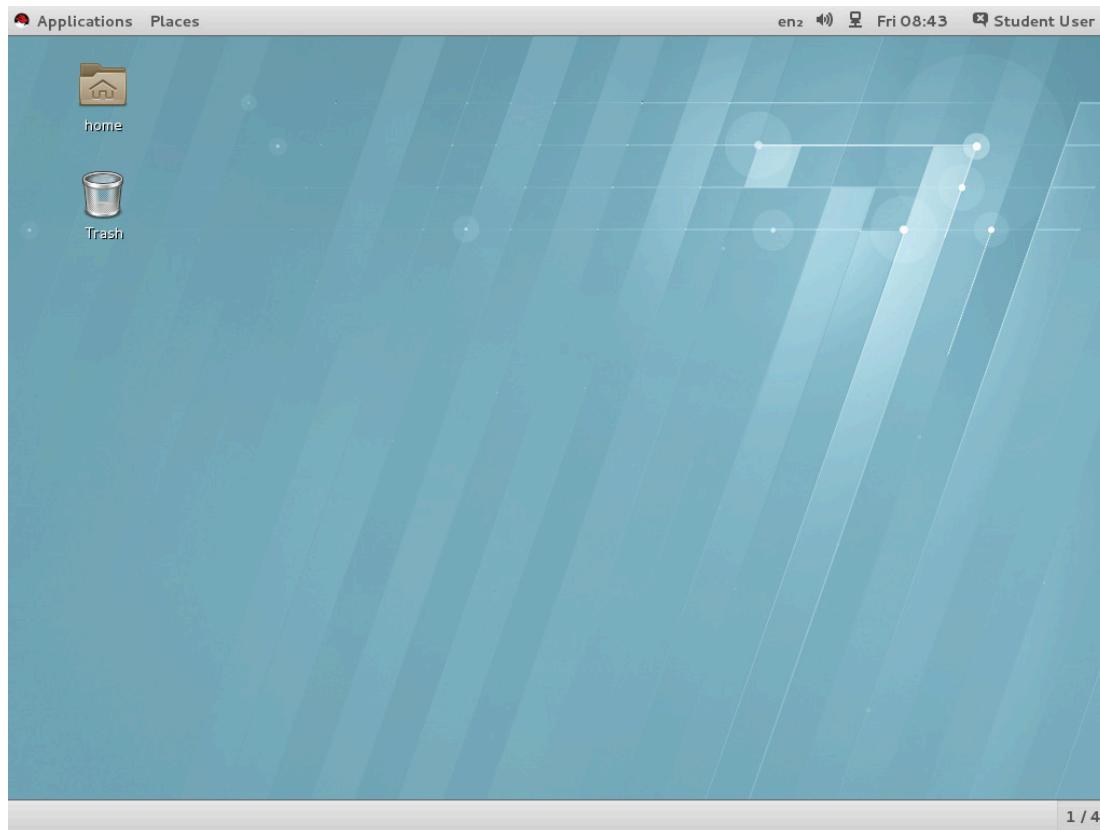


Figura 1.1: Un escritorio de GNOME 3 vacío

Partes de la shell de GNOME

Las diversas partes de la shell de GNOME tienen nombres y propósitos específicos. Estas partes incluyen lo siguiente:

- **barra superior:** La barra que se ejecuta en toda la parte superior de la pantalla. La barra superior proporciona los menús **Applications** y **Places** y controles para el volumen, redes, acceso al calendario, y para seleccionar entre los métodos de entrada del teclado (si hay más de uno configurado). En el menú del nombre del usuario, hay opciones para ajustar los parámetros de la cuenta, bloquear la pantalla, cambiar usuarios, cerrar la sesión del sistema o apagarlo.
- **Menú Applications:** Este menú en la barra superior proporciona una manera de iniciar aplicaciones, categorizadas en submenús. La sección **Activities Overview** también se puede iniciar desde este menú.
- **Menú Places:** Este menú a la derecha del menú **Applications** proporciona un acceso rápido a través de un administrador gráfico de archivos a menús importantes en el directorio de inicio del usuario, a /, y a exportaciones y archivos compartidos de la red.
- **lista de ventanas:** La barra que se ejecuta en toda la parte inferior de la pantalla. La lista de ventanas proporciona una manera fácil de acceder a todas las ventanas del espacio de trabajo actual, así como de minimizarlas y restaurarlas. En la esquina derecha, hay un indicador que informa al usuario en qué espacio de trabajo está y cuántos están disponibles.

Capítulo 1. Acceso a la línea de comandos

- **bandeja de mensajes:** La bandeja de mensajes proporciona una manera de revisar notificaciones enviadas mediante aplicaciones o componentes del sistema a GNOME. Si ocurre una notificación, normalmente esta aparece primero brevemente como una sola línea en la parte inferior de la pantalla, y aparece un indicador persistente en la esquina inferior derecha para informar al usuario la cantidad de notificaciones recibidas recientemente. Se puede abrir la bandeja de mensajes para revisar estas notificaciones al hacer clic en el indicador o al presionar **Super+m**. La tecla Super (a veces, denominada tecla Windows) se encuentra cerca de la esquina inferior izquierda de un teclado de 104/105 teclas de una PC IBM. La bandeja de mensajes se puede cerrar al presionar **Esc** o **Super+m** nuevamente.
- **Descripción general de actividades:** Este es un modo especial que ayuda a organizar ventanas e inicia aplicaciones. La sección Activities Overview se puede iniciar al seleccionar **Applications > Activities Overview**. Las tres áreas principales de Activities Overview son el **guión** a la izquierda de la pantalla, la **descripción general de ventanas** en el centro de la pantalla y el **selector de espacios de trabajo** a la derecha de la pantalla. Para salir de la sección Activities Overview, se puede presionar la tecla **Esc**.
- **guión** Esta es una lista configurable de iconos de las aplicaciones favoritas del usuario, aplicaciones que se están ejecutando actualmente, y un botón de **cuadrícula** que se puede usar para seleccionar aplicaciones de forma arbitraria. Las aplicaciones se pueden iniciar haciendo clic en uno de los íconos o al usar el botón de cuadrícula para buscar una aplicación que se usa con menos frecuencia. Al guión también a veces se lo denomina **dock**.

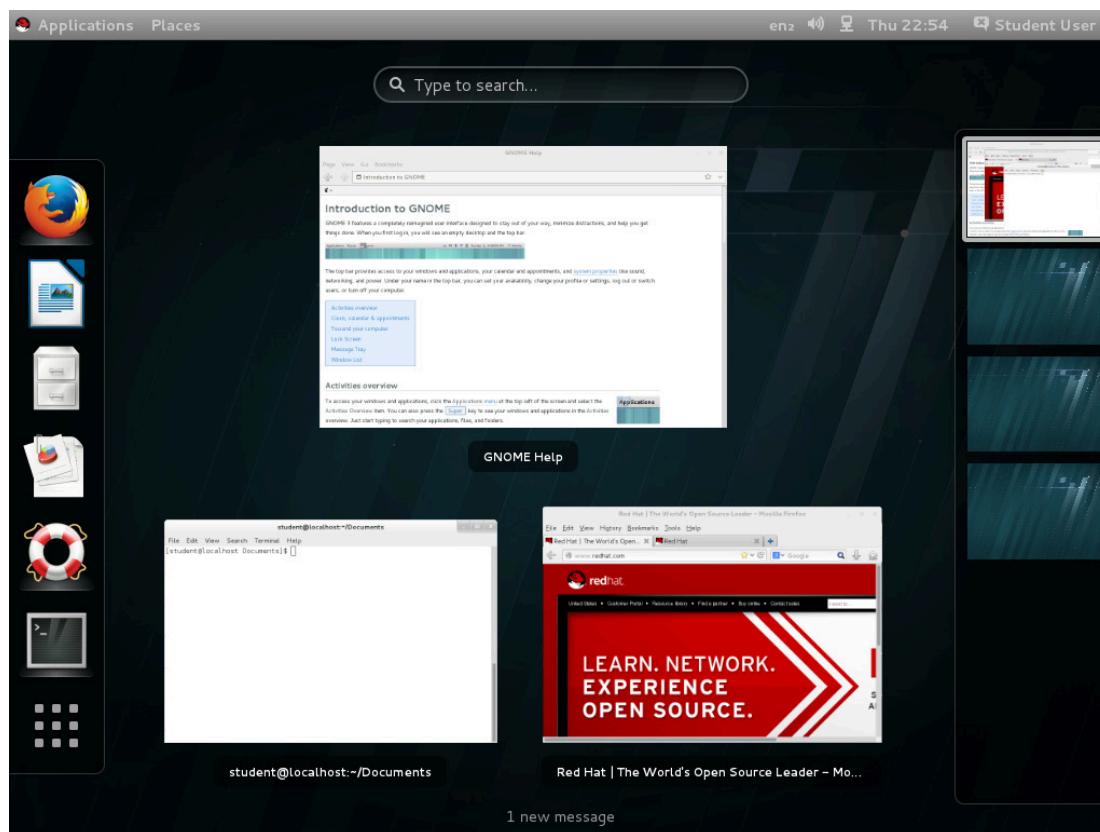


Figura 1.2: Sección Activities Overview de GNOME 3

Espacios de trabajo

Los espacios de trabajo son pantallas de escritorio por separado que tienen diferentes ventanas de aplicaciones. Se pueden utilizar para organizar el entorno de trabajo al agrupar las ventanas abiertas de la aplicación por tarea. Por ejemplo, las ventanas que se están usando para realizar una actividad de mantenimiento del sistema particular (como configurar un nuevo servidor remoto) se pueden agrupar en un espacio de trabajo, mientras que las aplicaciones de correo electrónico y otras aplicaciones de comunicación se pueden agrupar en otro espacio de trabajo.

Hay tres métodos para cambiar entre espacios de trabajo. Un método es hacer clic en el indicador que se encuentra en la esquina derecha de la lista de ventanas y seleccionar el espacio de trabajo deseado. Otro, tal vez el más rápido, es presionar **Ctrl+Alt+UpArrow** o **Ctrl+Alt+DownArrow** para cambiar entre espacios de trabajo de forma secuencial. Un tercer método es cambiar a **Activities Overview** y hacer clic en el espacio de trabajo deseado.

Una ventaja de usar la sección **Activities Overview** es que se puede hacer clic en las ventanas y arrastrarlas entre el espacio de trabajo actual y alguno de los otros mediante el uso del **selector de espacios de trabajo** en el lado derecho de la pantalla y la **descripción general de ventanas** en el centro de la pantalla.



nota

El uso de la combinación de teclas **Ctrl+Alt+UpArrow** o **Ctrl+Alt+DownArrow** para cambiar los espacios de trabajo no funciona en el entorno de aprendizaje virtual. En cambio, para cambiar de espacio de trabajo, se debe usar el applet del espacio de trabajo en el panel o **Activities Overview**.

Inicio de un terminal

Para obtener un aviso de shell en GNOME, inicie una aplicación de terminal gráfica como **GNOME Terminal**. Esto se puede realizar de varias maneras. A continuación, se detallan los tres métodos más comúnmente usados:

- Seleccione **Applications > Utilities > Terminal**.
- Haga clic derecho en un escritorio vacío o presione la tecla **Menú** y seleccione **Open in Terminal** en el menú de contexto que aparece.
- Desde la sección **Activities Overview**, seleccione **Terminal** desde el guión (ya sea desde el área de favoritos o al buscarla con el botón de cuadrícula [dentro de la agrupación **Utilities**] o el campo de búsqueda en la parte superior de la **descripción general de ventanas**).

Cuando se abre una ventana de terminal, se muestra un aviso de shell para el usuario que inició el programa de terminal gráfica. El aviso de shell y la barra de títulos de la ventana de terminal indicarán el nombre de usuario actual, el nombre del host y el directorio de trabajo.

Bloqueo de la ventana o cierre de sesión

El bloqueo de la ventana, o el cierre de sesión por completo, se puede realizar desde el menú del nombre del usuario bien a la derecha de la barra superior.

Para bloquear la ventana, seleccione **(User) > Lock** o presione **Ctrl+Alt+L**. La pantalla se bloqueará si la sesión gráfica está inactiva durante unos minutos.

Aparecerá una cortina de pantalla bloqueada que muestra el tiempo y el nombre del usuario que inició sesión. Para desbloquear la pantalla, presione **Enter** o **Space** para levantar la cortina de la pantalla bloqueada y, luego, ingrese la contraseña del usuario en la pantalla bloqueada.

Para cerrar sesión y finalizar la sesión gráfica actual, seleccione **(User) > Log Out** de la barra superior. Aparecerá una ventana de diálogo, que da la opción **Cancel** para cancelar el cierre de sesión en 60 segundos, o confirmar la acción **Log Out**.

Apagar o reiniciar el sistema

Para apagar el sistema, seleccione **(User) > Power Off** de la barra superior o presione **Ctrl+Alt+Del**. En el diálogo que aparece, el usuario puede elegir entre **Power Off** para apagar, **Restart** para reiniciar la máquina, o **Cancel** para cancelar la operación. Si no elige nada en este cuadro de diálogo, el sistema se apagará automáticamente después de 60 segundos.



Referencias

Ayuda de GNOME

- **yelp**

Ayuda de GNOME: *Introducción a GNOME*

- **yelp help:gnome-help/getting-started**

Práctica: Entorno de escritorio GNOME 3

En este trabajo de laboratorio, iniciará sesión como usuario regular a través del gestor de visualización gráfica para conocer el entorno de escritorio clásico de GNOME que ofrece GNOME 3.

Resultado:

Orientación básica sobre el entorno de escritorio GNOME 3

Andes de comenzar

Acceso a la pantalla de inicio de sesión gráfica de **desktopX.example.com**.



Importante

Hay dos máquinas virtuales disponibles para hacer ejercicios de laboratorio: una máquina de escritorio (de forma genérica denominada **desktopX**) y un servidor (de forma genérica denominado **serverX**).

Tenga cuidado de ver siempre qué máquina virtual se pide usar en un ejercicio.

Realice cada una de las siguientes tareas en su máquina **desktopX**.

1. Inicie sesión como **student** con la contraseña **student**.
 - 1.1. En la pantalla de inicio de sesión GNOME, haga clic en la cuenta de usuario **student**. Escriba **student** como contraseña cuando se le indique.
 - 1.2. Haga clic en **Sign In** una vez que haya escrito la contraseña.
2. Cambie la contraseña para **student** de **student** a **55TurnK3y**.
 - 2.1. La manera más simple de hacerlo es abriendo **GNOME Terminal** y usando el comando **passwd** en el aviso de la shell.

En el escritorio vacío, presione la tecla **Menú** o haga clic con el botón derecho del mouse para abrir el menú contextual.
 - 2.2. Seleccione **Open in Terminal**.
 - 2.3. En la ventana de terminal que aparece, escriba **passwd** en el aviso de la shell. Siga las instrucciones proporcionadas por el programa para cambiar la contraseña **student** de **student** a **55TurnK3y**.
3. Cierre sesión.
 - 3.1. Seleccione el elemento del menú **student > Log Out**.
 - 3.2. Haga clic en el botón **Log Out** en la ventana de confirmación que aparece.
4. Inicie sesión nuevamente como **student** con la nueva contraseña **55TurnK3y**.

Capítulo 1. Acceso a la línea de comandos

- 4.1. En la pantalla de inicio de sesión GNOME, haga clic en la cuenta de usuario **student**. Escriba **55TurnK3y** como contraseña cuando se le indique.
- 4.2. Haga clic en **Sign In** una vez que haya escrito la contraseña.
5. Determine cómo apagar **desktopX** desde la interfaz gráfica, pero haga clic en **Cancel** para cancelar la operación sin apagar el sistema.
 - 5.1. Seleccione el elemento del menú **student > Power Off**.
 - 5.2. Haga clic en el botón **Cancel** en la ventana de confirmación que aparece.

Ejecución de comandos con la shell Bash

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder ahorrar tiempo en la ejecución de comandos a partir de un aviso de shell con los accesos directos de Bash.

Sintaxis básica de comandos

GNU Bourne-Again Shell (**bash**) es un programa que interpreta comandos escritos por el usuario. Cada secuencia escrita en la shell puede tener un máximo de tres partes: el comando, las opciones (que comienzan con un - o --) y los argumentos. Cada palabra escrita en la shell está separada de las otras por espacios. Los comandos son nombres de programas que están instalados en el sistema. Cada comando tiene sus propias opciones y argumentos.

Cuando el usuario esté listo para ejecutar un comando, presiona la tecla **Enter**. Cada comando se escribe en una línea separada y el resultado de cada comando se muestra antes de que la shell muestre un aviso. Si un usuario quiere escribir más de un comando en una sola línea, puede usarse un punto y coma ; como separador de comando. Un punto y coma forma parte de una clase de caracteres denominados *metacaracteres*, que tienen significados especiales para **bash**.



nota

El comando **ps** puede aceptar opciones sin - o -. Este asunto será abordado en el Capítulo 7.

Ejemplos de comandos simples

El comando **date** se usa para mostrar la fecha y hora actuales. Además, puede ser usado por el superusuario para configurar el reloj del sistema. Un argumento que comienza con el signo más (+) especifica una secuencia de formato para el comando de fecha.

```
[student@desktopX ~]$ date
Sat Apr  5 08:13:50 PDT 2014
[student@desktopX ~]$ date +%R
08:13
[student@desktopX ~]$ date +%x
04/05/2014
```

El comando **passwd** cambia la contraseña propia del usuario. La contraseña original de la cuenta debe especificarse antes de que se permita un cambio. De manera predeterminada, **passwd** se configura para solicitar una contraseña más sólida, que esté compuesta por letras minúsculas, letras mayúsculas, números y símbolos, y que se base en una palabra del diccionario. El superusuario puede usar el comando **passwd** para cambiar las contraseñas de otros usuarios.

```
[student@desktopX ~]$ passwd
Changing password for user student.
Changing password for student.
(current) UNIX password: old_password
```

Capítulo 1. Acceso a la línea de comandos

```
New password: new_password
Retype new password: new_password
passwd: all authentication tokens updated successfully.
```

Linux no requiere de extensiones de nombre de archivo para clasificar los archivos por tipo. El comando **file** detecta el comienzo del contenido de un archivo y muestra qué tipo de archivo es. Los archivos que se clasificarán pasan como argumentos para el comando.

```
[student@desktopX ~]$ file /etc/passwd
/etc/passwd: ASCII text
[student@desktopX ~]$ file /bin/passwd
/bin/passwd: setuid ELF 64-bit LSB shared object, x86-64, version 1
(SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.32,
BuildID[sha1]=0x91a7160a019b7f5f754264d920e257522c5bce67, stripped
[student@desktopX ~]$ file /home
/home: directory
```

Los comandos **head** y **tail** muestran el comienzo y el final de un archivo, respectivamente. De manera predeterminada, estos comandos muestran 10 líneas, pero ambos tienen la opción **-n** que permite la especificación de una cantidad diferente de líneas. El archivo que se mostrará pasa como un argumento para estos comandos.

```
[student@desktopX ~]$ head /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
[student@desktopX ~]$ tail -n 3 /etc/passwd
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:993:991::/run/gnome-initial-setup/:/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
```

El comando **wc** cuenta líneas, palabras y caracteres en un archivo. Puede usar la opción **-l**, **-w** o **-c** para mostrar solo las líneas, las palabras o los caracteres, respectivamente.

```
[student@desktopX ~]$ wc /etc/passwd
39 70 2005 /etc/passwd
[student@desktopX ~]$ wc -l /etc/passwd ; wc -l /etc/group
39 /etc/passwd
63 /etc/group
[student@desktopX ~]$ wc -c /etc/group /etc/hosts
843 /etc/group
227 /etc/hosts
1070 total
```

Completar con el tabulador

Completar con el tabulador permite al usuario completar comandos o nombres de archivos rápidamente una vez que haya escrito lo suficiente en el aviso como para hacerlo único. Si los caracteres escritos no son únicos, al presionar la tecla **Tab** dos veces, aparecen todos los comandos que comienzan con los caracteres ya escritos.

```
[student@desktopX ~]$ pas<Tab><Tab>
passwd      paste      pasusponder
[student@desktopX ~]$ pass<Tab>
[student@desktopX ~]$ passwd
Changing password for user student.
Changing password for student.
(current) UNIX password:
```

La opción de completar con el tabulador puede usarse para completar nombres de archivo cuando se escriben como argumentos para comandos. Si se presiona la tecla **Tab**, completará el nombre del archivo tanto como pueda. Si se presiona la tecla **Tab** por segunda vez, provoca que la shell enumere todos los archivos que coinciden con el patrón actual. Escriba caracteres adicionales hasta que el nombre sea único; a continuación, use la opción de completar con el tabulador para finalizar la línea de comandos.

```
[student@desktopX ~]$ ls /etc/pas<Tab>
[student@desktopX ~]$ ls /etc/passwd<Tab>
passwd  passwd-
```

Con esta opción, se puede establecer una coincidencia entre argumentos y opciones para muchos comandos. El comando **useradd** es usado por el superusuario, el usuario **root**, para crear otros usuarios en el sistema. Tiene muchas opciones que pueden usarse para controlar el comportamiento del comando. Puede usarse la opción de completar con el tabulador después de una opción parcial para completar la opción sin necesidad de escribir mucho.

```
[root@desktopX ~]# useradd --<Tab><Tab>
--base-dir      --groups      --no-log-init      --shell
--comment      --help        --non-unique      --skel
--create-home   --home-dir    --no-user-group   --system
--defaults     --inactive    --password       --uid
--expiredate   --key         --root          --user-group
--gid          --no-create-home  --selinux-user
[root@desktopX ~]# useradd --
```

Comando history

El comando **history** muestra una lista de los comandos ejecutados anteriormente que tienen un número de comando como prefijo.

El signo de exclamación, **!**, es un metacaracter utilizado para ampliar comandos anteriores sin tener que escribirlos nuevamente. **!number** se amplía al comando que coincide con el número especificado. **!string** se amplía al comando más reciente que comienza con la cadena especificada.

```
[student@desktopX ~]$ history
...Output omitted...
23  clear
24  who
25  pwd
26  ls /etc
27  uptime
28  ls -l
29  date
30  history
[student@desktopX ~]$ !ls
ls -l
```

Capítulo 1. Acceso a la línea de comandos

```
total 0
drwxr-xr-x. 2 student student 6 Mar 29 21:16 Desktop
...Output omitted...
[student@desktopX ~]$ !26
ls /etc
abrt hosts pulse
adjtime hosts.allow purple
aliases hosts.deny qemu-ga
...Output omitted...
```

Las teclas de flecha pueden usarse para navegar por las líneas de comandos anteriores en el historial de la shell. La tecla **Up Arrow** edita el comando anterior en la lista de historial. La tecla **Down Arrow** edita el comando siguiente en la lista de historial. Use esta tecla cuando la tecla **Up Arrow** se haya presionado demasiada veces. Use las teclas **Left Arrow** y **Right Arrow** para mover el cursor hacia la izquierda y derecha en la línea de comandos actual que se está editando.

La combinación de teclas **Esc**+**.** provoca que la shell copie la última palabra del comando anterior en la línea de comandos actual donde está el cursor. Si se usa en forma reiterada, seguirá avanzando hasta los comandos anteriores.

Edición de línea de comandos

Cuando se usa en forma interactiva, **bash** tiene una función de edición de línea de comandos. Esto permite al usuario utilizar los comandos del editor de texto para desplazarse y modificar el comando actual que se está escribiendo. El uso de las teclas de flecha para moverse dentro del comando actual y pasar por el historial de comando se presentó anteriormente en esta sesión. En la siguiente tabla, se presentan comandos de edición más contundentes.

Accesos directos para la edición de línea de comandos

Acceso directo	Descripción
Ctrl+a	Ir al inicio de la línea de comandos.
Ctrl+e	Ir al final de la línea de comandos.
Ctrl+u	Borrar desde el cursor hasta el principio de la línea de comandos.
Ctrl+k	Borrar desde el cursor hasta el final de la línea de comandos.
Ctrl+Left Arrow	Ir al inicio de la palabra anterior en la línea de comandos.
Ctrl+Right Arrow	Ir al final de la palabra siguiente en la línea de comandos.
Ctrl+r	Buscar un patrón en la lista de historial de comandos.

Hay muchos otros comandos de edición de línea de comandos disponibles, pero estos son los más prácticos para usuarios principiantes. Los otros comandos están en la página de manual **bash(1)**.

Referencias

Páginas del manual: **bash(1)**, **date(1)**, **file(1)**, **head(1)**, **passwd(1)**, **tail(1)** y **wc(1)**

Práctica: comandos bash y atajos del teclado

Relacione los siguientes atajos de Bash con sus respectivas descripciones en la tabla.

!number	!string	;	Ctrl+Left Arrow	Ctrl+a
Ctrl+k	Esc+. 	Pestaña	history	

Descripción	Comando de la shell
Ir al inicio de la palabra anterior en la línea de comandos.	
Separar comandos en la misma línea.	
Borrar desde el cursor hasta el final de la línea de comandos.	
Volver a ejecutar un comando reciente mediante la coincidencia del nombre del comando.	
Atajo utilizado para completar comandos, nombres de archivos y opciones.	
Volver a ejecutar un comando específico en la lista del historial.	
Ir al inicio de la línea de comandos.	
Visualizar la lista de comandos anteriores.	

Descripción	Comando de la shell
Copiar el último argumento de los comandos anteriores.	

Solución

Relacione los siguientes atajos de Bash con sus respectivas descripciones en la tabla.

Descripción	Comando de la shell
Ir al inicio de la palabra anterior en la línea de comandos.	Ctrl+Left Arrow
Separar comandos en la misma línea.	;
Borrar desde el cursor hasta el final de la línea de comandos.	Ctrl+k
Volver a ejecutar un comando reciente mediante la coincidencia del nombre del comando.	!string
Atajo utilizado para completar comandos, nombres de archivos y opciones.	Pestaña
Volver a ejecutar un comando específico en la lista del historial.	!number
Ir al inicio de la línea de comandos.	Ctrl+a
Visualizar la lista de comandos anteriores.	history
Copiar el último argumento de los comandos anteriores.	Esc+.

Trabajo de laboratorio: Acceso a la línea de comandos

En este trabajo de laboratorio, usará la shell Bash para ejecutar comandos de manera eficiente con metacaracteres de la shell.

Recursos:
Archivos: /usr/bin/clean-binary-files

Resultados:

- Práctica del uso de las funciones de historial y edición de la línea de comandos de la shell para ejecutar comandos de manera eficiente con cambios menores.
- Cambie la contraseña del usuario **student** a **T3st1ngT1me**.
- Ejecute comandos utilizados para identificar tipos de archivos y visualizar partes de archivos de texto.

Andes de comenzar

Restablezca su sistema desktopX. Realice los siguientes pasos en desktopX.

- Inicie sesión en la pantalla de inicio de sesión gráfica del sistema **desktopX** como **student**.
- Abra una ventana de terminal en la que aparecerá un aviso de **bash**.
- Cambie la contraseña de **student** a **T3st1ngT1me**.
- Visualice la fecha y la hora actuales.
- Visualice la hora actual con el siguiente formato: HH:MM:SS A/PM Sugerencia: La cadena de formato que muestra el resultado es %r.
- ¿Qué tipo de archivo es **/usr/bin/clean-binary-files**? ¿Es legible por el ojo humano?
- Utilice el comando **wc** y los atajos de **bash** para visualizar el tamaño de **/usr/bin/clean-binary-files**.
- Visualice las primeras 10 líneas de **/usr/bin/clean-binary-files**.
- Visualice las últimas 10 líneas en la parte inferior del archivo **/usr/bin/clean-binary-files**.
- Repita el comando anterior, pero use la opción **-n 20** para visualizar las últimas 20 líneas del archivo. Utilice la edición de la línea de comandos para hacerlo con una cantidad mínima de teclas.
- Ejecute el comando **date** sin ningún argumento para visualizar la fecha y la hora actuales.
- Use el historial de **bash** para visualizar la hora solamente.

-
13. Termine la sesión con la shell de **bash**.

Capítulo 1. Acceso a la línea de comandos

Solución

En este trabajo de laboratorio, usará la shell Bash para ejecutar comandos de manera eficiente con metacaracteres de la shell.

Recursos:	
Archivos:	/usr/bin/clean-binary-files

Resultados:

- Práctica del uso de las funciones de historial y edición de la línea de comandos de la shell para ejecutar comandos de manera eficiente con cambios menores.
- Cambie la contraseña del usuario **student** a **T3st1ngT1me**.
- Ejecute comandos utilizados para identificar tipos de archivos y visualizar partes de archivos de texto.

Andes de comenzar

Restablezca su sistema desktopX. Realice los siguientes pasos en desktopX.

- Inicie sesión en la pantalla de inicio de sesión gráfica del sistema **desktopX** como **student**.
- Abra una ventana de terminal en la que aparecerá un aviso de **bash**.
Seleccione **Applications > Utilities > Terminal**.
- Cambie la contraseña de **student** a **T3st1ngT1me**.

Utilice el comando **passwd** para cambiar la contraseña. Asegúrese de proporcionar primero la contraseña original, **student**.

```
[student@desktopX ~]$ passwd
Changing password for user student.
Changing password for student.
(current) UNIX password: student
New password: T3st1ngT1me
Retype new password: T3st1ngT1me
passwd: all authentication tokens updated successfully.
```

- Visualice la fecha y la hora actuales.

```
[student@desktopX ~]$ date
Thu Apr  3 10:13:04 PDT 2014
```

- Visualice la hora actual con el siguiente formato: HH:MM:SS A/PM Sugerencia: La cadena de formato que muestra el resultado es **%r**.

Especifique el argumento **+%r** para **date**.

```
[student@desktopX ~]$ date +%
10:14:07 AM
```

6. ¿Qué tipo de archivo es **/usr/bin/clean-binary-files**? ¿Es legible por el ojo humano?

Utilice el comando **file** para determinar su tipo de archivo.

```
[student@desktopX ~]$ file /usr/bin/clean-binary-files
/usr/bin/clean-binary-files: POSIX shell script, ASCII text executable
```

7. Utilice el comando **wc** y los atajos de **bash** para visualizar el tamaño de **/usr/bin/clean-binary-files**.

El acceso directo más fácil de usar es **Esc+.** para volver a usar el argumento del comando anterior.

```
[student@desktopX ~]$ wc <Esc>.
[student@desktopX ~]$ wc /usr/bin/clean-binary-files
 594 1780 13220 /usr/bin/clean-binary-files
```

8. Visualice las primeras 10 líneas de **/usr/bin/clean-binary-files**.

El comando **head** muestra el inicio del archivo. ¿Volvió a usar el atajo de **bash**?

```
[student@desktopX ~]$ head <Esc>.
[student@desktopX ~]$ head /usr/bin/clean-binary-files
#!/bin/sh
#
# Script to clean binary files.
#
# JPackage Project <http://www.jpackage.org/>
#
# $Id: clean-binary-files,v 1.1 2006/09/19 19:39:37 fnasser Exp $
#
# Import java functions
[ -r "/usr/share/java-utils/java-functions" ] \
```

9. Visualice las últimas 10 líneas en la parte inferior del archivo **/usr/bin/clean-binary-files**.

Use el comando **tail**.

```
[student@desktopX ~]$ tail <Esc>.
[student@desktopX ~]$ tail /usr/bin/clean-binary-files
...Output omitted...
```

10. Repita el comando anterior, pero use la opción **-n 20** para visualizar las últimas 20 líneas del archivo. Utilice la edición de la línea de comandos para hacerlo con una cantidad mínima de teclas.

Up Arrow muestra el comando anterior. **Ctrl+a** mueve el cursor al inicio de la línea. **Ctrl+Right Arrow** avanza a la siguiente palabra; luego, añada la opción **-n 20** y presione **Enter** para ejecutar el comando.

```
[student@desktopX ~]$ tail -n 20 /usr/bin/clean-binary-files
```

Capítulo 1. Acceso a la línea de comandos

```
...Output omitted...
```

11. Ejecute el comando **date** sin ningún argumento para visualizar la fecha y la hora actuales.

```
[student@desktopX ~]$ date  
Thu Apr  3 10:48:30 PDT 2014
```

12. Use el historial de **bash** para visualizar la hora solamente.

Visualice la lista de comandos anteriores con el comando **history** para identificar el comando **date** que se ejecutará. Ejecute el comando con el comando histórico **!number**.

```
[student@desktopX ~]$ history  
...  
44  date +%r  
...  
[student@desktopX ~]$ !44  
date +%r  
10:49:56 AM
```

13. Termine la sesión con la shell de **bash**.

Use **exit** o la combinación de teclas **Ctrl+d** para cerrar la shell.

```
[student@desktopX ~]$ exit
```

Resumen

Acceso a la línea de comandos a través de la consola local

Uso de la consola física para ver comandos de entrada y salida con sintaxis correcta a través de la shell **bash**.

Acceso a la línea de comandos con el escritorio

Use el entorno gráfico de GNOME para iniciar aplicaciones, especialmente el programa de terminal gráfica.

Ejecución de comandos con la shell Bash

Use las funciones de completado con el tabulador, historial de comando y edición de línea de comandos de la shell Bash para ejecutar comandos de manera más eficiente.



CAPÍTULO 2

ADMINISTRACIÓN DE ARCHIVOS DESDE LA LÍNEA DE COMANDOS

Descripción general	
Meta	Copiar, mover, crear, eliminar y organizar archivos mientras se trabaja desde el aviso de la shell Bash.
Objetivos	<ul style="list-style-type: none">Identificar el objetivo de directorios importantes en un sistema Linux.Especificar archivos usando nombres de rutas absolutas y relativas.Crear, copiar, mover y quitar archivos y directorios usando utilidades de la línea de comandos.Hacer coincidir uno o más nombres de archivo con expansión de shell como argumentos de comandos de la shell.
Secciones	<ul style="list-style-type: none">Jerarquía del sistema de archivos Linux (y práctica)Búsqueda de archivos por nombre (y práctica)Administración de archivos con las herramientas de línea de comandos (y práctica)Coincidencia de nombres de archivo mediante el uso de expansión de nombre de ruta (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">Administración de archivos con expansión de shell

Jerarquía del sistema de archivos Linux

Objetivos

Tras finalizar esta sección, los estudiantes deberían entender el diseño y la organización fundamentales del sistema de archivos, y la ubicación de los tipos de archivo clave.

Jerarquía del sistema de archivos

Todos los archivos de un sistema Linux se guardan en sistemas de archivos que están organizados en un árbol de directorios *invertido* individual conocido como *jerarquía de sistema de archivos*. Este árbol está invertido porque se dice que la raíz del árbol está en la parte *superior* de la jerarquía y las ramas de los directorios y subdirectorios se extienden debajo de *root*.

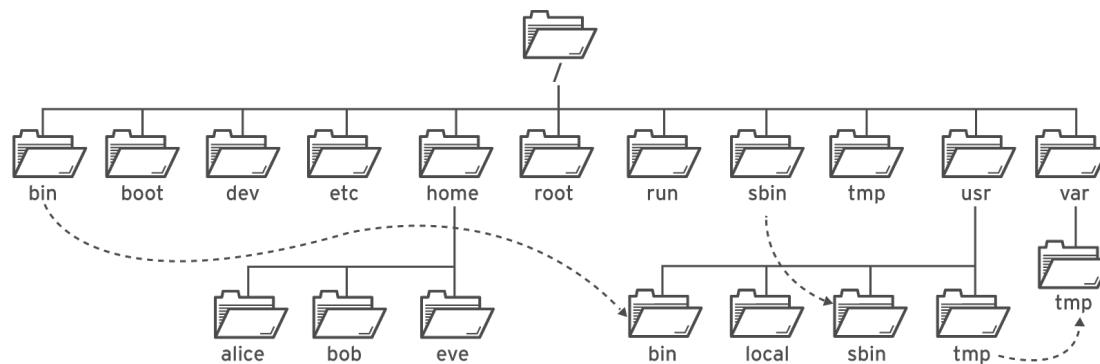


Figura 2.1: Directories del sistema de archivos importantes en Red Hat Enterprise Linux 7

El directorio `/` es el directorio raíz que está en la parte superior de la jerarquía del sistema de archivos. El carácter `/` también se usa como un *separador de directorio* en los nombres de archivo. Por ejemplo, si `etc` es un subdirectorio del directorio `/`, podemos llamar a ese directorio `/etc`. De la misma manera, si el directorio `/etc` contiene un archivo con el nombre `issue`, podemos referirnos a ese archivo como `/etc/issue`.

Los subdirectorios de `/` se usan con fines estandarizados para organizar archivos por tipo y objetivo. Esto facilita la posibilidad de encontrar archivos. Por ejemplo, en el directorio raíz, el subdirectorio `/boot` se usa para guardar archivos que se necesitan para arrancar el sistema.



nota

Los siguientes términos se encuentran en la descripción de los contenidos del directorio del sistema de archivos:

- *estático* es el contenido que no se modifica hasta que se edita o se reconfigura en forma explícita.
- *dinámico* o *variable* es el contenido que, por lo general, se modifica o se adjunta mediante procesos activos.
- *persistentes* es el contenido, en particular, los parámetros de configuración, que se mantiene después de un arranque nuevo.
- *tiempo de ejecución* es el contenido específico de un proceso o sistema o los atributos borrados durante un arranque nuevo.

La siguiente tabla enumera algunos de los directorios más importantes del sistema por nombre y objetivo.

Directarios Red Hat Enterprise Linux importantes

Ubicación	Propósito
/usr	Software instalado, bibliotecas compartidas, incluye archivos y datos de programa estáticos de solo lectura. Los subdirectorios importantes incluyen: <ul style="list-style-type: none"> - /usr/bin: Comandos del usuario. - /usr/sbin: Comandos de administración del sistema. - /usr/local: Software personalizado en forma local.
/etc	Archivos de configuración específicos para este sistema.
/var	Datos variables específicos de este sistema que deberían conservarse entre los arranques. Los archivos que cambian en forma dinámica (por ejemplo, bases de datos, directorios caché, archivos de registro, documentos en cola de impresión y contenido de sitio web) pueden encontrarse en /var.
/run	Datos de tiempo de ejecución para procesos que se iniciaron desde el último arranque. Esto incluye archivos de ID de proceso y archivos de bloqueo, entre otros elementos. El contenido de este directorio se vuelve a crear en el arranque nuevo. (Este directorio consolida /var/run y /var/lock de versiones anteriores de Red Hat Enterprise Linux).
/home	Los directorios de inicio son aquellos donde los usuarios habituales guardan sus datos personales y los archivos de configuración.
/root	Es el directorio de inicio para el superusuario administrativo, root.
/tmp	Es un espacio con capacidad de escritura para archivos temporales. Los archivos a los que no se haya accedido, y que no se hayan cambiado ni modificado durante 10 días se eliminan de este directorio automáticamente. Existe otro directorio temporal, /var/tmp, en el que los archivos que no tuvieron acceso, cambios ni modificaciones durante más de 30 días se eliminan automáticamente.
/boot	Son los archivos necesarios para iniciar el proceso de arranque.

Ubicación	Propósito
/dev	Contiene <i>archivos de dispositivo</i> especiales que son usados por el sistema para acceder al hardware.



Importante

En Red Hat Enterprise Linux 7, cuatro directorios antiguos en / ahora tienen contenido idéntico al de sus equivalentes que están en /usr:

- /bin y /usr/bin.
- /sbin y /usr/sbin.
- /lib y /usr/lib.
- /lib64 y /usr/lib64.

En versiones anteriores de Red Hat Enterprise Linux, estos eran directorios distintos que contenían diferentes conjuntos de archivos. En RHEL 7, los directorios de / son enlaces simbólicos para los directorios coincidentes de /usr.



Referencias

Página del manual: **hier(7)**

Estándar de jerarquía del sistema de archivos
<http://www.pathname.com/fhs>

Práctica: Jerarquía de sistemas de archivos

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

/	/etc	/home	/root	/run	/tmp	/usr
/usr/bin	/usr/sbin	/var				

Objetivo del directorio	Ubicación
Este directorio contiene datos de configuración del sistema estáticos y persistentes.	
Este es el directorio root del sistema.	
En este directorio se incluyen los directorios de inicio del usuario.	
Este es el directorio de inicio de la cuenta root.	
Este directorio contiene datos de configuración dinámicos, como FTP y sitios web.	
Aquí se ubican utilidades y comandos de usuario regular.	
Aquí se incluyen binarios de administración de sistemas para uso por parte de root.	
Aquí se almacenan los archivos temporales.	

Objetivo del directorio	Ubicación
Contiene datos dinámicos y no persistentes de tiempo de ejecución de aplicaciones.	
Contiene las bibliotecas y los programas de software instalados.	

Solución

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

Objetivo del directorio	Ubicación
Este directorio contiene datos de configuración del sistema estáticos y persistentes.	/etc
Este es el directorio root del sistema.	/
En este directorio se incluyen los directorios de inicio del usuario.	/home
Este es el directorio de inicio de la cuenta root.	/root
Este directorio contiene datos de configuración dinámicos, como FTP y sitios web.	/var
Aquí se ubican utilidades y comandos de usuario regular.	/usr/bin
Aquí se incluyen binarios de administración de sistemas para uso por parte de root.	/usr/sbin
Aquí se almacenan los archivos temporales.	/tmp
Contiene datos dinámicos y no persistentes de tiempo de ejecución de aplicaciones.	/run
Contiene las bibliotecas y los programas de software instalados.	/usr

Ubicación de archivos por nombre

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder usar en forma correcta los nombres de ruta, cambiar el directorio que está en uso y utilizar comandos para determinar los contenidos y las ubicaciones del directorio.

Rutas absolutas y relativas

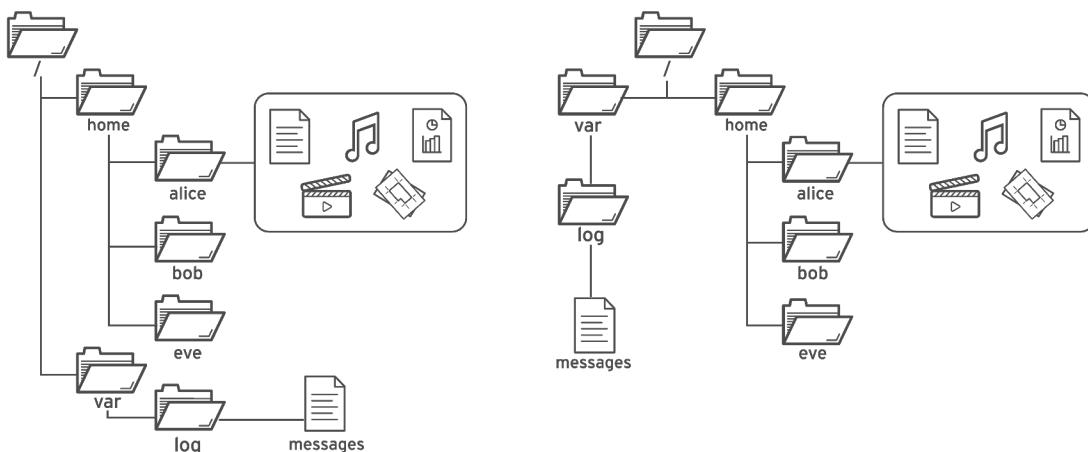


Figura 2.2: La vista del explorador de archivos habitual (izquierda) equivale a la vista descendente (derecha).

La *ruta* de un archivo o directorio especifica su ubicación exclusiva en el sistema de archivos. Si se sigue la ruta de un archivo, pasa por uno o más subdirectorios con nombre que están delimitados por una barra (/) hasta que se llega al destino. Las definiciones del comportamiento de archivos estándar rigen para los directorios (también denominados *carpetas*) al igual que con otros tipos de archivos.



Importante

Si bien un **espacio** es un carácter aceptable en los nombres de archivo de Linux, no es un delimitador usado por la shell para la interpretación de la sintaxis de comandos. Se recomienda a los administradores nuevos que eviten el uso de espacios en los nombres de archivos ya que aquellos que incluyan espacios, con frecuencia, generan comportamientos de ejecución de comandos no deseados.

Rutas absolutas

Una *ruta absoluta* es un nombre *completamente calificado* que comienza en el directorio (/) raíz y especifica cada subdirectorio que se atraviesa para llegar y que representa en forma exclusiva un solo archivo. Cada archivo del sistema de archivos tiene un único nombre de ruta absoluta, reconocido con una regla simple: un nombre de archivo con una barra (/) como primer carácter es el nombre de la ruta absoluta. Por ejemplo, el nombre de ruta absoluta para el archivo de registro de mensajes del sistema es **/var/log/messages**. Los nombres de rutas absolutas pueden ser extensos para escribir; en consecuencia, los archivos también pueden ubicarse *en forma relativa*.

Cuando un usuario inicia sesión y abre una ventana de comandos, la ubicación inicial es, por lo general, el directorio de inicio del usuario. Los procesos del sistema también tienen un directorio inicial. Los usuarios y procesos navegan a otros directorios según sea necesario; los términos *Directorio de trabajo* o *Directorio de trabajo actual* se refieren a la ubicación *actual*.

Rutas relativas

Al igual que una ruta absoluta, una *ruta relativa* identifica un archivo único y especifica solo la ruta necesaria para llegar al archivo desde el directorio de trabajo. Para reconocer nombres de ruta relativos, se sigue una regla simple: un nombre de ruta que no tenga *otro carácter más que una barra (/)* como primer carácter es un nombre de ruta relativo. Un usuario en el directorio **/var** podría referirse en forma relativa al archivo de registro del mensaje como **log/messages**.

Para sistemas de archivos Linux estándares, el nombre de ruta de un archivo, que incluya todos los caracteres / no puede tener más de 4095 bytes. Cada componente del nombre de la ruta separado por caracteres / no puede tener más de 255 bytes. Los nombres de archivo pueden usar cualquier carácter Unicode codificado UTF-8, excepto / y el carácter **NUL**. (Los caracteres ASCII requieren de un byte; otros caracteres, como los latinos, griegos, hebreos o cirílicos, necesitan de dos bytes; el resto de los caracteres del plano multilingüe básico de Unicode necesitan tres; y ningún carácter requerirá más de cuatro bytes).

Los sistemas de archivo Linux, que incluyen, entre otros, ext4, XFS, BTRFS, GFS2 y GlusterFS, distinguen entre letras minúsculas y mayúsculas. Si se crea un archivo **FileCase.txt** y un archivo **filecase.txt** en el mismo directorio, se obtienen dos archivos exclusivos. A pesar de que muchos sistemas de archivos que no son Linux son admitidos por Linux, cada uno tiene reglas de nombramiento de archivos exclusivas. Por ejemplo, el sistema de archivos VFAT masivo no distingue entre minúsculas y mayúsculas, y permite la creación solo de uno de los dos archivos de ejemplo. Sin embargo, VFAT, junto con NTFS de Microsoft y HFS + de Apple, tiene un comportamiento de *conservación de tipo de letra*. A pesar de que estos sistemas de archivos *no* distinguen entre minúsculas y mayúsculas (realizado, principalmente, para respaldar la compatibilidad retroactiva), muestran los nombres de archivo con el uso de mayúsculas original utilizado cuando se creó el archivo.

Rutas de navegación

El comando **pwd** muestra el nombre de ruta completo de la ubicación actual, que ayuda a determinar la sintaxis adecuada para llegar a los archivos con los nombres de ruta relativos. El comando **ls** enumera el contenido del directorio para el directorio especificado o, si no se indica un directorio, el directorio actual.

```
[student@desktopX ~]$ pwd
/home/student
[student@desktopX ~]$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[student@desktopX ~]$
```

Use el comando **cd** para cambiar los directorios. En caso del directorio de trabajo de **/home/student**, la sintaxis de ruta relativa es más corta para llegar al subdirectorio **Videos**. A continuación, se llega al subdirectorio **Documents** con la sintaxis de ruta absoluta.

```
[student@desktopX ~]$ cd Videos
[student@desktopX Videos]$ pwd
/home/student/Videos
[student@desktopX Videos]$ cd /home/student/Documents
```

Capítulo 2. Administración de archivos desde la línea de comandos

```
[student@desktopX Documents]$ pwd
/home/student/Documents
[student@desktopX Documents]$ cd
[student@desktopX ~]$ pwd
/home/student
[student@desktopX ~]$
```

La petición del programa de shell muestra, para ser breve, solo el último componente de la ruta de directorio actual. Para **/home/student/Videos**, solo se muestra **Videos**. Cuando lo desee, regrese al directorio de inicio de usuario con **cd** sin especificar un destino. El aviso muestra el carácter *tilde* (~) cuando el directorio actual del usuario es su directorio de inicio.

Por lo general, el comando **touch** actualiza la marca de tiempo de un archivo con respecto a la fecha y hora actual sin modificarlo. Esto es útil para crear archivos vacíos, que pueden usarse para practicar, ya que si se "toca" el nombre de un archivo que no existe, se produce la creación del archivo. Si se usa **touch**, se crean archivos de práctica en los subdirectorios **Documents** y **Videos**.

```
[student@desktopX ~]$ touch Videos/blockbuster1.ogg
[student@desktopX ~]$ touch Videos/blockbuster2.ogg
[student@desktopX ~]$ touch Documents/thesis_chapter1.odf
[student@desktopX ~]$ touch Documents/thesis_chapter2.odf
[student@desktopX ~]$
```

El comando **ls** tiene varias opciones para mostrar los atributos en los archivos. Los más comunes y útiles son **-l** (formato de lista extenso), **-a** (todos los archivos, incluidos los archivos ocultos) y **-R** (recursivos, incluido el contenido de todos los subdirectorios).

```
[student@desktopX ~]$ ls -l
total 15
drwxr-xr-x. 2 student student 4096 Feb  7 14:02 Desktop
drwxr-xr-x. 2 student student 4096 Jan  9 15:00 Documents
drwxr-xr-x. 3 student student 4096 Jan  9 15:00 Downloads
drwxr-xr-x. 2 student student 4096 Jan  9 15:00 Music
drwxr-xr-x. 2 student student 4096 Jan  9 15:00 Pictures
drwxr-xr-x. 2 student student 4096 Jan  9 15:00 Public
drwxr-xr-x. 2 student student 4096 Jan  9 15:00 Templates
drwxr-xr-x. 2 student student 4096 Jan  9 15:00 Videos
[student@desktopX ~]$ ls -la
total 15
drwx----- 16 student student 4096 Feb  8 16:15 .
drwxr-xr-x.  6 root    root   4096 Feb  8 16:13 ..
-rw-----  1 student student 22664 Feb  8 00:37 .bash_history
-rw-r--r--.  1 student student   18 Jul  9 2013 .bash_logout
-rw-r--r--.  1 student student   176 Jul  9 2013 .bash_profile
-rw-r--r--.  1 student student   124 Jul  9 2013 .bashrc
drwxr-xr-x.  4 student student 4096 Jan 20 14:02 .cache
drwxr-xr-x.  8 student student 4096 Feb  5 11:45 .config
drwxr-xr-x.  2 student student 4096 Feb  7 14:02 Desktop
drwxr-xr-x.  2 student student 4096 Jan  9 15:00 Documents
drwxr-xr-x.  3 student student 4096 Jan 25 20:48 Downloads
drwxr-xr-x. 11 student student 4096 Feb  6 13:07 .gnome2
drwx-----  2 student student 4096 Jan 20 14:02 .gnome2_private
-rw-----  1 student student 15190 Feb  8 09:49 .ICEauthority
drwxr-xr-x.  3 student student 4096 Jan  9 15:00 .local
drwxr-xr-x.  2 student student 4096 Jan  9 15:00 Music
drwxr-xr-x.  2 student student 4096 Jan  9 15:00 Pictures
drwxr-xr-x.  2 student student 4096 Jan  9 15:00 Public
drwxr-xr-x.  2 student student 4096 Jan  9 15:00 Templates
```

```
drwxr-xr-x. 2 student student 4096 Jan  9 15:00 Videos
[student@desktopX ~]$
```

Los dos directorios especiales que están en la parte superior del listado se refieren al directorio actual (.) y el directorio *principal* (...). Estos directorios especiales existen en cada directorio del sistema. Sus beneficios serán aparentes cuando se practiquen los comandos de administración de archivos.



Importante

Los nombres de archivo que comienzan con un punto (.) indican archivos *ocultos* de la vista normal con **ls** y otros comandos. Esta *no* es una característica de seguridad. Los archivos ocultos evitan que los archivos de configuración necesarios del usuario llenen los directorios principales. Existen muchos comandos que procesan archivos ocultos solo con opciones de línea de comandos específicas y previenen que la configuración de un usuario se copie por accidente en otros directorios o usuarios.

Para proteger el *contenido* de un archivo y que no sea visualizado en forma inadecuada se necesitan *permisos de archivos*.

```
[student@desktopX ~]$ ls -R
.:
Desktop Documents Downloads Music Pictures Public Templates Videos
./Desktop:
./Documents:
thesis_chapter1.odf thesis_chapter2.odf
./Downloads:
./Music:
./Pictures:
./Public:
./Templates:
./Videos:
blockbuster1.ogg blockbuster2.ogg
[student@desktopX ~]$
```

El comando **cd** tiene muchas opciones. Muy pocas son tan útiles como para justificar que se practiquen por anticipado y se usen con cierta frecuencia. El comando **cd** - cambia el directorio al directorio donde estaba el usuario *antes* de estar en el directorio actual. Observe cómo este usuario aprovecha este comportamiento para alternar entre dos directorios; esta opción es práctica cuando se procesa una serie de tareas similares.

```
[student@desktopX ~]$ cd Videos
[student@desktopX Videos]$ pwd
/home/student/Videos
[student@desktopX Videos]$ cd /home/student/Documents
[student@desktopX Documents]$ pwd
/home/student/Documents
[student@desktopX Documents]$ cd -
```

```
[student@desktopX Videos]$ pwd  
/home/student/Videos  
[student@desktopX Videos]$ cd -  
[student@desktopX Documents]$ pwd  
/home/student/Documents  
[student@desktopX Documents]$ cd -  
[student@desktopX Videos]$ pwd  
/home/student/Videos  
[student@desktopX Videos]$ cd  
[student@desktopX ~]$
```

El comando **cd ..** utiliza el directorio oculto **..** para subir un nivel al directorio *principal*, sin necesitar saber el nombre exacto del directorio principal. El otro directorio oculto **(.)** especifica el *directorio actual* en los comandos en que la ubicación actual es el argumento de origen o destino, y se evita la necesidad de escribir el nombre de la ruta absoluta del directorio.

```
[student@desktopX Videos]$ pwd  
/home/student/Videos  
[student@desktopX Videos]$ cd .  
[student@desktopX Videos]$ pwd  
/home/student/Videos  
[student@desktopX Videos]$ cd ..  
[student@desktopX ~]$ pwd  
/home/student  
[student@desktopX ~]$ cd ..  
[student@desktopX home]$ pwd  
/home  
[student@desktopX home]$ cd ..  
[student@desktopX /]$ pwd  
/  
[student@desktopX /]$ cd ..  
[student@desktopX ~]$ pwd  
/home/student  
[student@desktopX ~]$
```

Referencias

info libc 'file name resolution' (*Manual de referencia de la biblioteca GNU C*)

- Sección 11.2.2: Resolución de nombre de archivo

Páginas del manual: **bash(7)**, **cd(1)**, **ls(1)**, **pwd(1)**, **unicode(1)** y **utf-8(7)**.

UTF-8 y Unicode

<http://www.utf-8.com/>

Práctica: Ubicación de archivos y directorios

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

cd	cd -	cd ..	cd ../../	cd /bin	cd bin	ls -al
ls -l ~	pwd					

Acción que se debe completar	Comando
Liste el directorio de inicio del usuario actual (formato extenso) en la sintaxis más simple, cuando no sea la ubicación actual.	
Regrese al directorio de inicio del usuario actual.	
Determine el nombre de la ruta absoluta de la ubicación actual.	
Regrese al directorio de trabajo más anterior.	
Ascienda dos niveles desde la ubicación actual.	
Liste la ubicación actual (formato extenso) con archivos ocultos.	
Avance hasta la ubicación de los archivos binarios desde cualquier ubicación actual.	
Ascienda hasta el directorio principal de la ubicación actual.	

Acción que se debe completar	Comando
Avance hasta la ubicación de los archivos binarios desde el directorio root.	

Solución

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

Acción que se debe completar	Comando
Liste el directorio de inicio del usuario actual (formato extenso) en la sintaxis más simple, cuando no sea la ubicación actual.	ls -l ~
Regrese al directorio de inicio del usuario actual.	cd
Determine el nombre de la ruta absoluta de la ubicación actual.	pwd
Regrese al directorio de trabajo más anterior.	cd -
Ascienda dos niveles desde la ubicación actual.	cd ../../
Liste la ubicación actual (formato extenso) con archivos ocultos.	ls -al
Avance hasta la ubicación de los archivos binarios desde cualquier ubicación actual.	cd /bin
Ascienda hasta el directorio principal de la ubicación actual.	cd ..
Avance hasta la ubicación de los archivos binarios desde el directorio root.	cd bin

Administración de archivos con las herramientas de línea de comandos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder crear, copiar, vincular, desplazar y eliminar archivos y subdirectorios en varios directorios.

Administración de archivos de la línea de comandos

La administración de archivos implica la creación, la eliminación, el copiado y el desplazamiento de archivos. Además, los directorios pueden crearse, eliminarse, copiarse y desplazarse para organizar los archivos en forma lógica. Cuando se trabaja en la línea de comandos, la administración de archivos requiere el conocimiento del directorio de trabajo actual para elegir una sintaxis de ruta absoluta o relativa como la opción más eficiente para la tarea inmediata.

Comandos de administración de archivos

Actividad	Fuente única ^(nota)	Varias fuentes ^(nota)
Copiar archivo	cp file1 file2	cp file1 file2 file3 dir ⁽⁴⁾
Desplazar archivos	mv file1 file2 ⁽¹⁾	mv file1 file2 file3 dir ⁽⁴⁾
Eliminar archivo	rm file1	rm -f file1 file2 file3 ⁽⁵⁾
Crear directorio	mkdir dir	mkdir -p par1/par2/dir ⁽⁶⁾
Copiar directorio	cp -r dir1 dir2 ⁽²⁾	cp -r dir1 dir2 dir3 dir4 ⁽⁴⁾
Desplazar directorio	mv dir1 dir2 ⁽³⁾	mv dir1 dir2 dir3 dir4 ⁽⁴⁾
Eliminar directorio	rm -r dir1 ⁽²⁾	rm -rf dir1 dir2 dir3 ⁽⁵⁾
Nota:	⁽¹⁾ El resultado es un nombre nuevo. ⁽²⁾ La opción "recursive" se requiere para procesar un directorio fuente. ⁽³⁾ Si dir2 existe, el resultado es un movimiento. Si dir2 no existe, el resultado es un nombre nuevo. ⁽⁴⁾ El último argumento debe ser un directorio. ⁽⁵⁾ Tenga precaución con la opción "force"; no se le pedirá que confirme su acción. ⁽⁶⁾ Tenga precaución con la opción "create parent"; no se detectan errores de escritura.	

Creación de directorios

El comando **mkdir** crea uno o más directorios o subdirectorios y genera errores si ya existe el nombre del archivo o cuando se intenta crear un directorio en un directorio de inicio que no existe. La opción **-p parent** crea directorios de inicio faltantes para el destino solicitado. Tenga cuidado cuando use **mkdir -p** ya que los errores de ortografía accidentales generan directorios involuntarios sin activar mensajes de error.

En el siguiente ejemplo, un usuario intenta usar **mkdir** para crear un subdirectorio denominado **Watched** en el directorio existente **Videos**, pero escribe mal el nombre del directorio.

```
[student@desktopX ~]$ mkdir Video/Watched
mkdir: cannot create directory `Video/Watched': No such file or directory
```

mkdir generó un error porque **Videos** se escribió mal y el directorio **Video** no existe. Si el usuario utilizó **mkdir** con la opción **-p**, no habría ningún error y el usuario tendría dos directorios, **Videos** y **Video**, y el subdirectorio **Watched** se crearía en el lugar equivocado.

```
[student@desktopX ~]$ mkdir Videos/Watched
[student@desktopX ~]$ cd Documents
[student@desktopX Documents]$ mkdir ProjectX ProjectY
[student@desktopX Documents]$ mkdir -p Thesis/Chapter1 Thesis/Chapter2 Thesis/Chapter3
[student@desktopX Documents]$ cd
[student@desktopX ~]$ ls -R Videos Documents
Documents:
ProjectX ProjectY Thesis thesis_chapter1.odf thesis_chapter2.odf

Documents/ProjectX:

Documents/ProjectY:

Documents/Thesis:
Chapter1 Chapter2 Chapter3

Documents/Thesis/Chapter1:

Documents/Thesis/Chapter2:

Documents/Thesis/Chapter3:

Videos:
blockbuster1.ogg blockbuster2.ogg Watched

Videos/Watched:
[student@desktopX ~]$
```

El último **mkdir** creó tres subdirectorios de **ChapterN** con un comando. La opción **-p parent** creó el directorio principal faltante **Thesis**.

Copia de archivos

El comando **cp** copia uno o más archivos para que se conviertan en archivos nuevos e independientes. La sintaxis permite copiar un archivo existente en un archivo nuevo en un directorio actual o en otro directorio, o copiar varios archivos en otro directorio. En cualquier destino, los nombres de los archivos nuevos deben ser únicos. Si el nombre del archivo nuevo no es único, el comando de copia sobrescribirá el archivo existente.

```
[student@desktopX ~]$ cd Videos
[student@desktopX Videos]$ cp blockbuster1.ogg blockbuster3.ogg
[student@desktopX Videos]$ ls -l
total 0
-rw-rw-r--. 1 student student 0 Feb 8 16:23 blockbuster1.ogg
-rw-rw-r--. 1 student student 0 Feb 8 16:24 blockbuster2.ogg
-rw-rw-r--. 1 student student 0 Feb 8 19:02 blockbuster3.ogg
drwxrwxr-x. 2 student student 4096 Feb 8 23:35 Watched
```

Capítulo 2. Administración de archivos desde la línea de comandos

```
[student@desktopX Videos]$
```

Cuando se copian varios archivos con un comando, el último argumento debe ser un directorio. Los archivos copiados conservan su nombre original en el directorio nuevo. Es probable que se sobrescriban los nombres de archivo con conflicto que existan en un destino. Para evitar que los usuarios sobrescriban directorios con contenido, existen varios comandos **cp** de archivo que omiten directorios especificados como origen. Para poder copiar directorios que no están vacíos, es decir, con contenido, se requiere la opción **-r recursive**.

```
[student@desktopX Videos]$ cd ../Documents
[student@desktopX Documents]$ cp thesis_chapter1.odf thesis_chapter2.odf Thesis ProjectX
cp: omitting directory `Thesis'
[student@desktopX Documents]$ cp -r Thesis ProjectX
[student@desktopX Documents]$ cp thesis_chapter2.odf Thesis/Chapter2/
[student@desktopX Documents]$ ls -R
.:
ProjectX  ProjectY  Thesis  thesis_chapter1.odf  thesis_chapter2.odf

./ProjectX:
Thesis  thesis_chapter1.odf  thesis_chapter2.odf

./ProjectX/Thesis:

./ProjectY:

./Thesis:
Chapter1  Chapter2  Chapter3

./Thesis/Chapter1:

./Thesis/Chapter2:
thesis_chapter2.odf

./Thesis/Chapter3:
[student@desktopX Documents]$
```

En el primer comando **cp**, **Thesis** no pudo copiar, pero sí lo hicieron **thesis_chapter1.odf** y **thesis_chapter2.odf**. Con la opción **-r recursive**, se pudo copiar **Thesis**.

Desplazamiento de archivos

El comando **mv** cambia el nombre a los archivos en el mismo directorio o reubica archivos en un directorio nuevo. El contenido del archivo se conserva sin modificaciones. Los archivos que se desplazan hacia un sistema de archivos diferente requieren de la creación de un archivo nuevo mediante la copia del archivo de origen y, a continuación, la eliminación de dicho archivo. A pesar de que, por lo general, los archivos grandes son transparentes para el usuario, pueden demorar mucho en desplazarse.

```
[student@desktopX Videos]$ cd ../Documents
[student@desktopX Documents]$ ls -l
total 0
-rw-rw-r--. 1 student student    0 Feb  8 16:24 thesis_chapter1.odf
-rw-rw-r--. 1 student student    0 Feb  8 16:24 thesis_chapter2.odf
[student@desktopX Documents]$ mv thesis_chapter2.odf thesis_chapter2_reviewed.odf
[student@desktopX Documents]$ mv thesis_chapter1.odf Thesis/Chapter1
[student@desktopX Documents]$ ls -lR
.:
```

```

total 16
drwxrwxr-x. 2 student student 4096 Feb 11 11:58 ProjectX
drwxrwxr-x. 2 student student 4096 Feb 11 11:55 ProjectY
drwxrwxr-x. 5 student student 4096 Feb 11 11:56 Thesis
-rw-rw-r--. 1 student student    0 Feb 11 11:54 thesis_chapter2_reviewed.odf

./ProjectX:
total 0
-rw-rw-r--. 1 student student 0 Feb 11 11:58 thesis_chapter1.odf
-rw-rw-r--. 1 student student 0 Feb 11 11:58 thesis_chapter2.odf

./ProjectX/Thesis:
total 0

./ProjectY:
total 0

./Thesis:
total 12
drwxrwxr-x. 2 student student 4096 Feb 11 11:59 Chapter1
drwxrwxr-x. 2 student student 4096 Feb 11 11:56 Chapter2
drwxrwxr-x. 2 student student 4096 Feb 11 11:56 Chapter3

./Thesis/Chapter1:
total 0
-rw-rw-r--. 1 student student 0 Feb 11 11:54 thesis_chapter1.odf

./Thesis/Chapter2:
total 0
-rw-rw-r--. 1 student student 0 Feb 11 11:54 thesis_chapter2.odf

./Thesis/Chapter3:
total 0
[student@desktopX Documents]$
```

El primer comando **mv** es un ejemplo de cómo cambiarle el nombre a un archivo. El segundo provoca que el archivo sea reubicado en otro directorio.

Eliminación de archivos y directorios

La sintaxis predeterminada para **rm** elimina archivos, pero no directorios. La eliminación de un directorio y, potencialmente, de muchos subdirectorios y archivos que estén en él, requiere la opción **-r recursive**. No existe una función de deshacer la eliminación de línea de comandos; ni tampoco una papelera de reciclaje desde donde se pueda restaurar la eliminación.

```

[student@desktopX Documents]$ pwd
/home/student/Documents
[student@desktopX Documents]$ rm thesis_chapter2_reviewed.odf
[student@desktopX Documents]$ rm Thesis/Chapter1
rm: cannot remove `Thesis/Chapter1': Is a directory
[student@desktopX Documents]$ rm -r Thesis/Chapter1
[student@desktopX Documents]$ ls -l Thesis
total 8
drwxrwxr-x. 2 student student 4096 Feb 11 12:47 Chapter2
drwxrwxr-x. 2 student student 4096 Feb 11 12:48 Chapter3
[student@desktopX Documents]$ rm -ri Thesis
rm: descend into directory `Thesis'? y
rm: descend into directory `Thesis/Chapter2'? y
rm: remove regular empty file `Thesis/Chapter2/thesis_chapter2.odf'? y
rm: remove directory `Thesis/Chapter2'? y
rm: remove directory `Thesis/Chapter3'? y
```

```
rm: remove directory `Thesis'? y  
[student@desktopX Documents]$
```

Después de que **rm** no pudo eliminar el directorio **Chapter1**, la opción **-r recursive** pudo hacerlo en forma correcta. El último comando **rm** analizó primero cada subdirectorio y eliminó en forma individual los archivos que contenía antes de eliminar cada directorio que ahora está vacío. El uso de **-i** pide la confirmación para cada eliminación de forma interactiva. Esto es básicamente lo opuesto de **-f**, que fuerza la eliminación sin solicitar confirmación al usuario.

El comando **rmdir** elimina directorios solo si están vacíos. Los directorios eliminados no pueden recuperarse.

```
[student@desktopX Documents]$ pwd  
/home/student/Documents  
[student@desktopX Documents]$ rmdir ProjectY  
[student@desktopX Documents]$ rmdir ProjectX  
rmdir: failed to remove `ProjectX': Directory not empty  
[student@desktopX Documents]$ rm -r ProjectX  
[student@desktopX Documents]$ ls -lR  
.:  
total 0  
[student@desktopX Documents]$
```

El comando **rmdir** no pudo eliminar **ProjectX** que no estaba vacío, pero **rm -r** pudo hacerlo en forma correcta.

Referencias

Páginas del manual **cp(1)**, **mkdir(1)**, **mv(1)**, **rm(1)** y **rmdir(1)**

Práctica: Administración de archivo de línea de comandos

En este ejercicio de laboratorio, practicará técnicas eficientes para crear y organizar archivos con directorios y copias de archivos.

Resultados:

Los estudiantes practicarán cómo crear, reordenar y eliminar archivos.

Andes de comenzar

Inicie sesión en su cuenta de estudiante en serverX. Comience en su directorio de inicio.

1. En el directorio de inicio, cree conjuntos de archivos de práctica vacíos para usar durante el resto de este ejercicio de laboratorio. Si el comando pensado no se reconoce de inmediato, se espera que los estudiantes usen la solución orientada para ver y practicar cómo se resuelve la tarea. Use la opción completar con el tabulador de la shell y complete los nombres de ruta con más facilidad.

Cree seis archivos con nombres como **songX.mp3**.

Cree seis archivos con nombres como **snapX.jpg**.

Cree seis archivos con nombres como **filmX.avi**.

En cada conjunto, reemplace la X con los números del 1 al 6.

```
[student@serverX ~]$ touch song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3
song6.mp3
[student@serverX ~]$ touch snap1.jpg snap2.jpg snap3.jpg snap4.jpg snap5.jpg
snap6.jpg
[student@serverX ~]$ touch film1.avi film2.avi film3.avi film4.avi film5.avi
film6.avi
[student@serverX ~]$ ls -l
```

2. Desde el directorio principal, desplace los archivos de canciones al subdirectorío **Music**, los archivos de instantáneas al subdirectorío **Pictures** y los archivos de películas al subdirectorío **Videos**.

Cuando distribuya archivos desde una ubicación hacia muchas ubicaciones, primero cambie el directorio que contiene los archivos de *origen*. Use la sintaxis de ruta más simple, absoluta o relativa, para llegar al destino de cada tarea de administración de archivos.

```
[student@serverX ~]$ mv song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3
Music
[student@serverX ~]$ mv snap1.jpg snap2.jpg snap3.jpg snap4.jpg snap5.jpg snap6.jpg
Pictures
[student@serverX ~]$ mv film1.avi film2.avi film3.avi film4.avi film5.avi film6.avi
Videos
[student@serverX ~]$ ls -l Music Pictures Videos
```

Capítulo 2. Administración de archivos desde la línea de comandos

3. En su directorio de inicio, cree tres subdirectorios para organizar los archivos en proyectos. Denomine a estos directorios **friends**, **family** y **work**. Cree los tres directorios con un comando.

Usará estos directorios para reorganizar los archivos en proyectos.

```
[student@serverX ~]$ mkdir friends family work  
[student@serverX ~]$ ls -l
```

4. Ubicará algunos de los archivos nuevos en directorios de proyectos para familia y amigos. Use todos los comandos que necesite. En este ejemplo, no tiene que usar un solo comando. Para cada proyecto, primero cambie el directorio de proyecto y, a continuación, copie los archivos de origen en este directorio. Las copias se generan porque conservará los originales después de entregar estos proyectos a familiares y amigos.

Copie los archivos (de todo tipo) que tengan los números 1 y 2 en la carpeta de amigos.

Copie los archivos (de todo tipo) que tengan los números 3 y 4 en la carpeta de familia.

Cuando recopile archivos de varias ubicaciones en una ubicación, cambie el directorio que contendrá los archivos de *destino*. Use la sintaxis de ruta más simple, absoluta o relativa, para llegar al origen de cada tarea de administración de archivos.

```
[student@serverX ~]$ cd friends  
[student@serverX friends]$ cp ~/Music/song1.mp3 ~/Music/song2.mp3 ~/Pictures/  
snap1.jpg ~/Pictures/snap2.jpg ~/Videos/film1.avi ~/Videos/film2.avi .  
[student@serverX friends]$ ls -l  
[student@serverX friends]$ cd ../family  
[student@serverX family]$ cp ~/Music/song3.mp3 ~/Music/song4.mp3 ~/Pictures/  
snap3.jpg ~/Pictures/snap4.jpg ~/Videos/film3.avi ~/Videos/film4.avi .  
[student@serverX family]$ ls -l
```

5. Para su proyecto de trabajo, creará copias adicionales.

```
[student@serverX family]$ cd ../work  
[student@serverX work]$ cp ~/Music/song5.mp3 ~/Music/song6.mp3 ~/Pictures/snap5.jpg  
~/Pictures/snap6.jpg ~/Videos/film5.avi ~/Videos/film6.avi .  
[student@serverX work]$ ls -l
```

6. Ahora, los proyectos están listos. Es momento de borrar los proyectos.

Cambie a su directorio de inicio. Intente eliminar tanto el proyecto de familia como el de amigos con un solo comando **rmdir**.

```
[student@serverX work]$ cd  
[student@serverX ~]$ rmdir family friends  
rmdir: failed to remove `family': Directory not empty  
rmdir: failed to remove `friends': Directory not empty
```

El uso del comando **rmdir** debería generar un error ya que ambos directorios no están vacíos.

-
7. Use otro comando que pueda eliminar correctamente tanto la carpeta de familia como la de amigos.

```
[student@serverX ~]$ rm -r family friends  
[student@serverX ~]$ ls -l
```

8. Elimine todos los archivos del proyecto de trabajo, pero no elimine el directorio de trabajo.

```
[student@serverX ~]$ cd work  
[student@serverX work]$ rm song5.mp3 song6.mp3 snap5.jpg snap6.jpg film5.avi  
    film6.avi  
[student@serverX work]$ ls -l
```

9. Por último, desde el directorio de inicio, use el comando **rmdir** para eliminar el directorio de trabajo. El comando debería poder completar la acción sin errores ahora que está vacío.

```
[student@serverX work]$ cd  
[student@serverX ~]$ rmdir work  
[student@serverX ~]$ ls -l
```

Coincidencia de nombres de archivo mediante el uso de expansión de nombre de ruta

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder usar metacaracteres y técnicas de expansión para mejorar la eficiencia de procesamiento de administración de archivos.

Globbing de archivos: expansión de nombre de ruta

La shell Bash tiene una capacidad de coincidencia de nombre de ruta que, históricamente, se llamó *globbing*, que es la forma abreviada del programa de expansión de ruta de archivo del “comando global” de las primeras versiones de UNIX. La función globbing de Bash, que comúnmente se denomina *coincidencia de patrón* o “comodines”, facilita la administración de grandes cantidades de archivos. Con *metacaracteres* que se “expanden” para establecer una coincidencia entre los archivos y los nombres de ruta que se buscan, los comandos trabajan en un conjunto de archivos orientado al mismo tiempo.

Coincidencia del patrón

Globbing es una operación de análisis de comandos de la shell que expande un patrón de comodín en una lista de nombres de ruta coincidentes. Los metacaracteres de la línea de comandos se reemplazan por la lista de coincidencia antes de la ejecución del comando. Los patrones, en especial las clases de carácter entre corchetes, que no ofrecen coincidencias, muestran la solicitud de patrón original como texto literal. Los siguientes son metacaracteres y clases de patrón de uso frecuente.

Patrón	Coincidencias
*	Cualquier secuencia de cero o más caracteres.
?	Cualquier carácter individual.
~	El directorio de inicio del usuario actual.
<code>~username</code>	Directorio de inicio del <i>username</i> del usuario.
<code>~+</code>	El directorio de trabajo actual.
<code>~-</code>	El directorio de trabajo anterior.
<code>[abc...]</code>	Cualquier carácter en la clase incluida.
<code>[!abc...]</code>	Cualquier carácter que <i>no</i> esté incluido en la clase.
<code>[^abc...]</code>	Cualquier carácter que <i>no</i> esté incluido en la clase.
<code>[:alpha:]</code>	Cualquier carácter alfabético. ⁽¹⁾
<code>[:lower:]</code>	Cualquier carácter en minúsculas. ⁽¹⁾
<code>[:upper:]</code>	Cualquier carácter en mayúscula. ⁽¹⁾
<code>[:alnum:]</code>	Cualquier dígito o carácter alfabético. ⁽¹⁾
<code>[:punct:]</code>	Cualquier carácter imprimible que no sea un espacio o alfanumérico. ⁽¹⁾
<code>[:digit:]</code>	Cualquier dígito, 0 - 9 . ⁽¹⁾

Patrón	Coincidencias
[:space:]	Cualquier carácter de espacio en blanco; puede incluir tabulaciones, renglón nuevo, retornos de carro y avances de página, así como el espacio. ⁽¹⁾
Nota	⁽¹⁾ clase de carácter POSIX establecido previamente; se adapta a la región actual.

Un conjunto de archivos de muestra sirve para demostrar la expansión.

```
[student@desktopX ~]$ mkdir glob; cd glob
[student@desktopX glob]$ touch alfa bravo charlie delta echo able baker cast dog easy
[student@desktopX glob]$ ls
able alfa baker bravo cast charlie delta dog easy echo
[student@desktopX glob]$
```

Primero, coincidencias de patrón simple que usan * y ?.

```
[student@desktopX glob]$ ls a*
able alfa
[student@desktopX glob]$ ls *a*
able alfa baker bravo cast charlie delta easy
[student@desktopX glob]$ ls [ac]*
able alfa cast charlie
[student@desktopX glob]$ ls ???
able alfa cast easy echo
[student@desktopX glob]$ ls ****
baker bravo delta
[student@desktopX glob]$
```

Expansión de tilde

El carácter del tilde (~), cuando está seguido de una barra separadora, coincide con el directorio principal del usuario actual. Si está seguido por una secuencia de caracteres hasta la barra, se interpretará como un nombre de usuario, en caso de que uno coincida. Si ningún nombre de usuario coincide, aparecerá el propio tilde seguido de la secuencia de caracteres.

```
[student@desktopX glob]$ ls ~/glob
able alfa baker bravo cast charlie delta dog easy echo
[student@desktopX glob]$ echo ~/glob
/home/student/glob
[student@desktopX glob]$
```

Expansión de llaves

La expansión de llaves se usa para generar secuencias discretionales de caracteres. Las llaves contienen una lista de secuencias, o una expresión de secuencias, separadas por comas. El resultado incluye el texto que antecede o que sigue a la definición de llaves. Las expansiones de llaves pueden estar anidadas, una dentro de la otra.

```
[student@desktopX glob]$ echo {Sunday,Monday,Tuesday,Wednesday}.log
Sunday.log Monday.log Tuesday.log Wednesday.log
[student@desktopX glob]$ echo file{1..3}.txt
file1.txt file2.txt file3.txt
[student@desktopX glob]$ echo file{a..c}.txt
```

Capítulo 2. Administración de archivos desde la línea de comandos

```
filea.txt fileb.txt filec.txt
[student@desktopX glob]$ echo file{a,b}{1,2}.txt
filea1.txt filea2.txt fileb1.txt fileb2.txt
[student@desktopX glob]$ echo file{a{1,2},b,c}.txt
filea1.txt filea2.txt fileb.txt filec.txt
[student@desktopX glob]$
```

Sustitución de comandos

La sustitución de comandos permite obtener un comando para reemplazar el comando mismo. La sustitución de comandos se produce cuando un comando está encerrado entre un signo de dólar al principio y paréntesis, `$(command)`, o con acento grave, ``command``. La forma con acento grave es más antigua y tiene dos desventajas: 1) el acento grave puede confundirse fácilmente a la vista con las comillas simples, y 2) el acento grave no puede anidarse dentro de los acentos graves. La forma `$(command)` puede anidar varias expansiones de comando dentro de cada una.

```
[student@desktopX glob]$ echo Today is `date +%A`.
Today is Wednesday.
[student@desktopX glob]$ echo The time is $(date +%M) minutes past $(date +%l%p).
The time is 26 minutes past 11AM.
[student@desktopX glob]$
```

Evitar la expansión de argumentos

Muchos caracteres tienen un significado especial en la shell Bash. Para ignorar los significados especiales del metacaracter, se usa la *cita* y el *escape* para evitar la expansión de la shell. La barra invertida (\) es un carácter de escape en Bash y protege al carácter individual siguiente de que se interprete de manera especial. Para proteger las secuencias de carácter más extensas, se usan comillas simples ('') o dobles ("") para encerrar las secuencias.

Use comillas dobles para suprimir el globbing y la expansión de la shell, pero permita la sustitución de comandos y variables. A nivel conceptual, la sustitución de variables es idéntica a la sustitución de comandos, pero puede usar sintaxis de llaves opcional.

```
[student@desktopX glob]$ host=$(hostname -s); echo $host
desktopX
[student@desktopX glob]$ echo "***** hostname is ${host} ****"
***** hostname is desktopX ****
[student@desktopX glob]$ echo Your username variable is \$USER.
Your username variable is $USER.
[student@desktopX glob]$
```

Use comillas simples para interpretar *todo* el texto literalmente. Observe la diferencia, tanto en la pantalla como en el teclado, entre las comillas simples ('') y el acento grave de sustitución de comando (`). Además de suprimir el globbing y la expansión de la shell, las comillas dirigen a la shell para que también suprima la sustitución de comandos y variables. El signo de interrogación es el metacaracter que también necesita protección para evitar la expansión.

```
[student@desktopX glob]$ echo "Will variable $host evaluate to $(hostname -s)?"
Will variable desktopX evaluate to desktopX?
[student@desktopX glob]$ echo 'Will variable $host evaluate to $(hostname -s)?'
Will variable $host evaluate to $(hostname -s)?
[student@desktopX glob]$
```



Referencias

Páginas del manual: **bash(1)**, **cd(1)**, **glob(7)**, **isalpha(3)**, **ls(1)**,
path_resolution(7) y **pwd(1)**

Práctica: Expansión del nombre de ruta

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

<code>*[:digit:]*</code>	<code>*b</code>	<code>*b*</code>	<code>???</code> *	<code>[!b]*</code>	<code>[:upper:]*</code>
<code>b*</code>					

Coincidencia solicitada que se debe encontrar	Patrones
Solo nombres de archivos que comienzan con "b"	
Solo nombres de archivos que terminan con "b"	
Solo nombres de archivos que contienen una "b"	
Solo nombres de archivos donde el primer carácter no es "b"	
Solo nombres de archivos que tengan al menos 3 caracteres de largo	
Solo nombres de archivos que contengan un número	
Solo nombres de archivos que comienzan con una letra mayúscula	

Solución

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

Coincidencia solicitada que se debe encontrar	Patrones
Solo nombres de archivos que comienzan con "b"	b*
Solo nombres de archivos que terminan con "b"	*b
Solo nombres de archivos que contienen una "b"	*b*
Solo nombres de archivos donde el primer carácter no es "b"	[!b]*
Solo nombres de archivos que tengan al menos 3 caracteres de largo	???
Solo nombres de archivos que contengan un número	*[:digit:]*
Solo nombres de archivos que comienzan con una letra mayúscula	[:upper:]*

Ejercicio de laboratorio: Administración de archivos con expansión de shell

En este ejercicio de laboratorio, creará, moverá y eliminará archivos y carpetas usando una variedad de atajos correspondientes a los nombres de archivos.

Resultados:

Familiaridad y práctica con muchas formas de comodines para localizar y usar archivos.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario. Inicie sesión como **student** y comience en el directorio de inicio.

1. Para comenzar, cree conjuntos de archivos de práctica vacíos para usar en este ejercicio de laboratorio. Si no se reconoce inmediatamente un atajo deseado de ampliación de la shell, se espera que los estudiantes usen la solución para aprender y practicar. Utilice la terminación (completado) del tabulador shell para localizar los nombres de ruta de archivos fácilmente.

Cree un total de 12 archivos con nombres **tv_seasonX_episodeY.ogg**. Reemplace X con el número de temporada e Y con el episodio de esa temporada, para dos temporadas de seis episodios cada una.

2. Como autor de una serie exitosa de novelas de misterio, los capítulos de su próximo bestseller se están editando para publicarlos. Cree un total de ocho archivos con nombres **mystery_chapterX.odf**. Reemplace la X con los números del 1 al 8.
3. Para organizar los episodios de TV, cree dos subdirectorios denominados **season1** y **season2** en el directorio **Videos** existente. Use solamente un comando.
4. Traslade los episodios de TV adecuados a los subdirectorios de temporadas. Use solo dos comandos, especificando destinos con la sintaxis relativa.
5. Para organizar los capítulos del libro de misterios, cree una jerarquía de directorios de dos niveles con un comando. Cree **my_bestseller** en el directorio existente **Documents** y **chapters** en el nuevo directorio **my_bestseller**.
6. Con un comando, cree más subdirectorios directamente en el directorio **my_bestseller**. Nombre a estos subdirectorios **editor**, **plot_change** y **vacation**. La opción *create parent* no es necesaria porque el directorio principal **my_bestseller** ya existe.
7. Cambie al directorio **chapters**. Use el atajo del directorio de inicio para especificar los archivos de recursos, mueva todos los capítulos del libro al directorio **chapters**, que ahora es el directorio actual. ¿Cuál es la sintaxis más simple para especificar el directorio de destino?
8. Los primeros dos capítulos se envían al editor para la revisión. Para recordar no modificar estos capítulos durante la revisión, traslade estos dos capítulos solamente al directorio **editor**. Use la sintaxis relativa comenzando desde el subdirectorio **chapters**.

-
9. Los capítulos 7 y 8 se escribirán mientras esté de vacaciones. Mueva los archivos desde **chapters** hacia **vacation**. Use un comando sin caracteres comodines.
 10. Con un comando, cambie el directorio de trabajo para la ubicación de episodios de TV de la temporada 2 y, luego, copie el primer episodio de la temporada en el directorio **vacation**.
 11. Con un comando, cambie el directorio de trabajo a **vacation**; luego, detalle sus archivos. También se necesita el episodio 2. Vuelva al directorio **season2** usando el atajo *directorio de trabajo anterior*. Este paso dará resultado si se logró el último cambio de directorio con un comando. Copie el archivo del episodio 2 en **vacation**. Vuelva a **vacation** usando el atajo nuevamente.
 12. Es posible que los capítulos 5 y 6 necesiten un cambio de argumento. Para evitar que estos cambios modifiquen los archivos originales, copie ambos archivos en **plot_change**. Mueva un directorio al directorio principal de **vacation**, luego use un comando desde allí.
 13. Para realizar un seguimiento de los cambios, haga tres copias de seguridad del capítulo 5. Cambie al directorio **plot_change**. Copie **mystery_chapter5.odf** como un nombre de archivo nuevo para incluir la fecha completa (años-mes-día). Realice otra copia anexando el sello de tiempo actual (como el número de segundos desde *epoch*) para asegurar un nombre de archivo único. También haga una copia anexando el usuario actual (**\$USER**) al nombre del archivo. Consulte la solución para la sintaxis de todo lo que no esté seguro (como qué argumentos pasar al comando **date**).

Observe que también podríamos hacer las mismas copias de seguridad de los archivos del capítulo 6.
 14. Los cambios de argumento no fueron exitosos. Elimine el directorio **plot_change**. Primero, elimine todos los archivos en el directorio **plot_change**. Suba el directorio un nivel debido a que el directorio no se puede eliminar mientras sea el directorio de trabajo. Intente eliminar el directorio usando el comando **rm** sin la opción *recursive*. Este intento debe fallar. Ahora, use comando **rmdir**, que será correcto.
 15. Cuando finalicen las vacaciones, el directorio **vacation** ya no será necesario. Elimínelo usando el comando **rm** con la opción *recursive*.

Una vez que haya finalizado, regrese al directorio de inicio.

Capítulo 2. Administración de archivos desde la línea de comandos

Solución

En este ejercicio de laboratorio, creará, moverá y eliminará archivos y carpetas usando una variedad de atajos correspondientes a los nombres de archivos.

Resultados:

Familiaridad y práctica con muchas formas de comodines para localizar y usar archivos.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario. Inicie sesión como **student** y comience en el directorio de inicio.

1. Para comenzar, cree conjuntos de archivos de práctica vacíos para usar en este ejercicio de laboratorio. Si no se reconoce inmediatamente un atajo deseado de ampliación de la shell, se espera que los estudiantes usen la solución para aprender y practicar. Utilice la terminación (completado) del tabulador shell para localizar los nombres de ruta de archivos fácilmente.

Cree un total de 12 archivos con nombres **tv_seasonX_episodeY.ogg**. Reemplace X con el número de temporada e Y con el episodio de esa temporada, para dos temporadas de seis episodios cada una.

```
[student@serverX ~]$ touch tv_season{1..2}_episode{1..6}.ogg  
[student@serverX ~]$ ls -l
```

2. Como autor de una serie exitosa de novelas de misterio, los capítulos de su próximo bestseller se están editando para publicarlos. Cree un total de ocho archivos con nombres **mystery_chapterX.odf**. Reemplace la X con los números del 1 al 8.

```
[student@serverX ~]$ touch mystery_chapter{1..8}.odf  
[student@serverX ~]$ ls -l
```

3. Para organizar los episodios de TV, cree dos subdirectorios denominados **season1** y **season2** en el directorio **Videos** existente. Use solamente un comando.

```
[student@serverX ~]$ mkdir Videos/season{1..2}  
[student@serverX ~]$ ls -lR
```

4. Traslade los episodios de TV adecuados a los subdirectorios de temporadas. Use solo dos comandos, especificando destinos con la sintaxis relativa.

```
[student@serverX ~]$ mv tv_season1* Videos/season1  
[student@serverX ~]$ mv tv_season2* Videos/season2  
[student@serverX ~]$ ls -lR
```

5. Para organizar los capítulos del libro de misterios, cree una jerarquía de directorios de dos niveles con un comando. Cree **my_bestseller** en el directorio existente **Documents** y **chapters** en el nuevo directorio **my_bestseller**.

```
[student@serverX ~]$ mkdir -p Documents/my_bestseller/chapters  
[student@serverX ~]$ ls -lR
```

6. Con un comando, cree más subdirectorios directamente en el directorio **my_bestseller**. Nombre a estos subdirectorios **editor**, **plot_change** y **vacation**. La opción *create parent* no es necesaria porque el directorio principal **my_bestseller** ya existe.

```
[student@serverX ~]$ mkdir Documents/my_bestseller/{editor,plot_change,vacation}
[student@serverX ~]$ ls -lR
```

7. Cambie al directorio **chapters**. Use el atajo del directorio de inicio para especificar los archivos de recursos, mueva todos los capítulos del libro al directorio **chapters**, que ahora es el directorio actual. ¿Cuál es la sintaxis más simple para especificar el directorio de destino?

```
[student@serverX ~]$ cd Documents/my_bestseller/chapters
[student@serverX chapters]$ mv ~/mystery_chapter* .
[student@serverX chapters]$ ls -l
```

8. Los primeros dos capítulos se envían al editor para la revisión. Para recordar no modificar estos capítulos durante la revisión, translade estos dos capítulos solamente al directorio **editor**. Use la sintaxis relativa comenzando desde el subdirectorio **chapters**.

```
[student@serverX chapters]$ mv mystery_chapter1.odf mystery_chapter2.odf ../editor
[student@serverX chapters]$ ls -l
[student@serverX chapters]$ ls -l ../editor
```

9. Los capítulos 7 y 8 se escribirán mientras esté de vacaciones. Mueva los archivos desde **chapters** hacia **vacation**. Use un comando sin caracteres comodines.

```
[student@serverX chapters]$ mv mystery_chapter7.odf mystery_chapter8.odf ../vacation
[student@serverX chapters]$ ls -l
[student@serverX chapters]$ ls -l ../vacation
```

10. Con un comando, cambie el directorio de trabajo para la ubicación de episodios de TV de la temporada 2 y, luego, copie el primer episodio de la temporada en el directorio **vacation**.

```
[student@serverX chapters]$ cd ~/Videos/season2
[student@serverX season2]$ cp tv_season2_episode1.ogg ~/Documents/my_bestseller/vacation
```

11. Con un comando, cambie el directorio de trabajo a **vacation**; luego, detalle sus archivos. También se necesita el episodio 2. Vuelva al directorio **season2** usando el atajo *directorío de trabajo anterior*. Este paso dará resultado si se logró el último cambio de directorio con un comando. Copie el archivo del episodio 2 en **vacation**. Vuelva a **vacation** usando el atajo nuevamente.

```
[student@serverX season2]$ cd ~/Documents/my_bestseller/vacation
[student@serverX vacation]$ ls -l
[student@serverX vacation]$ cd -
[student@serverX season2]$ cp tv_season2_episode2.ogg ~/Documents/my_bestseller/vacation
```

Capítulo 2. Administración de archivos desde la línea de comandos

```
[student@serverX vacation]$ cd -
[student@serverX vacation]$ ls -l
```

12. Es posible que los capítulos 5 y 6 necesiten un cambio de argumento. Para evitar que estos cambios modifiquen los archivos originales, copie ambos archivos en **plot_change**. Mueva un directorio al directorio principal de **vacation**, luego use un comando desde allí.

```
[student@serverX vacation]$ cd ..
[student@serverX my_bestseller]$ cp chapters/mystery_chapter[56].odf plot_change
[student@serverX my_bestseller]$ ls -l chapters
[student@serverX my_bestseller]$ ls -l plot_change
```

13. Para realizar un seguimiento de los cambios, haga tres copias de seguridad del capítulo 5. Cambie al directorio **plot_change**. Copie **mystery_chapter5.odf** como un nombre de archivo nuevo para incluir la fecha completa (años-mes-día). Realice otra copia anexando el sello de tiempo actual (como el número de segundos desde *epoch*) para asegurar un nombre de archivo único. También haga una copia anexando el usuario actual (**\$USER**) al nombre del archivo. Consulte la solución para la sintaxis de todo lo que no esté seguro (como qué argumentos pasar al comando **date**).

```
[student@serverX my_bestseller]$ cd plot_change
[student@serverX plot_change]$ cp mystery_chapter5.odf mystery_chapter5_$(date + %F).odf
[student@serverX plot_change]$ cp mystery_chapter5.odf mystery_chapter5_$(date + %s).odf
[student@serverX plot_change]$ cp mystery_chapter5.odf mystery_chapter5_${USER}.odf
[student@serverX plot_change]$ ls -l
```

Observe que también podríamos hacer las mismas copias de seguridad de los archivos del capítulo 6.

14. Los cambios de argumento no fueron exitosos. Elimine el directorio **plot_change**. Primero, elimine todos los archivos en el directorio **plot_change**. Suba el directorio un nivel debido a que el directorio no se puede eliminar mientras sea el directorio de trabajo. Intente eliminar el directorio usando el comando **rm** sin la opción *recursive*. Este intento debe fallar. Ahora, use comando **rmdir**, que será correcto.

```
[student@serverX plot_change]$ rm mystery*
[student@serverX plot_change]$ cd ..
[student@serverX my_bestseller]$ rm plot_change
rm: cannot remove 'plot_change': Is a directory
[student@serverX my_bestseller]$ rmdir plot_change
[student@serverX my_bestseller]$ ls -l
```

15. Cuando finalicen las vacaciones, el directorio **vacation** ya no será necesario. Elimínelo usando el comando **rm** con la opción *recursive*.

Una vez que haya finalizado, regrese al directorio de inicio.

```
[student@serverX my_bestseller]$ rm -r vacation
[student@serverX my_bestseller]$ ls -l
```

```
[student@serverX my_bestseller]$ cd
```

Resumen

Jerarquía del sistema de archivos Linux

Identifique el objetivo de los directorios de nivel superior en la jerarquía Linux.

Ubicación de archivos por nombre

Interprete y use en forma adecuada la sintaxis de nombre de archivo de ruta total o parcial.

Administración de archivos con las herramientas de línea de comandos

Trabaje a partir de la línea de comandos para crear, desplazar y eliminar archivos y directorios.

Coincidencia de nombres de archivo mediante el uso de expansión de nombre de ruta

Aprenda cómo especificar varios archivos con muchas técnicas de comodín.



CAPÍTULO 3

OBTENCIÓN DE AYUDA EN RED HAT ENTERPRISE LINUX

Descripción general	
Meta	Resolver problemas a través de sistemas de ayuda en línea y las utilidades de asistencia de Red Hat.
Objetivos	<ul style="list-style-type: none">• Usar <code>man</code>, el lector del manual de Linux.• Usar <code>pinfo</code>, el lector de información de GNU.• Usar la documentación del paquete Red Hat Package Manager (RPM)• Usar el comando <code>redhat-support-tool</code>.
Secciones	<ul style="list-style-type: none">• Lectura de la documentación con el comando <code>man</code> (y práctica)• Lectura de la documentación con el comando <code>pinfo</code> (y práctica)• Lectura de la documentación en <code>/usr/share/doc</code> (y práctica)• Obtención de ayuda de Red Hat (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">• Visualización e impresión de la documentación de ayuda

Lectura de la documentación utilizando el comando man

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder buscar documentación y responder preguntas sobre comandos.

Presentación del comando man

El histórico manual para el programador de Linux, del cual provienen las páginas de manual, era lo suficientemente extenso como para convertirse en múltiples libros impresos. Cada uno incluía información sobre tipos específicos de archivos, que se han convertido en las *secciones* que figuran a continuación. A los artículos se los denomina *temas*, ya que el término *páginas* ya no es válido.

Secciones del manual de Linux

Sección	Tipo de contenido
1	Comandos del usuario (<i>ejecutables y programas de la shell</i>)
2	Llamadas del sistema (<i>rutinas del núcleo invocadas desde el espacio del usuario</i>)
3	Funciones de la biblioteca (<i>proporcionadas por bibliotecas de programas</i>)
4	Archivos especiales (<i>como archivos de dispositivos</i>)
5	Formatos de archivos (<i>para muchos archivos y estructuras de configuración</i>)
6	Juegos (<i>sección histórica destinada a programas increíbles</i>)
7	Convenciones, estándares y páginas varias (<i>protocolos, sistemas de archivos</i>)
8	Comandos de administración del sistema y con privilegios (<i>tareas de mantenimiento</i>)
9	API del núcleo de Linux (<i>llamadas del núcleo internas</i>)

nota

La sección 9 del manual se añadió recientemente a Linux. No todas las listas de secciones del manual hacen referencia a ella.

Para diferenciar nombres de temas idénticos en secciones diferentes, las referencias de las páginas de manual incluyen el número de la sección entre paréntesis después del tema. Por ejemplo: por un lado, en **passwd(1)** se describe el comando para cambiar contraseñas; por otro lado, en **passwd(5)** se explica el formato de archivo **/etc/passwd** para almacenar cuentas de usuario local.

Si desea leer páginas de manual específicas, utilice **man topic**. El contenido del tema aparece en una pantalla a la vez. Emplee las teclas de flechas para desplazarse por una sola línea o la barra espaciadora para avanzar a la siguiente pantalla. El comando **man** busca secciones del manual en un orden configurado y muestra las secciones conocidas en primer lugar. Por ejemplo, **man passwd** muestra **passwd(1)** de manera predeterminada. Para

visualizar el tema de una página de manual de una sección específica, incluya el argumento de número de sección: **man 5 passwd** muestra **passwd(5)**.

Navegación y búsqueda de páginas del **man**

La capacidad de realizar búsquedas por temas de manera eficiente y de navegar por páginas del **man** es una habilidad de administración fundamental. En la siguiente tabla, se incluyen comandos de navegación **man** básicos:

Navegación de páginas de **man**

Comando	Resultado
Spacebar	Avanzar (abajo) una pantalla
PageDown	Avanzar (abajo) una pantalla
PageUp	Retroceder (arriba) una pantalla
DownArrow	Avanzar (abajo) una línea
UpArrow	Retroceder (arriba) una línea
d	Avanzar (abajo) la mitad de una pantalla
u	Retroceder (arriba) la mitad de una pantalla
/string	Avanzar (abajo) para buscar <i>string</i> en la página de manual
n	Repetir la búsqueda anterior más adelante (abajo) en la página del manual
N	Repetir la búsqueda anterior más atrás (arriba) en la página del manual
g	Ir al inicio de la página del manual
G	Ir al final de la página del manual
q	Salir de man y regresar al aviso de la shell de comandos



Importante

Al realizar búsquedas, el comando *string* permite usar sintaxis de expresión regular. Mientras que el texto simple (como **passwd**) funciona según lo esperado, las expresiones regulares utilizan metacaracteres (como \$, *, . y ^) para lograr una coincidencia de patrón más sofisticada. Por lo tanto, la realización de búsquedas con cadenas que incluyen metacaracteres de expresión de programa, como **make \$ \$\$**, puede arrojar resultados imprevistos.

En *Administración del sistema Red Hat II* y en el tema del manual **regex(7)** se abordan la sintaxis y las expresiones regulares.

Búsqueda de páginas de manual por palabra clave

Una búsqueda de páginas de manual por palabra clave se realiza usando la palabra clave **man -k keyword**, que arroja una lista de temas de páginas de manual con números de sección que coinciden con la palabra clave.

```
[student@desktopX ~]$ man -k passwd
checkPasswdAccess (3) - query the SELinux policy database in the kernel.
chpasswd (8)           - update passwords in batch mode
ckpasswd (8)           - nnrpd password authenticator
```

```
fgetpwent_r (3)      - get passwd file entry reentrantly  
getpwent_r (3)      - get passwd file entry reentrantly  
...  
passwd (1)          - update user's authentication tokens  
sslpasswd (1ssl)    - compute password hashes  
passwd (5)          - password file  
passwd.nntp (5)     - Passwords for connecting to remote NNTP servers  
passwd2des (3)      - RFS password encryption  
...
```

Los temas conocidos de administración del sistema se tratan en las secciones 1 (comandos del usuario), 5 (formatos de archivos) y 8 (comandos administrativos). Los administradores que emplean ciertas herramientas para la solución de problemas también recurren a la sección 2 (llamadas del sistema). Las secciones restantes generalmente se utilizan para consulta de programadores y administración avanzada.



nota

Las búsquedas por palabra clave se basan en un índice generado con el comando **mandb(8)**, que se debe ejecutar como usuario root. El comando se ejecuta a diario a través de **cron.daily** o de **anacrontab** durante la hora posterior al arranque si está desactualizado.



Importante

El comando **man**, opción **-K**, realiza una búsqueda en páginas de texto completo, no solo en títulos y descripciones, como lo hace **-k**. Una búsqueda en texto completo puede emplear mayores recursos del sistema y llevar más tiempo.



Referencias

Páginas de manual **man(1)**, **mandb(8)**, **man-pages(7)**, **less(1)**, **intro(1)**, **intro(2)**, **intro(5)**, **intro(7)**, **intro(8)**

Práctica: Uso del comando del man

En este ejercicio de laboratorio, practicará cómo encontrar información relevante con opciones y argumentos usando **man**.

Resultados

Familiarícese con el manual de sistema Linux **man** y practique cómo encontrar información útil mediante la búsqueda y la exploración.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario.

1. Visualice la página de manual **gedit(1)**.

```
[student@serverX ~]$ man 1 gedit
```

2. Investigue cómo editar un archivo específico utilizando **gedit** desde la línea de comando.

gedit filename

3. Investigue la opción **gedit** que se usa para comenzar una sesión de edición con el cursor al final del archivo.

gedit + filename

4. Investigue la página de manual **su(1)**.

```
[student@serverX ~]$ man 1 su
```

5. Investigue qué sucede con **su** cuando se omite el argumento del *nombre de usuario*.

su supone un *nombre de usuario* de **root**.

6. Investigue cómo se comporta **su** cuando se usa la opción de un solo guión.

su inicia una *shell de inicio de sesión* secundaria (crea un entorno de inicio de sesión mediante la provisión de secuencias de comandos de inicio de sesión). Sin el guío, se crea una shell de no inicio de sesión, que coincide con el entorno actual del usuario.

7. Consulte la página del manual **passwd(1)**. Determine cuáles son las opciones que bloquearán y desbloquearán una cuenta de usuario cuando este comando sea utilizado por el usuario **root**.

```
[student@serverX ~]$ man 1 passwd
```

passwd -l username

passwd -u username

8. Ubique los dos principios que debe recordar de acuerdo con los autores de las páginas **passwd man**. Busque la palabra “principio”.

- Proteja su contraseña.
- Elija una contraseña que sea difícil de descubrir.

9. Consulte la página del manual que documenta la sintaxis del archivo **/etc/passwd**. ¿Qué se almacena en el tercer campo de cada línea?

La página de manual relevante es **passwd(5)**, encontrada con **man -f passwd**.

El UID (ID de usuario numérico) para cada cuenta.

10. ¿Qué comando proporciona información detallada sobre un archivo **zip**?

zipinfo(1) encontrado con **man -k zip**

11. ¿Qué página del manual contiene una lista de los parámetros que se pueden pasar para el kernel durante el proceso de arranque?

bootparam(7) encontrado con **man -k boot**

12. ¿Qué comando se utiliza para ajustar los parámetros de sistema de archivos **ext4**?

tune2fs(8) encontrado con **man -k ext4**

Lectura de la documentación utilizando el comando pinfo

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder buscar respuestas usando la documentación de GNU Info.

Presentación de GNU Info

Las páginas de manual tienen un formato formal que resulta útil como referencia para los comandos, pero no tan útil como documentación general. Para los documentos de este tipo, como parte del proyecto GNU se creó un sistema de documentación en línea diferente, conocido como GNU info. Los documentos del sistema info son un recurso importante en un sistema Red Hat Enterprise Linux porque muchos componentes y utilidades fundamentales, como el paquete *coreutils* y las bibliotecas estándares *glibc*, se crean como parte del proyecto GNU o utilizan el sistema de documentos Info.

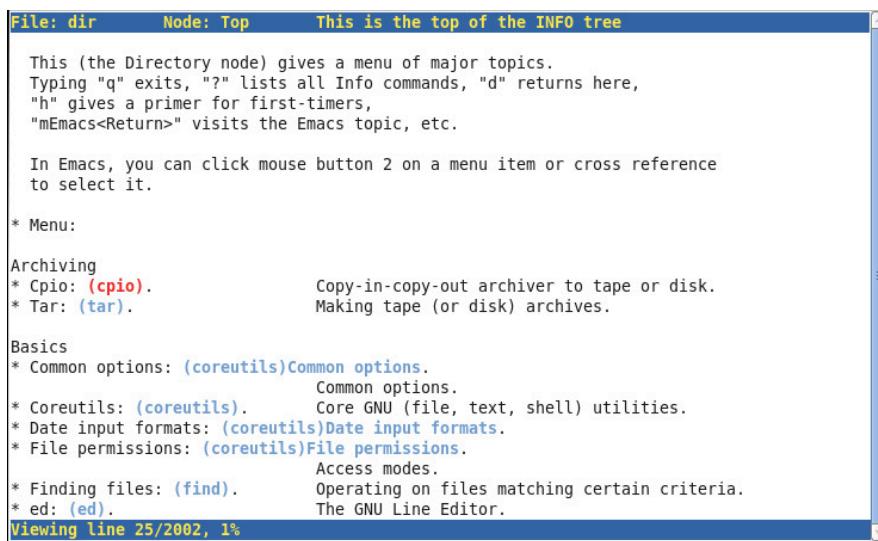


Figura 3.1: Visor de documentos Info con pinfo, directorio superior

La documentación del sistema Info se estructura en nodos de información con hipervínculos. Este formato es más flexible que las páginas del manual, lo que permite realizar análisis minuciosos de comandos y conceptos complejos. Al igual que las páginas del manual, los nodos de información se leen desde la línea de comandos mediante el uso de los comandos **info** o **pinfo**.

Algunos comandos y utilidades tienen páginas de **man** y documentación del sistema Info; por lo general, la documentación del sistema Info incluye más detalles. Compare las diferencias en la documentación **tar** usando los comandos **man** y **pinfo**:

```
[student@desktopX ~]$ man tar
[student@desktopX ~]$ pinfo tar
```

El lector de información **pinfo** es más avanzado que el comando **info** original. Ha sido diseñado para coincidir con las teclas del navegador web en modo texto **lynx**; además, incorpora colores. A fin de navegar a través de los nodos de información para un tema en particular, se utiliza **pinfo topic**. Ingrese **pinfo** solamente para el directorio de temas de información. Nuevos nodos de documentación se ponen a disposición en **pinfo** cuando se instalan sus paquetes de software correspondientes.

Comparación entre la navegación por GNU Info y la navegación por páginas del manual

El comando **info** utiliza teclas de navegación diferentes de las que usa **man**. El comando **info** ha sido diseñado para coincidir con las teclas del navegador web **lynx** que admite hipertexto. Compare los enlaces clave en la siguiente tabla:

Comandos pinfo y man: comparación de enlaces clave

Navegación	pinfo	man
Avanzar (abajo) una pantalla	PageDown o Space	PageDown o Space
Retroceder (arriba) una pantalla	PageUp o b	PageUp o b
Mostrar el directorio de temas	d	-
Avanzar (abajo) la mitad de una pantalla	-	d
Mostrar el nodo principal de un tema	u	-
Mostrar la parte superior (arriba) de un tema	INICIO	1G
Retroceder (arriba) la mitad de una pantalla	-	u
Avanzar (abajo) al siguiente hipervínculo	DownArrow	-
Abrir el tema en la posición del cursor	Ingresé	-
Avanzar (abajo) una línea	-	DownArrow o Enter
Retroceder (arriba) al hipervínculo anterior	UpArrow	-
Retroceder (arriba) una línea	-	UpArrow
Buscar un patrón	/string	/string
Mostrar siguiente nodo (capítulo) en tema	n	-
Repetir la búsqueda anterior más adelante (abajo)	/ luego Enter	n
Mostrar nodo anterior (capítulo) en tema	p	-
Repetir la búsqueda anterior más atrás (arriba)	-	N
Salir del programa	q	q



Referencias

pinfo info (*Info: Una introducción*)

- Todas las secciones

pinfo pinfo (*documentación para 'pinfo'*)

- Todas las secciones

El proyecto GNU

| <http://www.gnu.org/gnu/thegnuproject.html>

Páginas del manual: **pinfo(1)**, **info(1)**

Práctica: uso del comando pinfo

En este ejercicio de laboratorio, navegará por la documentación de GNU Info con herramientas de la línea de comandos.

Resultados

Comprender la documentación del programa en el sistema de nodos de GNU Info.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario.

1. Invoque **pinfo** sin argumentos.

```
[student@serverX ~]$ pinfo
```

2. Navegue hasta el tema **Opciones comunes**.

Utilice **UpArrow** o **DownArrow** hasta que se resalte **(coreutils) Common options**. Presione **Enter** para ver este tema.

3. Navegue a través de este tema de **info**. Aprenda si las opciones con estilo prolongado pueden abreviarse.

Utilice las teclas **PageUp** y **PageDown** para navegar por el tema. Efectivamente, muchos programas permiten que se abrevien las opciones prolongadas.

4. Determine el significado de los símbolos **--** cuando se utilizan como argumentos de comandos.

Los símbolos **--** señalan el final de las *opciones del comando* y el inicio de los *argumentos* del comando en el caso de comandos complejos en los que posiblemente el analizador de la línea de comandos de la shell no haga correctamente la distinción.

5. Sin salir de **pinfo**, desplácese hacia arriba hasta el nodo **GNU Coreutils**

Presione **u** para desplazarse hacia arriba hasta el nodo superior del tema.

6. Vuelva a desplazarse hacia arriba, hasta el tema superior.

Presione **u** nuevamente. Observe que cuando se posiciona en la parte superior del nodo de un tema, el desplazamiento hacia arriba lo regresa al directorio de temas. De manera alternativa, si presiona **d** desde cualquier nivel o tema, se desplazará directamente al directorio de temas.

7. Busque el patrón **nano** y seleccione ese tema.

Presione **/** seguida del patrón de búsqueda “nano”. Con el tema resaltado, presione **Enter**.

8. En la **Introducción**, busque y seleccione **Opciones de la línea de comandos**. Navegue por el tema.

Presione **Enter** para seleccionar **Introducción** y, luego, presione **DownArrow** y **Enter** para seleccionar **Opciones de la línea de comandos**. Navegue por el tema con las teclas de flechas.

9. Suba un nivel para regresar a **Introducción**. Avance al siguiente tema.

Presione **u** para subir un nivel. La nueva ubicación será el tema de **nano 1 Introducción**. Ahora presione **n**. Pasará al tema de **nano 2 Aspectos básicos del Editor**.

10. Salga de **pinfo**.

Presione **q** para salir de **pinfo**.

11. Invoque **pinfo** nuevamente y especifique **nano** como el tema de destino desde la línea de comandos.

```
[student@serverX ~]$ pinfo nano
```

12. Seleccione el tema **Aspectos básicos del Editor**.

Presione **DownArrow** para resaltar **Aspectos básicos del Editor** y, luego, presione **Enter** para seleccionar este tema.

13. Lea los subtemas **Introducción de texto** y **Funciones especiales**.

Utilice las teclas de flecha para resaltar un tema, **PageUp** y **PageDown** para navegar por el texto; luego, presione **u** para subir un nivel. Presione **q** para salir de **pinfo** cuando termine.

Lectura de documentación en /usr/share/doc

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder investigar información con la documentación del administrador de paquetes de Red Hat.

Presentación de la documentación de paquete

Además de `man` y `pinfo`, los desarrolladores también pueden elegir la inclusión de documentación en su paquete de distribución RPM de la aplicación. Cuando se instala el paquete, los archivos reconocidos como documentación se trasladan a `/usr/share/doc/packagename`. Los desarrolladores de paquetes de software pueden incluir cualquier cosa que consideren útil como complemento, pero que no genere una duplicación, `man` páginas. Los paquetes GNU también usan `/usr/share/doc` para complementar los nodos de información.

La mayoría de los paquetes incluye archivos que describen licencias de distribución de paquetes. Algunos paquetes incluyen amplia documentación en PDF o HTML. Del mismo modo, un método de exploración de paquete práctico es designar un explorador para `file:///usr/share/doc` y usar un mouse.

```
[student@desktopX ~]$ firefox file:///usr/share/doc
```

Algunos paquetes se presentan con ejemplos exhaustivos, plantillas de archivos de configuración, secuencias de comandos, tutoriales o guías de usuario. Explore `/usr/share/doc/vsftpd-*` como ejemplo. Alguna documentación no es suficiente; la utilidad `zip` incluye el algoritmo de compresión usado y muy poco más. Otros paquetes incluyen manuales de usuario grandes o guías para desarrollador, o copias en forma electrónica de libros publicados relacionados.



nota

Los desarrolladores pueden elegir agrupar la documentación amplia en un RPM separado. El programa `gnuplot` tiene el paquete extra `gnuplot-doc`, que debe instalarse por separado. Otros paquetes similares que se pueden explorar son `bash-doc` y `samba-doc`. A menudo, se encuentran paquetes adicionales en el canal de software *opcional* de Red Hat Enterprise Linux.

Muchos paquetes también incluyen documentación del desarrollador, como la especificación de la interfaz de programación de aplicación (API), que se proporciona en un paquete con un nombre que finaliza en `-devel` o similar. Los paquetes pueden incluir otros archivos, como encabezados; es decir, la documentación práctica que, por lo general, solo es necesaria para la compilación o el desarrollo de software.



nota

El propio kernel tiene un paquete de documentación importante. El paquete *kernel-doc* es la parte fundamental de la información del kernel, el controlador, el ajuste y la configuración avanzada. En forma habitual, los administradores experimentados del sistema investigan los archivos *kernel-doc*.



Referencias

Página de manual **hier** (7)

- Analiza la jerarquía de los directorios Linux, que incluyen **/usr/share/doc**.

Práctica: Visualización de la documentación del paquete

En este ejercicio de laboratorio, investigará la documentación que se encuentra en **/usr/share/doc** para responder preguntas. Use la opción de **less**, **gedit** o un explorador para ver el contenido del archivo de documentación.

Resultados

Conocimiento más amplio, mediante la práctica, de los tipos de información que los desarrolladores incluyen con los paquetes de software.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario.

1. ¿Dónde puede encontrar las noticias más recientes sobre el proyecto *vim*?

```
[student@serverX ~]$ cd /usr/share/doc  
[student@serverX doc]$ less vim-common-*/*README.txt
```

Visualice el *vim-common* README y busque las “noticias”.

2. ¿Cuál es el wiki URI para el paquete *yum*?

```
[student@serverX doc]$ less yum-3*/README
```

Busque el “wiki” en **/usr/share/doc/yum-3*/README**.

3. ¿Qué ejemplos se proporcionan en la calculadora **bc** de la línea de comandos?

```
[student@serverX doc]$ ls -l bc-*/*Examples
```

Se encontró en el directorio **/usr/share/doc/bc-*/Examples**.

4. ¿Cómo leería el manual GRUB2 provisto?

```
[student@serverX doc]$ firefox grub2-tools-*/*grub.html
```

Utilice **firefox** para mostrar **/usr/share/doc/grub2-tools-*/*grub.html**.

5. ¿Qué software proporciona sus documentos como un paquete separado?

```
[student@serverX doc]$ yum list *-doc*  
[student@serverX doc]$ cd  
[student@serverX ~]$
```

Use **yum** para mostrar solo aquellos paquetes que contengan “-doc”, “-docs”, or “-documentation” en el nombre de paquete. Una vez que haya finalizado, regrese al directorio de inicio.

Obtención de ayuda de Red Hat

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder ver información de la base de conocimientos y administrar casos de asistencia desde la línea de comando.

Portal de clientes de Red Hat

Con el portal de clientes de Red Hat (<https://access.redhat.com>), los clientes obtienen acceso a todo lo que se ofrece con su suscripción a través de una práctica ubicación. Los clientes pueden buscar soluciones, preguntas frecuentes y artículos a través de la base de conocimientos. Se otorga acceso a la documentación oficial de los productos. Se pueden enviar y administrar solicitudes de asistencia. Las suscripciones a productos de Red Hat pueden asignarse a sistemas registrados o puede anularse la asignación a ellos; también pueden obtenerse descargas, actualizaciones y evaluaciones de software. Hay algunas secciones del sitio de acceso público y otras exclusivas para clientes con suscripciones activas. Para obtener ayuda con el acceso al Portal de clientes, visite <https://access.redhat.com/help/>.

Los clientes pueden trabajar con el portal de clientes de Red Hat a través de un navegador web. En esta sección se presentará **redhat-support-tool**, una herramienta de línea de comandos que también puede utilizarse para obtener acceso a los servicios del portal de clientes de Red Hat.

Knowledgebase

 SOLUTIONS	 ARTICLES	 DOCUMENTATION	 VIDEOS
Find answers to questions or issues you may experience	Read technical articles and best practices for your Red Hat products	Learn how to install, configure and use your Red Hat products	Watch short tutorials and presentations for Red Hat products and events

Figura 3.2: Base de conocimientos en el portal de clientes de Red Hat

Uso de redhat-support-tool para realizar búsquedas en la base de conocimientos

La utilidad Red Hat Support Tool **redhat-support-tool** proporciona una interfaz de consola de texto para los servicios Red Hat Access que se basan en suscripciones. Hay que tener acceso a Internet para poder acceder al portal de clientes de Red Hat. La herramienta **redhat-support-tool** se basa en texto para su uso desde cualquier terminal o conexión SSH; no se proporciona ninguna interfaz gráfica.

El comando **redhat-support-tool** puede utilizarse como una shell interactiva o invocarse como si fuera un comando que se ejecuta en forma individual con opciones y argumentos. La sintaxis disponible de la herramienta es idéntica para los dos métodos. De manera predeterminada, el programa se inicia en modo de shell. Utilice el subcomando **help** proporcionado para ver todos los comandos disponibles. El modo de shell admite la compleción con el tabulador y la capacidad de solicitar programas en la shell principal.

```
[student@desktopX ~]$ redhat-support-tool
```

```
Welcome to the Red Hat Support Tool.  
Command (? for help):
```

Cuando se invoca por primera vez, **redhat-support-tool** solicita la información necesaria de inicio de sesión como suscriptor a Red Hat Access. Para evitar proporcionar esta información en reiteradas ocasiones, la herramienta le pregunta si desea almacenar la información de la cuenta en el directorio de inicio del usuario (`~/.redhat-support-tool/redhat-support-tool.conf`). Si varios usuarios comparten una cuenta de Red Hat Access, la opción `--global` permite guardar la información de la cuenta en `/etc/redhat-support-tool.conf`, junto con la configuración de todo el sistema. El comando `config` modifica los valores de configuración de la herramienta.

La herramienta **redhat-support-tool** permite que los suscriptores busquen y muestren el mismo contenido de la base de conocimientos que se ve cuando están en el portal de clientes de Red Hat. La base de conocimientos permite realizar búsquedas por palabras clave, similar al comando man. Los usuarios pueden ingresar códigos de error, sintaxis de archivos de registro o cualquier combinación de palabras clave para producir una lista de documentos de soluciones relevantes.

A continuación se incluye una demostración de búsqueda básica y configuración inicial:

```
[student@desktopX ~]$ redhat-support-tool  
Welcome to the Red Hat Support Tool.  
Command (? for help): search How to manage system entitlements with subscription-manager  
Please enter your RHN user ID: subscriber  
Save the user ID in /home/student/.redhat-support-tool/redhat-support-tool.conf (y/n): y  
Please enter the password for subscriber: password  
Save the password for subscriber in /home/student/.redhat-support-tool/redhat-support-  
tool.conf (y/n): y
```

La herramienta, tras solicitarle al usuario la configuración de usuario requerida, continúa con la solicitud de búsqueda original.

```
Type the number of the solution to view or 'e' to return to the previous menu.  
1 [ 253273:VER] How to register and subscribe a system to Red Hat Network  
(RHN) using Red Hat Subscription Manager (RHSM)?  
2 [ 17397:VER] What are Flex Guest Entitlements in Red Hat Network?  
3 [ 232863:VER] How to register machines and manage subscriptions using Red  
Hat Subscription Manager through an invisible HTTP proxy / Firewall?  
3 of 43 solutions displayed. Type 'm' to see more, 'r' to start from the beginning  
again, or '?' for help with the codes displayed in the above output.  
Select a Solution:
```

Pueden seleccionarse secciones específicas de documentos de soluciones para su visualización.

```
Select a Solution: 1  
  
Type the number of the section to view or 'e' to return to the previous menu.  
1 Title  
2 Issue  
3 Environment  
4 Resolution  
5 Display all sections  
End of options.  
Section: 1
```

```
Title
=====
How to register and subscribe a system to Red Hat Network (RHN) using Red Hat
Subscription Manager (RHSM)?
URL:      https://access.redhat.com/site/solutions/253273
(END) q
[student@desktopX ~]$
```

Acceso directo a artículos de la base de conocimientos por ID de documento

Encuentre artículos en línea en forma directa con el comando **kb** de la herramienta con la ID de documento de la base de conocimientos. Los documentos arrojados pasan por la pantalla sin paginación, lo que le permite al usuario redirigir el resultado obtenido mediante el uso de otros comandos locales. En este ejemplo, se puede ver el documento con el comando **less**.

```
[student@desktopX ~]$ redhat-support-tool kb 253273 | less

Title: How to register and subscribe a system to Red Hat Network (RHN) using Red Hat
Subscription Manager (RHSM)?
ID: 253273
State: Verified: This solution has been verified to work by Red Hat Customers and
Support Engineers for the specified product version(s).
URL: https://access.redhat.com/site/solutions/253273
: q
```

Los documentos arrojados en formato sin paginar pueden enviarse fácilmente a una impresora, convertirse a PDF u a otro formato de documento, o redirigirse a un programa de entrada de datos para seguimiento de incidentes o sistema de administración de cambios, mediante el uso de otras utilidades instaladas y disponibles en Red Hat Enterprise Linux.

Uso de redhat-support-tool para administrar casos de asistencia

Un beneficio de la suscripción a un producto es el acceso a asistencia técnica a través del portal de clientes de Red Hat. Según el nivel de soporte de suscripción del sistema, Red Hat puede comunicarse mediante herramientas en línea o por teléfono. Consulte https://access.redhat.com/site/support/policy/support_process para obtener enlaces a información detallada acerca del proceso de soporte.

Preparación de un informe de error

Antes de comunicarse con la asistencia de Red Hat, reúna información relevante para un informe de errores.

Defina el problema. Indique el problema y los síntomas con claridad. Sea lo más específico posible. Detalle los pasos que reproducirían el problema.

Reúna información básica. ¿Qué producto y versión se ven afectados? Esté preparado para brindar información de diagnóstico relevante, que puede incluir el resultado de **sosreport**, que se abordará posteriormente en esta sección. En el caso de problemas del kernel, dicha información podría incluir un vuelco de errores de **kdump** del sistema o una fotografía digital del seguimiento de kernel mostrado en el monitor de un sistema bloqueado.

Determine el nivel de gravedad. Red Hat utiliza cuatro niveles de gravedad para clasificar los problemas. Después de los informes de problemas con gravedad *urgente* y *alta*, debe

realizarse una llamada telefónica al centro de asistencia local pertinente (visite <https://access.redhat.com/site/support/contact/technicalSupport>).

Descripción de	Descripción
<i>Urgente</i> (Gravedad 1)	Un problema que afecta gravemente el uso del software en un entorno de producción (como la pérdida de los datos de producción o en las que los sistemas de producción no están funcionando). La situación interrumpe las operaciones empresariales y no existe un procedimiento de resolución.
<i>Alta</i> (Gravedad 2)	Un problema donde el software funciona, pero su uso en un entorno de producción se ve gravemente reducido. La situación tiene un gran impacto en parte de las operaciones empresariales y no existe un procedimiento de resolución.
<i>Media</i> (Gravedad 3)	Un problema que implica una pérdida parcial no fundamental de la capacidad de uso del software en un entorno de producción o desarrollo. Para los entornos de producción, hay un impacto de mediano a bajo en su negocio, pero su negocio sigue funcionando, incluso mediante el uso de una solución de proceso. Para entornos de desarrollo, donde la situación está causando que su proyecto continúe o no migre a la producción.
<i>Baja</i> (Gravedad 4)	Un asunto de uso general, la comunicación de un error de documentación o una recomendación para una mejora o modificación futura del producto. Para entornos de producción, el impacto en su negocio, en el rendimiento o en la funcionalidad de su sistema es de bajo a cero. Para los entornos de desarrollo, hay un impacto de mediano a bajo en su negocio, pero su negocio sigue funcionando, incluso mediante el uso de una solución de proceso.

Administración de un informe de errores con **redhat-support-tool**

Los suscriptores pueden crear, ver, modificar y cerrar casos de asistencia de Red Hat Support mediante el uso de **redhat-support-tool**. Cuando se abren y mantienen casos de asistencia, los usuarios pueden incluir archivos o documentación, como informes de diagnóstico (sosreport). La herramienta carga y adjunta archivos a casos en línea. Los detalles del caso, como *producto*, *versión*, *resumen*, *descripción*, *gravedad* y *grupo de caso*, pueden asignarse con opciones de comandos o si se deja la solicitud de la herramienta de información necesaria. En el siguiente ejemplo, se especifican las opciones **--product** y **--version**, pero **redhat-support-tool** proporcionará una lista de elecciones para esas opciones si el comando **opencase** no las especificó.

```
[student@desktopX ~]$ redhat-support-tool
Welcome to the Red Hat Support Tool.
Command (? for help): opencase --product="Red Hat Enterprise Linux" --version="7.0"
Please enter a summary (or 'q' to exit): System fails to run without power
Please enter a description (Ctrl-D on an empty line when complete):
When the server is unplugged, the operating system fails to continue.
1 Low
2 Normal
3 High
4 Urgent
Please select a severity (or 'q' to exit): 4
Would you like to assign a case group to this case (y/N)? N
Would see if there is a solution to this problem before opening a support case? (y/N) N
-----
```

Capítulo 3. Obtención de ayuda en Red Hat Enterprise Linux

```
Support case 01034421 has successfully been opened.
```

Inclusión de información de diagnóstico con el archivo de informe de SoS adjunto

La inclusión de información de diagnóstico cuando un caso de asistencia se crea por primera vez contribuye con una resolución del problema más rápida. El comando **sosreport** genera un archivo tar comprimido de información de diagnóstico reunida del sistema en ejecución.

La herramienta **redhat-support-tool** le pide que incluya uno en caso de que un archivo se haya creado previamente:

```
Please attach a SoS report to support case 01034421. Create a SoS report as  
the root user and execute the following command to attach the SoS report  
directly to the case:
```

```
redhat-support-tool addattachment -c 01034421 path to sosreport
```

```
Would you like to attach a file to 01034421 at this time? (y/N) N  
Command (? for help):
```

Si todavía no hay un informe SoS actual preparado, un administrador puede generar y adjuntar uno más tarde con el comando **addattachment** de la herramienta, como se recomendó anteriormente. En el ejercicio práctico de esta sección se incluirán los pasos para crear y visualizar un informe de diagnóstico SoS actual.

Usted puede ver, modificar y cerrar los casos de asistencia como suscriptor:

```
Command (? for help): listcases
```

```
Type the number of the case to view or 'e' to return to the previous menu.
```

```
1 [Waiting on Red Hat] System fails to run without power
```

```
No more cases to display
```

```
Select a Case: 1
```

```
Type the number of the section to view or 'e' to return to the previous menu.
```

```
1 Case Details
```

```
2 Modify Case
```

```
3 Description
```

```
4 Recommendations
```

```
5 Get Attachment
```

```
6 Add Attachment
```

```
7 Add Comment
```

```
End of options.
```

```
Option: q
```

```
Select a Case: q
```

```
Command (? for help):q
```

```
[student@desktopX ~]$ redhat-support-tool modifycase --status=Closed 01034421  
Successfully updated case 01034421  
[student@desktopX ~]$
```

La herramienta Red Hat Support cuenta con capacidades avanzadas de análisis y diagnóstico de aplicaciones. Mediante el uso de los archivos principales del vuelco de errores de kernel, **redhat-support-tool** puede crear y extraer un *seguimiento*, un informe de tramas de pila activas en el momento en que se realiza un vuelco de errores, para proporcionar diagnóstico in situ y abrir un caso de asistencia.

La herramienta también proporciona análisis de archivo de registro. Mediante el uso del comando **analyze** de la herramienta, los archivos de registro de muchos tipos,

como de sistema operativo, JBoss, Python, Tomcat, oVirt, etc., pueden analizarse para reconocer síntomas de problemas que pueden verse y diagnosticarse de manera individual. Proporcionar análisis preprocesado, en oposición a datos sin procesar como archivos de registro o vuelcos de errores, permite que se abran los casos de asistencia y que se pongan a disposición de ingenieros más rápidamente.



Referencias

Página del manual (1)**sosreport**

Acceso a Red Hat Access: Herramienta de soporte de Red Hat
<https://access.redhat.com/site/articles/445443>

Primer uso de la Herramienta de soporte de Red Hat
<https://access.redhat.com/site/videos/534293>

Contacto con la Asistencia técnica de Red Hat
https://access.redhat.com/site/support/policy/support_process/

Ayuda: Portal de clientes de Red Hat
<https://access.redhat.com/site/help/>

Práctica: Crear y visualizar un SoS Report

En este ejercicio de laboratorio, usará el comando sosreport para generar un SoS Report y, a continuación, visualizará el contenido de ese archivo de diagnóstico.

Resultados

Un archivo tar comprimido de información de diagnóstico de todo el sistema.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario.

- Si actualmente trabaja como usuario no root, cambie a root.

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

- Ejecute el comando **sosreport**. Esto puede demorar varios minutos en sistemas más grandes.

```
[root@serverX ~]# sosreport

sosreport (version 3.0)

This command will collect system configuration and
diagnostic information from this Red Hat Enterprise Linux
system. An archive containing the collected information
will be generated in /var/tmp and may be provided to a Red
Hat support representative or used for local diagnostic or
recording purposes.

Any information provided to Red Hat will be treated in
strict confidence in accordance with the published support
policies at:

https://access.redhat.com/support/

The generated archive may contain data considered
sensitive and its content should be reviewed by the
originating organization before being passed to any third party.

No changes will be made to system configuration.

Press ENTER to continue, or CTRL-C to quit. ENTER

Please enter your first initial and last name [serverX.example.com]: yourname
Please enter the case number that you are generating this report for: 01034421
```

Presione **Enter**. Proporcione la información solicitada. Elabore un valor para el número de caso.

```
Running 17/74: general...
Creating compressed archive...

Your sosreport has been generated and saved in:
/var/tmp/sosreport-yourname.01034421-20140129000049.tar.xz
```

```
The checksum is: b2e78125290a4c791162e68da8534887
```

```
Please send this file to your support representative.
```

- Cambie el directorio a **/var/tmp** y descomprima el archivo.

```
[root@serverX ~]# cd /var/tmp  
[root@serverX tmp]# tar -xvJf sosreport-*.tar.xz
```

- Cambie el directorio al subdirectorio resultante y explore los archivos que ahí se encuentran.

```
[root@serverX tmp]# cd sosreport-yourname.01034421-20140129000049  
[root@serverX sosreport-yourname.01034421-20140129000049]# ls -lR
```

Abra los archivos, enumere los directorios y siga explorando para conocer la información incluida en los informes SoS. Con el formato del archivo comprimido y archivado original, esta es la información de diagnóstico que adjuntará a un caso de soporte de **redhat-support-tool**. Una vez que haya finalizado, elimine el directorio del archivo y los archivos, y regrese al directorio de inicio.

```
[root@serverX sosreport-yourname.01034421-20140129000049]# cd /var/tmp  
[root@serverX tmp]# rm -rf sosreport*  
[root@serverX tmp]# exit  
[student@serverX ~]$
```

Ejercicio de laboratorio: Visualización e impresión de la documentación de ayuda

En este ejercicio de laboratorio, practicará métodos de investigación que normalmente utilizan los administradores de sistemas para aprender a realizar tareas necesarias.

Resultados

- Realice una tarea determinada; practique la realización de búsquedas en páginas **man** y en nodos **pinfo** para encontrar comandos relevantes.
- Aprenda opciones nuevas para comandos de documentación que se usan con frecuencia.
- Reconozca diversos formatos de archivos de documentos; use herramientas adecuadas para ver e imprimir documentación y otros archivos que no son texto.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario.

- Investigue **man(1)** para determinar cómo preparar una página de manual para su impresión. ¿Qué formato o lenguaje de representación se usa frecuentemente?
- Cree un archivo de salida con formato de la página de manual **passwd**. Determine el formato del contenido del archivo.
- Use **man** para investigar y conocer los comandos utilizados para ver o imprimir archivos en formato PostScript después de actualizar el caché del índice de páginas del manual.
- Investigue **evince(1)** usando **man** para aprender a usar el visor en modo de vista previa. Además, determine la manera de abrir un documento a partir de una página específica.
- Vea su archivo en formato PostScript con las diversas opciones **evince** que investigó. Cierre su archivo de documento cuando termine.
- Utilice **man** para investigar **lp(1)** y determinar cómo imprimir cualquier documento a partir de una página específica. Sin ingresar ningún comando (ya que no hay ninguna impresora), ¿qué sintaxis debería usarse, en una línea de comandos, para imprimir las páginas 2 y 3 solamente de su archivo en formato PostScript?

Una respuesta es **lp passwd.ps -P 2-3**.

Desde **lp(1)**, aprenda que la opción **-P** especifica páginas. El comando **lp** envía la solicitud de impresión a la cola de la impresora *predeterminada*, e incluye únicamente el rango de páginas que empieza en 2 y termina en 3.



nota

Actualmente, no hay impresoras configuradas en el aula. Sin embargo, quizás más adelante pueda practicar el uso de modelos de impresoras configuradas en su propio entorno. Generalmente, resulta de utilidad conocer estos comandos.

-
7. Utilice **pinfo** para buscar información sobre el visor **evince** en GNU info.
 8. Para observar la riqueza de las utilidades fundamentales de GNU, use **pinfo** para ubicar y explorar todos los nodos de documentos en busca de programas y comandos de *coreutils*.
 9. Use **firefox** para abrir el directorio de documentación de paquetes del sistema y navegue por el subdirectorio de paquetes **man-db**. Vea los manuales provistos.
 10. Use el navegador **Firefox** abierto para localizar y navegar por el subdirectorio de paquetes **initscripts**. Vea el archivo **sysconfig.txt**, en el que se describen opciones de configuración del sistema importantes almacenadas en el directorio **/etc/sysconfig**.

Solución

En este ejercicio de laboratorio, practicará métodos de investigación que normalmente utilizan los administradores de sistemas para aprender a realizar tareas necesarias.

Resultados

- Realice una tarea determinada; practique la realización de búsquedas en páginas **man** y en nodos **pinfo** para encontrar comandos relevantes.
- Aprenda opciones nuevas para comandos de documentación que se usan con frecuencia.
- Reconozca diversos formatos de archivos de documentos; use herramientas adecuadas para ver e imprimir documentación y otros archivos que no son texto.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario.

- Investigue **man(1)** para determinar cómo preparar una página de manual para su impresión. ¿Qué formato o lenguaje de representación se usa frecuentemente?

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

man utiliza **-t** a fin de preparar una página del manual para su impresión utilizando PostScript.

- Cree un archivo de salida con formato de la página de manual **passwd**. Determine el formato del contenido del archivo.

```
[student@serverX ~]$ man -t passwd > passwd.ps
[student@serverX ~]$ file passwd.ps
[student@serverX ~]$ less passwd.ps
```

El archivo está en formato PostScript, que se conoce con el comando **file** y se confirma viendo el contenido del archivo. Observe las líneas del encabezado de información de PostScript.

- Use **man** para investigar y conocer los comandos utilizados para ver o imprimir archivos en formato PostScript después de actualizar el caché del índice de páginas del manual.

```
[student@serverX ~]$ su -
Password: redhat
[root@serverX ~]# mandb
[root@serverX ~]# exit
[student@serverX ~]$ man -k postscript viewer
```

Si utiliza varias palabras con la opción **-k**, se encuentran páginas del manual que coinciden con *cualquier* palabra; las que contienen "postscript" o "visor" en sus descripciones. Observe los comandos **evince(1)** y **ghostscript(1)** (o **gs(1)**) en la salida.

- Investigue **evince(1)** usando **man** para aprender a usar el visor en modo de vista previa. Además, determine la manera de abrir un documento a partir de una página específica.

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

La opción **-w** (o **--preview**) abre **evince** en modo de vista previa. La opción **-i** se utiliza para especificar una página de inicio.

- Vea su archivo en formato PostScript con las diversas opciones **evince** que investigó. Cierre su archivo de documento cuando termine.

```
[student@serverX ~]$ evince passwd.ps
[student@serverX ~]$ evince -w passwd.ps
[student@serverX ~]$ evince -i 3 passwd.ps
```

Cuando el modo **evince** normal permite una visualización en pantalla completa y con estilo de presentación, el modo de vista previa **evince** resulta útil para tareas rápidas de navegación e impresión. Observe el ícono de impresión en la parte superior.

- Utilice **man** para investigar **lp(1)** y determinar cómo imprimir cualquier documento a partir de una página específica. Sin ingresar ningún comando (ya que no hay ninguna impresora), ¿qué sintaxis debería usarse, en una línea de comandos, para imprimir las páginas 2 y 3 solamente de su archivo en formato PostScript?

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

Una respuesta es **lp passwd.ps -P 2-3**.

Desde **lp(1)**, aprenda que la opción **-P** especifica páginas. El comando **lp** envía la solicitud de impresión a la cola de la impresora *predeterminada*, e incluye únicamente el rango de páginas que empieza en 2 y termina en 3.



nota

Actualmente, no hay impresoras configuradas en el aula. Sin embargo, quizás más adelante pueda practicar el uso de modelos de impresoras configuradas en su propio entorno. Generalmente, resulta de utilidad conocer estos comandos.

- Utilice **pinfo** para buscar información sobre el visor **evince** en GNU info.

```
[student@serverX ~]$ pinfo evince
```

Observe que, en su lugar, aparece la página de manual **evince(1)**. El visor de documentos **pinfo** busca la página de manual relevante cuando no existe ningún nodo de documentación de GNU pertinente al tema solicitado. Presione **q** para cerrar **pinfo**.

- Para observar la riqueza de las utilidades fundamentales de GNU, use **pinfo** para ubicar y explorar todos los nodos de documentos en busca de programas y comandos de *coreutils*.

```
[student@serverX ~]$ pinfo
```

Desde el nodo de directorios, presione **DownArrow** hasta que el enlace esté seleccionado para **Coreutils: utilidades centrales de GNU (archivo, texto, shell)**. Presione **Enter** para que el enlace lo lleve a **GNU Coreutils**. Observe la lista extensa del menú, en la que la opción **Introduction** está actualmente seleccionada. Presione **Enter**. En la parte superior de la pantalla, preste atención al encabezado, que muestra los nodos anterior, actual y siguiente. Navegue por la información y presione **n** para ir al siguiente nodo y repetir el paso. Navegue por cada pantalla y solo observe los comandos y sus descripciones. Continúe hasta llegar al nodo **29 Apertura de la caja de herramientas de software**. Lea completamente este capítulo usando las herramientas de navegación aprendidas. Cuando termine, regrese de la misma manera en que llegó al nodo usando *sólo* la **flecha izquierda** hasta alcanzar finalmente el nodo del directorio superior. Presione **q** para cerrar **pinfo**.

9. Use **firefox** para abrir el directorio de documentación de paquetes del sistema y navegue por el subdirectorio de paquetes **man-db**. Vea los manuales provistos.

```
[student@serverX ~]$ firefox /usr/share/doc
```

Recuerde que los directorios de uso frecuente pueden marcarse como favoritos. Después de navegar al directorio **man-db**, haga clic para abrir y ver la versión del texto del manual; luego ciérrelo. Haga clic para abrir la versión de PostScript. Como se observó anteriormente, **evince** es el visor predeterminado del sistema para documentos en formato PDF y PostScript. Puede que desee regresar a estos documentos en el futuro para obtener más conocimientos sobre **man**. Cuando termine, cierre el visor **evince**.

10. Use el navegador **Firefox** abierto para localizar y navegar por el subdirectorio de paquetes **initscripts**. Vea el archivo **sysconfig.txt**, en el que se describen opciones de configuración del sistema importantes almacenadas en el directorio **/etc/sysconfig**.

Observe la conveniencia que ofrece un navegador a la hora de localizar y visualizar documentación del sistema local. Cierre el documento cuando termine, pero deje Firefox abierto.

Resumen

Lectura de la documentación utilizando el comando man

Una descripción general del manual de Linux en formato de páginas de manual, que incluye cómo realizar tareas de navegación y búsqueda de manera eficiente.

Lectura de la documentación utilizando el comando pinfo

Una descripción general del sistema de documentación GNU Info, que incluye cómo navegar y realizar búsquedas de manera eficiente.

Lectura de documentación en /usr/share/doc

Práctica de agrupamiento de documentación con paquetes RPM que luego se almacenan en el directorio **/usr/share/doc**.

Obtención de ayuda de Red Hat

Utilice redhat-support-tool para buscar artículos en la base de conocimientos de Red Hat y administrar casos de asistencia.



CAPÍTULO 4

CREACIÓN, VISUALIZACIÓN Y EDICIÓN DE ARCHIVOS DE TEXTO

Descripción general	
Meta	Crear, visualizar y editar archivos de texto desde un resultado de comando o en un editor.
Objetivos	<ul style="list-style-type: none">Redirigir el resultado de texto de un programa a un archivo o a otro programa.Editar archivos de texto existentes y crear archivos nuevos a partir de avisos de shell con un editor de texto.Copiar texto desde una ventana gráfica a un archivo de texto con un editor de texto que se ejecute en un entorno gráfico.
Secciones	<ul style="list-style-type: none">Redirección del resultado a un archivo o programa (y práctica)Edición de archivos de texto desde el aviso de shell (y práctica)Edición de archivos de texto con un editor gráfico (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">Creación, visualización y edición de archivos de texto

Redireccionamiento de la salida a un archivo o programa

Objetivos

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

- Describir los términos técnicos "entrada estándar", "salida estándar" y "error estándar".
- Utilizar caracteres de redireccionamiento para controlar la salida a archivos.
- Usar tubería para controlar la salida a otros programas.

Entrada estándar, salida estándar y error estándar

Un programa, o un *proceso*, en ejecución necesita leer entradas desde alguna parte y escribir salidas en la pantalla o en archivos. Un comando ejecutado desde el aviso de shell normalmente lee su entrada desde el teclado y envía su salida a su ventana de terminal.

Un proceso utiliza canales numerados denominados *descriptores de archivo* para obtener entradas y enviar salidas. Todos los procesos tendrán al menos tres descriptores de archivo para comenzar. *Entrada estándar* (canal 0) lee entradas desde el teclado. *Salida estándar* (canal 1) envía una salida normal al terminal. *Error estándar* (canal 2) envía mensajes de error al terminal. Si un programa abre conexiones independientes para otros archivos, puede usar descriptores de archivo con números superiores.

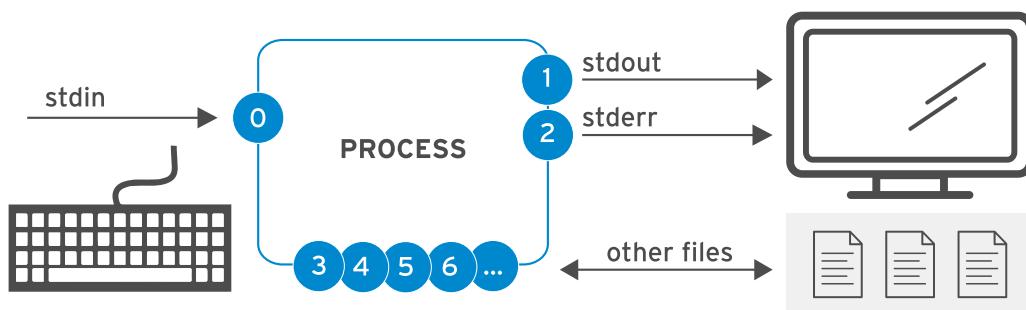


Figura 4.1: Canales de E/S de un proceso (descriptores de archivo)

Canales (descriptores de archivo)

Número	Nombre de canal	Descripción	Conexión predeterminada	Uso
0	stdin	Entrada estándar	Teclado	Solo lectura
1	stdout	Salida estándar	Terminal	Solo escritura
2	stderr	Error estándar	Terminal	Solo escritura
3+	filename	Otros archivos	<i>none (ninguno)</i>	Lectura y escritura

Redireccionamiento de la salida a un archivo

El redireccionamiento de E/S reemplaza los destinos de canales predeterminados con nombres de archivos que representan dispositivos o archivos de salida. Con el uso del redireccionamiento, los mensajes de error y la salida de un proceso que se envían generalmente a la ventana de terminal pueden capturarse como contenido de archivo, enviarse a un dispositivo o descartarse.

El redireccionamiento de **stdout** evita que la salida de un proceso aparezca en el terminal. Como se puede ver en la siguiente tabla, el redireccionamiento de **únicamente stdout** no evita que los mensajes de error **stderr** aparezcan en el terminal. Si el archivo no existe, se creará. Si el archivo existe y el redireccionamiento no es uno que se agregue al archivo, el contenido de archivo se sobrescribirá. El archivo especial **/dev/null** descarta discretamente la salida del canal redirigida a él y es siempre un archivo vacío.

Operadores de redireccionamiento de salida

Uso	Explicación	Ayuda visual
<code>>file</code>	redirigir stdout para sobrescribir un archivo	
<code>>>file</code>	redirigir stdout para agregar a un archivo	
<code>2>file</code>	redirigir stderr para sobrescribir un archivo	
<code>2>/dev/null</code>	descartar mensajes de error stderr mediante el redireccionamiento a /dev/null	
<code>>file 2>&1</code>	redirigir stdout y stderr para sobrescribir el mismo archivo	
<code>&>file</code>		

Uso	Explicación	Ayuda visual
<code>>>file 2>&1</code>	redirigir stdout y stderr para agregar al mismo archivo	
<code>&>>file</code>		



Importante

El orden de las operaciones de redireccionamiento es importante. La siguiente secuencia redirige la salida estándar a **file** y, luego, redirige el error estándar al mismo lugar que la salida estándar (**file**).

```
> file 2>&1
```

Sin embargo, la siguiente secuencia realiza el redireccionamiento en el orden opuesto. Redirige el error estándar al lugar predeterminado para la salida estándar (la ventana de terminal, de modo que no hay cambios) y, luego, redirige solo la salida estándar a **file**.

```
2>&1 > file
```

Por esto, algunas personas prefieren usar los operadores de redireccionamiento de fusión:

&>file	en lugar de	>file 2>&1
&>>file	en lugar de	>>file 2>&1 (en Bash 4 / RHEL 6 y posteriores)

Sin embargo, otros administradores de sistemas y programadores que usan además otras shells relacionadas con **bash** ("shells compatibles con Bourne") para comandos para crear scripts piensan que se deben evitar los operadores de redireccionamiento de fusión más nuevos, dado que no están estandarizados ni implementados en todas aquellas shells y tienen otras limitaciones.

Los autores de este curso tienen una postura neutral respecto de este tema, y es probable que se encuentren ambas sintaxis en el campo.

Ejemplos de redireccionamiento de salidas

El uso del redireccionamiento permite simplificar muchas tareas de administración de rutina. Use la tabla anterior como ayuda mientras aborda los siguientes ejemplos:

- Guarde un sello de fecha y hora para su posterior consulta.

```
[student@desktopX ~]$ date > /tmp/saved-timestamp
```

- Copie las últimas 100 líneas de un archivo de registro en otro archivo.

```
[student@desktopX ~]$ tail -n 100 /var/log/dmesg > /tmp/last-100-boot-messages
```

- Concatene cuatro archivos en uno.

```
[student@desktopX ~]$ cat file1 file2 file3 file4 > /tmp/all-four-in-one
```

- Detalle los nombres de archivos regulares y ocultos del directorio de inicio en un archivo.

```
[student@desktopX ~]$ ls -a > /tmp/my-file-names
```

- Adjunte salida a un archivo existente.

```
[student@desktopX ~]$ echo "new line of information" >> /tmp/many-lines-of-information  
[student@desktopX ~]$ diff previous-file current-file >> /tmp/tracking-changes-made
```

- En los siguientes ejemplos, se generan errores porque los usuarios normales no tienen acceso a los directorios del sistema. Redirija errores a un archivo mientras se visualiza la salida de un comando normal en el terminal.

```
[student@desktopX ~]$ find /etc -name passwd 2> /tmp/errors
```

- Guarde la salida de un proceso y mensajes de error en archivos separados.

```
[student@desktopX ~]$ find /etc -name passwd > /tmp/output 2> /tmp/errors
```

- Omita y descarte mensajes de error.

```
[student@desktopX ~]$ find /etc -name passwd > /tmp/output 2> /dev/null
```

- Almacene la salida y errores generados en forma conjunta.

```
[student@desktopX ~]$ find /etc -name passwd &> /tmp/save-both
```

- Adjunte la salida y errores generados en un archivo existente.

```
[student@desktopX ~]$ find /etc -name passwd >> /tmp/save-both 2>&1
```

Construcción de tubería

Una *tubería* es una secuencia de uno o más comandos separados por |, el carácter de *tubería*. Una tubería conecta la salida estándar del primer comando con la entrada estándar del siguiente comando.

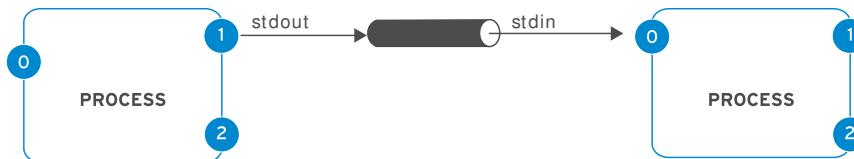


Figura 4.8: Tubería de E/S de proceso

Las tuberías permiten que la salida de un proceso sea manipulada y formateada por otros procesos antes de su salida al terminal. Una imagen mental útil es imaginar que los datos "fluyen" a través de la tubería de un proceso a otro, y que son alterados levemente por cada comando en la tubería a través de la cual pasan.



nota

Las tuberías y el redireccionamiento de E/S manipulan la salida y la entrada estándares. El *redireccionamiento* envía la salida estándar a *files* o recibe la entrada estándar de estos. Las *tuberías* envían la salida estándar a otro *proceso* o reciben la entrada estándar de este.

Ejemplos de tuberías

Este ejemplo toma la salida del comando **ls** y usa **less** para mostrarla en el terminal de a una pantalla por vez.

```
[student@desktopX ~]$ ls -l /usr/bin | less
```

La salida del comando **ls** se envía por tubería a **wc -l**, que cuenta la cantidad de líneas recibidas de **ls** y la imprime en el terminal.

```
[student@desktopX ~]$ ls | wc -l
```

En esta tubería, **head** enviará las primeras 10 líneas de salida de **ls -t**, y el resultado final se redirigirá a un archivo.

```
[student@desktopX ~]$ ls -t | head -n 10 > /tmp/ten-last-changed-files
```

Tuberías, redireccionamiento y tee

Cuando el redireccionamiento se combina con una tubería, la shell primero configura toda la tubería y, luego, redirige la entrada/salida. Esto significa que si el redireccionamiento de la salida se usa en el *medio* de una tubería, la salida irá al archivo y no al siguiente comando en la tubería.

En este ejemplo, la salida del comando **ls** irá al archivo, y **less** no mostrará nada en el terminal.

```
[student@desktopX ~]$ ls > /tmp/saved-output | less
```

El comando **tee** se usa para proporcionar soluciones alternativas para esto. En una tubería, **tee** copiará su entrada estándar y además redirigirá su salida estándar a los archivos

denominados como argumentos para el comando. Si se imaginan los datos como agua que fluye a través de una tubería, se puede visualizar **tee** como una junta en "T" en la tubería que dirige la salida en dos direcciones.

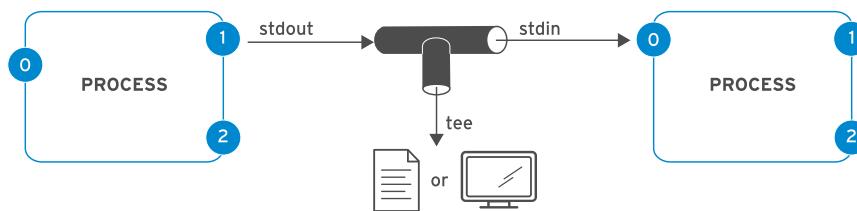


Figura 4.9: Tubería de E/S de proceso con tee

Ejemplos de tuberías que usan el comando tee

Este ejemplo redirigirá la salida del comando **ls** al archivo y la pasará a **less** para que se muestre en el terminal de a una pantalla por vez.

```
[student@desktopX ~]$ ls -l | tee /tmp/saved-output | less
```

Si **tee** se usa al final de una tubería, la salida final de un comando se puede guardar y enviar al terminal al mismo tiempo.

```
[student@desktopX ~]$ ls -t | head -n 10 | tee /tmp/ten-last-changed-files
```

Este ejemplo más sofisticado aprovecha el hecho de que existe un *archivo de dispositivo* especial que representa el terminal. El nombre del archivo de dispositivo para un terminal específico puede determinarse mediante la ejecución del comando **tty** en su aviso de shell. Luego, se puede usar **tee** para redirigir la salida a ese archivo para mostrarla en la ventana de terminal, mientras que la salida estándar se puede pasar a algún otro programa a través de la tubería. En este caso, **mail** enviará por correo electrónico la salida a student@desktop1.example.com.

```
[student@desktopX ~]$ tty
/dev/pts/0
[student@desktopX ~]$ ls -l | tee /dev/pts/0 | mail student@desktop1.example.com
```



Importante

El error estándar puede redirigirse por la tubería, pero no se pueden usar los operadores de redireccionamiento de fusión (**&>** y **&>>**) para esto.

La siguiente es la manera correcta de redirigir la salida y el error estándares a través de una tubería:

```
[student@desktopX ~]$ find -name / passwd 2>&1 | less
```



Referencias

info bash (*Manual de referencia de Bash para GNU*)

- Sección 3.2.2: Tuberías
- Sección 3.6: Redireccionamientos

info coreutils 'tee invocation' (*Manual de GNU coreutils*)

- Sección 17.1: Redireccionamiento de la salida a varios archivos o procesos

Páginas del manual: **bash(1)**, **cat(1)**, **head(1)**, **less(1)**, **mail(1)**, **tee(1)**, **tty(1)**, **wc(1)**

Práctica: Redirección y canalizaciones de E/S

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

&>/dev/null	&>file	2>/dev/null	> file 2> /dev/null
>>file 2>&1	>file 2>file2	tee file	

Resultado necesario	Sintaxis de redirección usada
Mostrar resultado de comando para el terminal; omitir todos los errores.	
Enviar resultado de comando a archivo; errores a otro archivo.	
Enviar resultado y errores al mismo archivo nuevo y vacío.	
Enviar resultado y errores al mismo archivo, pero conservar el contenido del archivo existente.	
Ejecutar un comando, pero descartar todas las pantallas de terminal posibles.	
Enviar resultado de comando tanto a la pantalla como al archivo al mismo tiempo.	
Ejecutar comando, guardar resultado en un archivo, descartar mensajes de error.	

Solución

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

Resultado necesario	Sintaxis de redirección usada
Mostrar resultado de comando para el terminal; omitir todos los errores.	2>/dev/null
Enviar resultado de comando a archivo; errores a otro archivo.	>file 2>file2
Enviar resultado y errores al mismo archivo nuevo y vacío.	&>file
Enviar resultado y errores al mismo archivo, pero conservar el contenido del archivo existente.	>>file 2>&1
Ejecutar un comando, pero descartar todas las pantallas de terminal posibles.	&>/dev/null
Enviar resultado de comando tanto a la pantalla como al archivo al mismo tiempo.	tee file
Ejecutar comando, guardar resultado en un archivo, descartar mensajes de error.	> file 2> /dev/null

Edición de archivos de texto desde el aviso de shell

Objetivos

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

- Crear archivos nuevos y editar archivos existentes de texto desde el aviso de shell.
- Navegar en un editor para realizar tareas de edición correctamente.

Editar archivos con Vim

Un principio clave de diseño de Linux es que la información se almacena en archivos basados en texto. Los archivos de texto incluyen tanto *archivos planos* con filas de información similar como archivos de configuración en **/etc**, y *archivos de Lenguaje de marcado ampliable (XML)*, los cuales definen la estructura de datos mediante etiquetas de texto, las cuales se ven en archivos de configuración de aplicaciones tanto en **/etc** como en **/usr**. La ventaja de los archivos de texto es que se pueden trasladar o compartir entre los sistemas sin necesidad de conversión, y se los puede ver y editar con cualquier editor de texto simple.

Vim es una versión mejorada del editor vi que se distribuye con los sistemas Linux y UNIX. Vim es altamente configurable y eficaz para usuarios avanzados; incluye funciones como edición en pantalla partida, formateo de color y resaltado para la edición de texto.

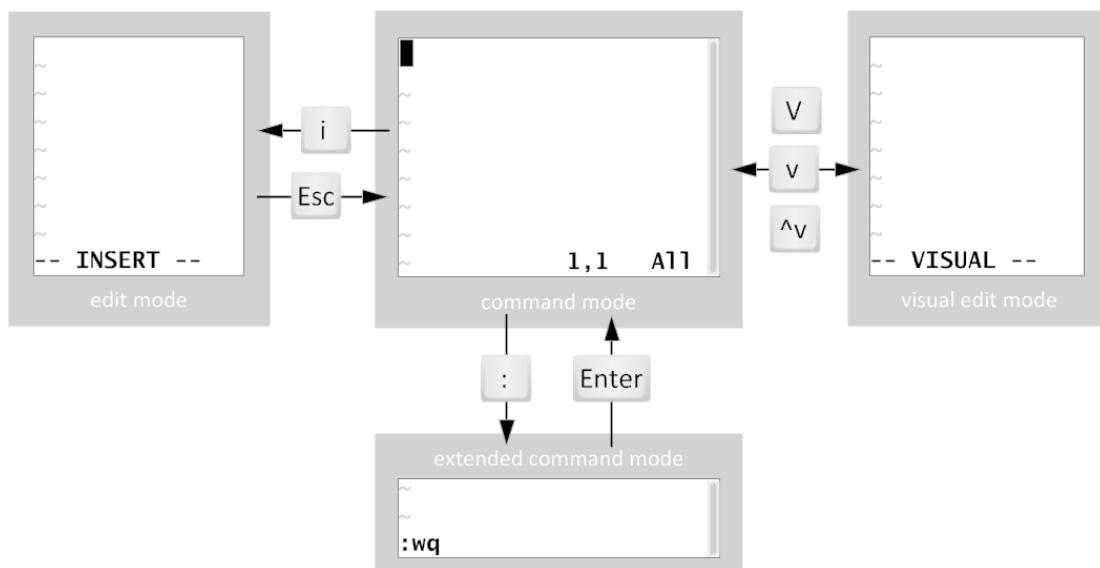


Figura 4.10: Cambio entre modos Vim

Cuando se abre por primera vez, Vim arranca en *modo comando*, utilizado para navegar, cortar y pegar, y otro tipo de manipulación de texto. Ingrese en cada uno de los otros modos con pulsaciones de tecla de caracteres únicos para acceder a funciones de edición específicas:

- Una pulsación de la tecla **i** ingresa al *modo insert*, en el cual todo el texto ingresado se convierte en contenido de archivo. Al presionar **Esc** se vuelve al modo comando.

Capítulo 4. Creación, visualización y edición de archivos de texto

- Una pulsación de la tecla **v** ingresa al *modo visual*, en el cual se pueden seleccionar varios caracteres para la manipulación de texto. Utilice **V** para líneas múltiples y **Ctrl+v** para seleccionar en bloque. La misma pulsación de tecla utilizada para ingresar al modo visual (**v**, **V** o **Ctrl+v**) se utiliza para salir.
- La pulsación de la tecla **:** comienza el *modo comando extendido* para tareas como escritura del archivo para guardararlo y salida del editor Vim.

El flujo de trabajo mínimo y básico de Vim

Vim tiene pulsaciones de teclas eficaces y coordinadas para tareas de edición avanzadas. Aunque se las considera útiles con la práctica, las capacidades de Vim pueden abrumar a los nuevos usuarios. El siguiente flujo de trabajo presenta las *mínimas* pulsaciones de tecla que todo usuario de Vim debe aprender para realizar *cualquier* tarea de edición.

El instructor demostrará una sesión típica de edición de archivo empleando solo pulsaciones de teclas básicas de Vim.

1. Abrir un archivo con **vim filename**.
2. Repetir este ciclo de entrada de texto tantas veces como lo requiera la tarea:
 - Usar las teclas de flechas para ubicar el cursor.
 - Presionar **i** para ingresar al modo insert.
 - Ingresar el texto.
 - Presionar **Esc** para volver al modo comando.
 - Si es necesario, presionar **u** para deshacer ediciones incorrectas en la línea actual.
3. Repetir este ciclo de eliminación de texto tantas veces como lo requiera la tarea:
 - Usar las teclas de flechas para ubicar el cursor.
 - Presionar **x** para eliminar un texto seleccionado.
 - Si es necesario, usar **u** para deshacer ediciones incorrectas en la línea actual.
4. Para guardar o salir, elija una de las siguientes opciones para escribir o descartar ediciones del archivo:
 - Ingresar **:w** para escribir (guardar) el archivo y permanecer en el modo comando para continuar editando.
 - Ingresar **:wq** para escribir el archivo y salir de Vim.
 - Ingresar **:q!** para salir de Vim, pero descartar todos los cambios del archivo desde la última escritura.

Reorganización de texto existente

En **Vim**, copiar y pegar se conoce como *jalar y colocar*, utilizando los caracteres de comando **y** y **p**. Comience colocando el cursor en el primer carácter que se seleccionará, luego ingrese al modo visual. Use las teclas de flechas para expandir la selección visual. Cuando esté listo, presione **y** para *yank* (copiar) lo seleccionado en la memoria. Coloque el cursor en la nueva ubicación **y**, luego, presione **p** para colocar lo seleccionado en el cursor.

El instructor demostrará “yank and put” usando el modo visual.

1. Abrir un archivo con **vim filename**.
2. Repita este ciclo de selección de texto tantas veces como lo requiera la tarea:
 - Use las teclas de flechas para colocar el cursor en el primer carácter.
 - Presione **v** para ingresar al modo visual.
 - Use las teclas de flechas para colocar el cursor en el último carácter.
 - Presione **y** para yank (copiar) lo seleccionado.
 - Use las teclas de flechas para colocar el cursor en el lugar de inserción.
 - Presione **p** para put (pegar) lo seleccionado.
3. Para guardar o salir, elija una de las siguientes opciones para escribir o descartar ediciones del archivo:
 - Ingresar **:w** para escribir (guardar) el archivo y permanecer en el modo comando para continuar editando.
 - Ingresar **:wq** para escribir el archivo y salir de Vim.
 - Ingresar **:q!** para salir de Vim, pero descartar todos los cambios del archivo desde la última escritura.



nota

Tenga la precaución de no ofrecerle al usuario avanzado de Vim atajos y trucos si no maneja bien los aspectos básicos. Se requiere práctica para que Vim sea eficaz. Se recomienda continuar aprendiendo nuevas pulsaciones de teclas para incrementar la utilidad de Vim. Quienes desean saber hasta dónde se puede extender su utilidad deben buscar en Internet “Vim tips” (sugerencias de Vim).

Se incluye una presentación detallada de **Vim** en el curso *Red Hat Enterprise Linux 7 Administración de sistemas II*.



Referencias

Página del manual (1)**vim**

Editor Vim
<http://www.vim.org/>

Práctica: Edición de archivos con Vim

En este ejercicio de laboratorio, usará un recurso instalado localmente para practicar técnicas de edición de **vim** de nivel inicial.

Resultados:

Experiencia con vim y conocimiento sobre el uso de **vimtutor** para adquirir capacidades.

Andes de comenzar

Para realizar este ejercicio, utilice el tutorial de Vim existente incluido con el editor Vim. El paquete *vim-enhanced* instalado proporciona **vimtutor**. En cada paso del ejercicio, consulte la lección correspondiente en vimtutor para practicar. Regrese aquí una vez que finalice el paso de la lección. Realice los siguientes pasos en serverX, a menos que se le indique lo contrario.

1. Abra **vimtutor**. Lea la pantalla de bienvenida y realice la Lección 1.1.

```
[student@serverX ~]$ vimtutor
```

En la clase, solo las teclas de flechas del teclado se usaron para la navegación.

Anteriormente en **vi**, los usuarios no podían confiar en las asignaciones del teclado en funcionamiento para las teclas de flechas. Por lo tanto, **vi** se diseñó con comandos mediante teclas de caracteres estándar solamente, como las teclas agrupadas convenientemente **h**, **j**, **k** y **l**. A continuación se incluye una manera de recordarlas:

hang atrás, jump abajo, kick arriba, leap adelante.

2. Regrese a la ventana **vimtutor**. Realice la Lección 1.2.

En esta lección se enseña a salir sin necesidad de conservar un cambio en un archivo no deseado. Todos los cambios se pierden, pero esto es mejor que dejar un archivo fundamental en un estado incorrecto.

3. Regrese a la ventana **vimtutor**. Realice la Lección 1.3.

Vim ofrece teclas más rápidas y eficientes para eliminar una cantidad exacta de palabras, líneas, oraciones y párrafos. Sin embargo, las tareas de edición *pueden* realizarse usando solamente **x** para la eliminación de un único carácter.

4. Regrese a la ventana **vimtutor**. Realice la Lección 1.4.

Se necesita una cantidad mínima de teclas para entrar o salir del modo de edición, usar las teclas de edición y eliminar contenido. Para la mayoría de las tareas de edición, la primera tecla que se presiona es **i**.

5. (*Opcional*) Regrese a la ventana **vimtutor**. Realice la Lección 1.5.

En la clase, solo el comando **i** (*insertar*) se enseñó como la tecla para ingresar al modo de edición. En esta lección de vimtutor se demuestra que hay otras teclas disponibles para cambiar la posición del cursor cuando se ingresa al modo de inserción. Sin embargo, una vez que se ingresa al modo de inserción, todo el texto escrito sigue siendo contenido de archivo.

-
6. Regrese a la ventana **vimtutor**. Realice la *Lección 1.6*.

Guarde el archivo; para ello, **w**escriba y **q**salga. Esta es la última lección en la que se aborda la cantidad mínima de teclas *necesaria* para realizar cualquier tarea de edición.

7. Regrese a la ventana **vimtutor**. Para finalizar, lea *Resumen de la lección 1*.

Hay otras seis lecciones que comprenden varios pasos en **vimtutor**. Ninguna ha sido asignada como lección adicional de este curso, pero no dude en usar **vimtutor** por su cuenta para adquirir más conocimientos sobre **Vim**.

Edición de archivos de texto con un editor gráfico

Objetivos

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

- Editar archivos de texto con gedit.
- Copiar texto entre ventanas gráficas.

Edición de archivos con gedit

La aplicación **gedit** es un editor de texto con todas las funciones para el entorno de escritorio GNOME. Inicie **gedit** al seleccionar **Applications > Accessories > gedit** en el menú GNOME. Al igual que otras aplicaciones gráficas, **gedit** puede iniciarse sin navegar por el menú. Presione **Alt+F2** para abrir el cuadro de diálogo **Enter a Command**. Escriba **gedit** y presione **Enter**.

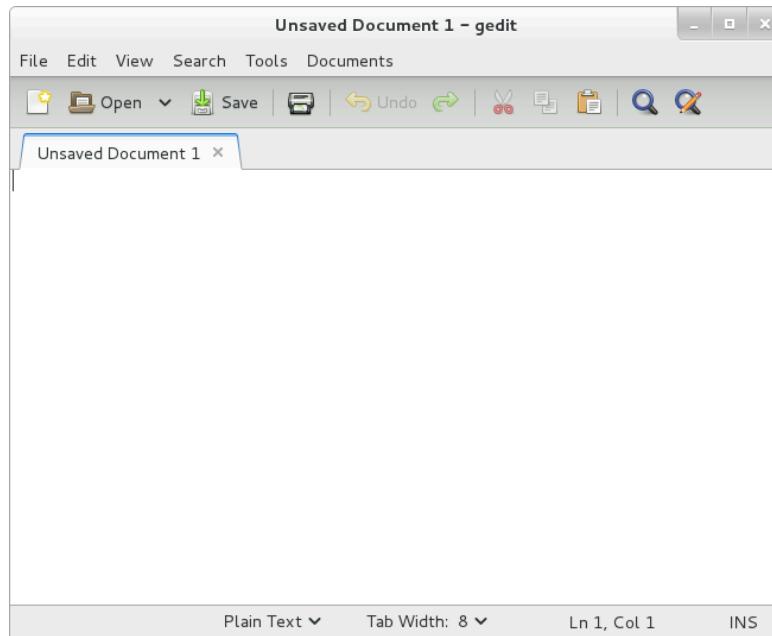


Figura 4.11: Editor de texto gedit

La ayuda de GNOME incluye una guía de ayuda **gedit** que podrá encontrar seleccionando **Applications > Favorites > Help** del menú GNOME. A continuación, seleccione **Go > All Documents** para ver la lista de aplicaciones gráficas. Desplácese hacia abajo y seleccione el hipervínculo **Text Editor**.

Teclas básicas de gedit

Realice varias tareas de administración de archivos con el menú de **gedit**:

- Para crear un archivo nuevo en gedit, haga clic en el ícono de papel en blanco de la barra de herramientas o seleccione **File > New (Ctrl+n)** del menú.

- Para guardar un archivo, haga clic en el ícono de guardar en unidad de disco duro de la barra de herramientas o seleccione **File > Save (Ctrl+s)** del menú.
- Para abrir un archivo existente, haga clic en el ícono **Open** de la barra de herramientas o seleccione **File > Open (Ctrl+o)** del menú. Aparecerá la ventana de diálogo **Open Files** y en ella los usuarios pueden buscar y seleccionar el archivo que deseen abrir.

Varios archivos pueden abrirse simultáneamente, cada uno con una sola pestaña debajo de la barra de menús. Las pestañas muestran el nombre de un archivo después de que se guardó la primera vez.

Copia de texto entre ventanas gráficas

Es posible copiar texto entre documentos, ventanas de texto y ventanas de comandos en el entorno gráfico. El texto seleccionado se duplica usando *copiar y pegar*, o se mueve usando *copiar y pegar*. Ya sea que se corte o que se copie, el texto se conserva en la memoria para pegarse en otra ubicación.

Para seleccionar texto:

- Haga clic y mantenga presionado el botón izquierdo del mouse antes del primer carácter que desea seleccionar.
- Arrastre el mouse sobre todo el texto que desea hasta que quede resaltado como una única selección y, luego, suelte el botón izquierdo. No vuelva a hacer clic en el botón izquierdo porque anulará la selección del texto.

Para pegar la selección, pueden emplearse diversos métodos y obtener el mismo resultado.

Primer método:

- Haga clic en el botón derecho del mouse en cualquier parte del área del texto que acaba de seleccionar.
- En el menú contextual que obtiene como resultado, seleccione *either cut or copy*.
- Desplace el mouse hacia la ventana o el documento donde se colocará el texto, haga clic con el botón izquierdo del mouse para posicionarlo donde debe ir el texto y haga clic con el botón derecho del mouse nuevamente; ahora, seleccione **paste**.

A continuación se incluye una técnica con el mouse más breve para practicar:

- Primero, seleccione el texto.
- Desplace el mouse sobre la ventana de destino y haga clic en el botón central del mouse solo una vez para pegar el texto en la posición del cursor.

Este último método solo permite copiar, no cortar. El texto original permanece seleccionado y puede eliminarse. Al igual que con otros métodos, el texto se conserva en la memoria y puede pegarse reiteradamente.

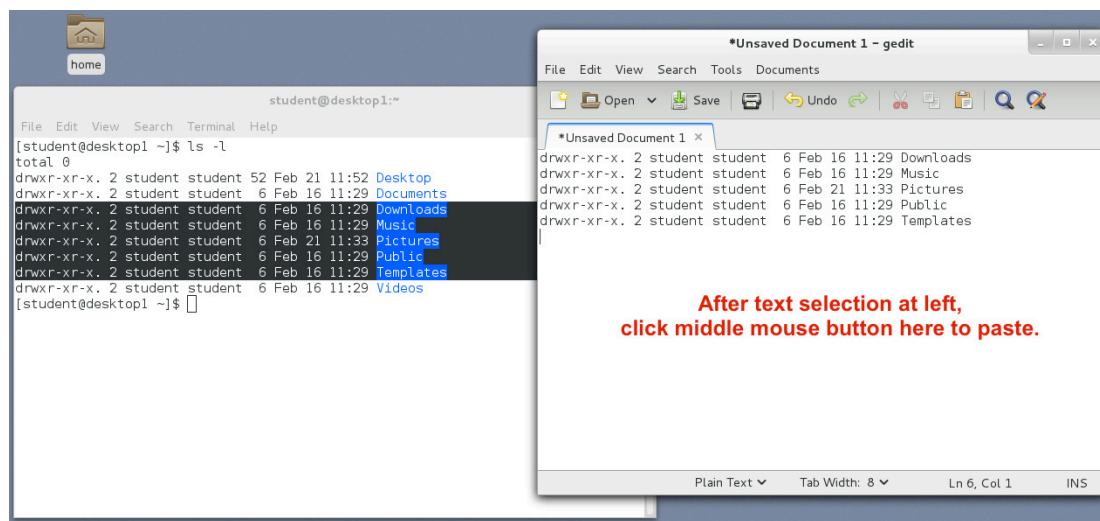


Figura 4.12: Selección y pegado de texto con el botón del medio del mouse

El método de atajo del teclado también puede usarse en aplicaciones gráficas:

- Primero, seleccione el texto.
- Use **Ctrl+c** para cortar o **Ctrl+c** para copiar el texto.
- Haga clic en la ubicación en la que el texto debe colocarse a fin de posicionar el cursor.
- Use **Ctrl+v** para pegar.



Importante

Ctrl+c y **Ctrl+v** no copiarán ni pegarán dentro de una ventana de terminal.
Ctrl+c en realidad finalizará el proceso en ejecución actual dentro de una ventana de terminal. Para copiar y pegar dentro de una ventana de terminal, use **Ctrl+Shift+c** and **Ctrl+Shift+v**.



Referencias

Página del manual (1)gedit

Editor de textos gedit

- **yelp help:gedit**

gedit Wiki

<https://wiki.gnome.org/Apps/Gedit>

Práctica: Copiado de texto entre ventanas

En este ejercicio de laboratorio, editará un archivo con gedit, seleccionará texto y lo pegará en el editor.

Resultados:

Una lista editada de archivos de configuración hallada en el directorio de inicio del usuario.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario. Inicie sesión como student y comience en el directorio de inicio de **student**.

- Redirija un listado extenso de todos los archivos del directorio de inicio, incluidos los ocultos, dentro de un archivo denominado gedit_lab.txt. Confirme que el archivo contiene el listado.

```
[student@serverX ~]$ cd
[student@serverX ~]$ ls -al > gedit_lab.txt
[student@serverX ~]$ cat gedit_lab.txt
```

- Abra el archivo con el editor de textos **gedit**. Incluya el símbolo & al final para que el aviso de la shell pueda retornar cuando se esté ejecutando **gedit**.

```
[student@serverX ~]$ gedit gedit_lab.txt &
```

- Inserte la fecha en la parte superior de su documento de archivos.
 - En la ventana de comandos de la shell, visualice la fecha de hoy con el día de la semana, el mes y el año.

```
[student@serverX ~]$ date +%A", "%B" "%d", "%Y
Friday, February 21, 2014
```

- Seleccione el texto usando el mouse.
 - Inserte el texto en la parte superior del documento de archivos. Cambie a la ventana **gedit**. Usando las teclas de flecha y coloque el cursor en la esquina superior izquierda del documento. Presione el botón medio del mouse para pegar el texto.
 - Presione **Enter** una o más veces al final del texto insertado para abrir las líneas en blanco arriba del listado de archivos.
- Inserte una descripción para este documento, que incluya su nombre de usuario y el nombre del host, en la línea 2.

Capítulo 4. Creación, visualización y edición de archivos de texto

- 4.1. En la ventana de comandos de la shell, cree texto descriptivo usando los conceptos de expansión de la shell para incluir el nombre de usuario y el nombre del host donde se generó la lista de archivos.

```
[student@serverX ~]$ echo "$USER's configuration files on" $(hostname)  
student's configuration files on serverX.example.com
```

- 4.2. Seleccione el texto usando el mouse.

```
[student@desktop1 ~]$  
[student@desktop1 ~]$ echo "$USER's configuration files on" $(hostname)  
student's configuration files on desktop1.example.com  
[student@desktop1 ~]$
```

- 4.3. Inserte el texto en la segunda línea del documento de archivos. Cambie a la ventana **gedit**. Usando las teclas de flecha, coloque el cursor en el carácter más a la izquierda de la segunda línea. Presione el botón medio del mouse para pegar el texto.

- 4.4. Presione **Enter** o **Delete**, según sea necesario, para mantener las líneas en blanco sobre el listado de archivos.

5. Elimine las líneas de archivos que no son directorios ni archivos de configuración ocultos.

- 5.1. Elimine la línea “total” al inicio del listado.

- 5.2. Elimine las dos líneas que representan el directorio actual y el directorio principal.

- 5.3. Elimine las líneas de nombres de archivos que *no* comienzan con un punto. No edite ni elimine líneas de archivos o directorios ocultos que comienzan con un punto.

6. El documento de archivos final debe ser similar a la siguiente imagen. Edite manualmente el archivo para hacer correcciones. El asterisco en la pestaña del documento o el encabezado de la ventana es un recordatorio de las ediciones que no se guardaron. Guarde el archivo y salga de gedit.

The screenshot shows a terminal window titled '*gedit_lab.txt (~) - gedit'. The window contains the following text:

```
File Edit View Search Tools Documents
Open Save Undo Redo Cut Copy Paste Find Replace
*gedit_lab.txt x
Friday, February 21, 2014
student's configuration files on desktop1.example.com

-rw----- 1 student student 194 Feb 21 16:00 .bash_history
-rw-r--r-- 1 student student 18 Aug 9 2013 .bash_logout
-rw-r--r-- 1 student student 193 Aug 9 2013 .bash_profile
-rw-r--r-- 1 student student 231 Aug 9 2013 .bashrc
drwx----- 9 student student 4096 Feb 21 16:02 .cache
drwxr-xr-x. 15 student student 4096 Feb 21 16:11 .config
-rw----- 1 student student 16 Feb 16 04:48 .esd_auth
-rw----- 1 student student 1550 Feb 21 16:02 .ICEauthority
drwx----- 3 student student 18 Feb 16 04:48 .local
drwx----- 2 student student 28 Feb 15 13:47 .ssh
```

At the bottom of the window, there are status indicators: Plain Text ▾, Tab Width: 8 ▾, Ln 12, Col 43, and INS.

Ejercicio de laboratorio: Crear, visualizar y editar archivos de texto

En este ejercicio de laboratorio, editará un archivo con el modo visual Vim para simplificar las ediciones reiteradas.

Resultados:

Conocimiento de las utilidades y técnicas requeridas para realizar la edición de archivos. El archivo final editado será una lista de los archivos seleccionados y los datos tabulares.

Antes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario. Inicie sesión como **student** y comience en el directorio de inicio de student.

1. Redirija un listado extenso de todo el contenido del directorio de inicio de student, incluidos los directorios y archivos ocultos, dentro de un archivo denominado **editing_final_lab.txt**. Es probable que los archivos del directorio de inicio no coincidan exactamente con los que se muestran en los gráficos de ejemplo. En este ejercicio de laboratorio, se editan líneas y columnas de forma arbitraria. El resultado importante es practicar el proceso de selección visual.
2. Edite el archivo con Vim para aprovechar el *modo visual*.
3. Elimine las tres primeras líneas ya que dichas líneas no son nombres de archivo habituales. Ingrese el modo visual basado en líneas con una **V** mayúscula.
4. Elimine las columnas de permiso para grupo y otros en la primera fila. En este paso, ingrese en el modo visual con la **v** minúscula, que le permite seleccionar caracteres únicamente en una sola línea.
5. Elimine las columnas de permiso para grupo y otros en el resto de las filas. Este paso usará un modo visual de selección de bloque más eficiente para evitar tener que repetir la edición de una sola línea varias veces. Esta vez, ingrese el modo visual con la secuencia de control **Ctrl+v**, que permite seleccionar un bloque de caracteres en varias líneas.
6. Elimine la columna *propietario de grupo* y deje solo una columna "student" en todas las líneas. Use la misma técnica de selección de bloque que en el último paso.
7. Elimine la columna de tiempo, pero deje el mes y el día en todas las líneas. Una vez más, use el modo visual de selección de bloque.
8. Elimine las filas **Desktop** y **Public**. Esta vez, ingrese el modo visual con la **V** mayúscula, que selecciona automáticamente las líneas completas.
9. Guarde y salga. Realice una copia de seguridad con la fecha (en segundos) para crear un nombre de archivo único.
10. Envíe los contenidos del archivo como mensaje y no como adjunto al usuario student.
11. Incluya una línea de puntos al archivo para reconocer el inicio del contenido más nuevo.

-
12. Agregue un listado de procesos completo, pero solo de procesos que son propiedad del usuario **student** actual y que se estén ejecutando en el terminal utilizado actualmente. Visualice el listado de procesos y envíelo al archivo que tenga una línea de comandos.
 13. Confirme que el listado de procesos esté en la parte inferior del archivo de ejercicio de laboratorio.

Solución

En este ejercicio de laboratorio, editará un archivo con el modo visual Vim para simplificar las ediciones reiteradas.

Resultados:

Conocimiento de las utilidades y técnicas requeridas para realizar la edición de archivos. El archivo final editado será una lista de los archivos seleccionados y los datos tabulares.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario. Inicie sesión como **student** y comience en el directorio de inicio de student.

1. Redirija un listado extenso de todo el contenido del directorio de inicio de student, incluidos los directorios y archivos ocultos, dentro de un archivo denominado **editing_final_lab.txt**. Es probable que los archivos del directorio de inicio no coincidan exactamente con los que se muestran en los gráficos de ejemplo. En este ejercicio de laboratorio, se editan líneas y columnas de forma arbitraria. El resultado importante es practicar el proceso de selección visual.

```
[student@serverX ~]$ cd  
[student@serverX ~]$ ls -al > editing_final_lab.txt
```

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

```
[student@serverX ~]$ vim editing_final_lab.txt
```

3. Elimine las tres primeras líneas ya que dichas líneas no son nombres de archivo habituales. Ingrese el modo visual basado en líneas con una **V** mayúscula.

Use las teclas de flecha para ubicar el cursor en el primer carácter de la primera fila. Ingrese el modo visual basado en líneas con **V**. Desplácese hacia abajo usando la tecla de flecha dos veces para seleccionar las primeras tres filas. Elimine las filas con **x**.

4. Elimine las columnas de permiso para grupo y otros en la primera fila. En este paso, ingrese en el modo visual con la **v** minúscula, que le permite seleccionar caracteres únicamente en una sola línea.

Use las teclas de flecha para ubicar el cursor en el primer carácter. Ingrese el modo visual con **v**. Use las teclas de flecha para ubicar el cursor en el último carácter, como se muestra en la captura de pantalla. Elimine la selección con **x**.

```
student@desktop1:~
File Edit View Search Terminal Help
-rw-----[ 1 student student 7691 Mar  5 10:56 .bash_history
-rw-r--r--[ 1 student student 18 Jan 29 05:45 .bash_logout
-rw-r--r--[ 1 student student 193 Jan 29 05:45 .bash_profile
-rw-r--r--[ 1 student student 231 Jan 29 05:45 .bashrc
drwx-----[ 12 student student 4096 Feb 22 13:23 .cache
drwxr-xr-x[ 18 student student 4096 Feb 21 11:33 .config
drwxr-xr-x[ 2 student student 6 Feb 21 20:06 Desktop
drwxr-xr-x[ 2 student student 4096 Feb 23 17:46 Documents
drwxr-xr-x[ 2 student student 6 Feb 16 11:29 Downloads
drwxr-xr-x[ 2 student student 4096 Feb 23 14:06 Music
drwxr-xr-x[ 2 student student 6 Feb 23 16:23 Pictures
drwxr-xr-x[ 2 student student 6 Feb 16 11:29 Public
drwx-----[ 2 student student 24 Feb 22 15:33 .ssh
drwxr-xr-x[ 2 student student 6 Feb 16 11:29 Templates
drwxr-xr-x[ 2 student student 4096 Feb 23 16:35 Videos
-rw-----[ 1 student student 1020 Feb 21 21:14 .viminfo
~
~
~
~
~
~
~
-- VISUAL --
```

1,11 All

5. Elimine las columnas de permiso para grupo y otros en el resto de las filas. Este paso usará un modo visual de selección de bloque más eficiente para evitar tener que repetir la edición de una sola línea varias veces. Esta vez, ingrese el modo visual con la secuencia de control **Ctrl+v**, que permite seleccionar un bloque de caracteres en varias líneas.

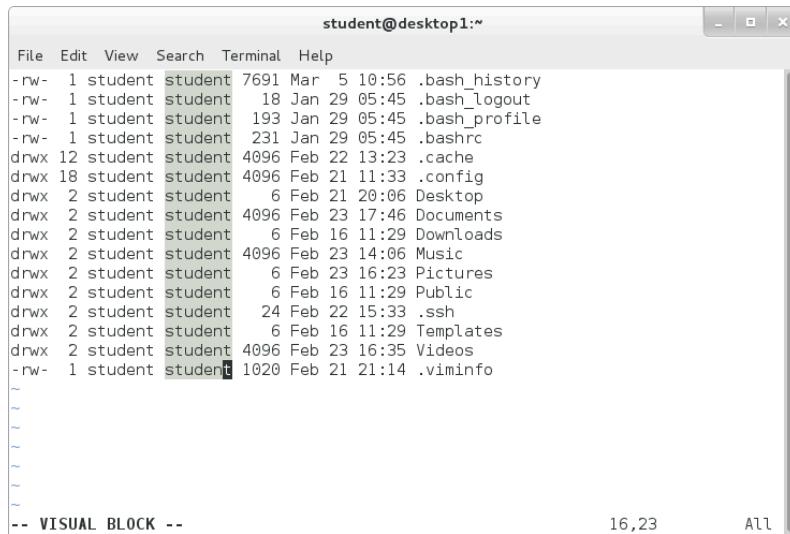
Use las teclas de flecha para ubicar el cursor en el primer carácter. Ingrese en el modo visual con la secuencia de control **Ctrl+v**. Use las teclas de flecha para ubicar el cursor en el último carácter de la columna de la última línea, como se muestra en la captura de pantalla. Elimine la selección con **x**.

```
student@desktop1:~
File Edit View Search Terminal Help
-rw- 1 student student 7691 Mar  5 10:56 .bash_history
-rw-r--r-- 1 student student 18 Jan 29 05:45 .bash_logout
-rw-r--r-- 1 student student 193 Jan 29 05:45 .bash_profile
-rw-r--r-- 1 student student 231 Jan 29 05:45 .bashrc
drwx-----[ 12 student student 4096 Feb 22 13:23 .cache
drwxr-xr-x[ 18 student student 4096 Feb 21 11:33 .config
drwxr-xr-x[ 2 student student 6 Feb 21 20:06 Desktop
drwxr-xr-x[ 2 student student 4096 Feb 23 17:46 Documents
drwxr-xr-x[ 2 student student 6 Feb 16 11:29 Downloads
drwxr-xr-x[ 2 student student 4096 Feb 23 14:06 Music
drwxr-xr-x[ 2 student student 6 Feb 23 16:23 Pictures
drwxr-xr-x[ 2 student student 6 Feb 16 11:29 Public
drwx-----[ 2 student student 24 Feb 22 15:33 .ssh
drwxr-xr-x[ 2 student student 6 Feb 16 11:29 Templates
drwxr-xr-x[ 2 student student 4096 Feb 23 16:35 Videos
-rw-----[ 1 student student 1020 Feb 21 21:14 .viminfo
~
~
~
~
~
~
~
-- VISUAL BLOCK --
```

16,11 All

6. Elimine la columna *propietario de grupo* y deje solo una columna "student" en todas las líneas. Use la misma técnica de selección de bloque que en el último paso.

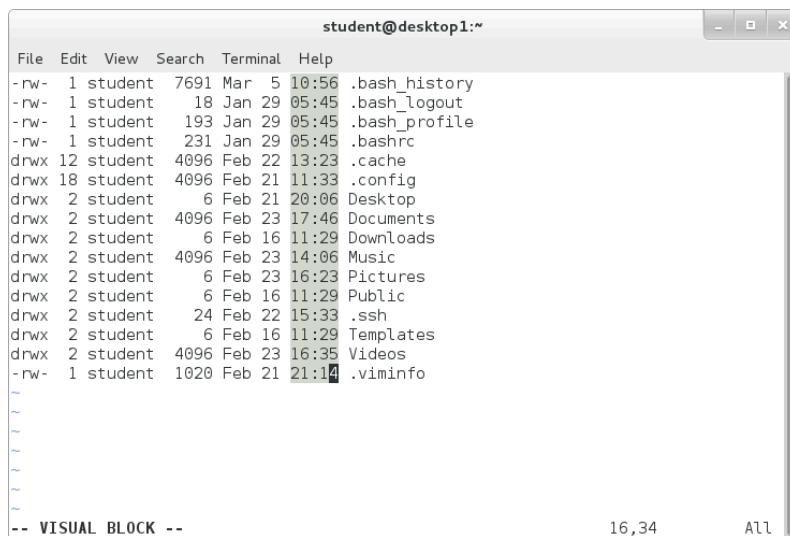
Use las teclas de flecha para ubicar el cursor en el primer carácter de la columna de propietario del grupo. Ingrese al modo visual con **Ctrl+v**. Use las teclas de flecha para ubicar el cursor en el último carácter y la última fila de la columna de propietario del grupo, como se muestra en la captura de pantalla. Elimine la selección con **x**.



```
student@desktop1:~  
File Edit View Search Terminal Help  
-rw- 1 student student 7691 Mar 5 10:56 .bash_history  
-rw- 1 student student 18 Jan 29 05:45 .bash_logout  
-rw- 1 student student 193 Jan 29 05:45 .bash_profile  
-rw- 1 student student 231 Jan 29 05:45 .bashrc  
drwx 12 student student 4096 Feb 22 13:23 .cache  
drwx 18 student student 4096 Feb 21 11:33 .config  
drwx 2 student student 6 Feb 21 20:06 Desktop  
drwx 2 student student 4096 Feb 23 17:46 Documents  
drwx 2 student student 6 Feb 16 11:29 Downloads  
drwx 2 student student 4096 Feb 23 14:06 Music  
drwx 2 student student 6 Feb 23 16:23 Pictures  
drwx 2 student student 6 Feb 16 11:29 Public  
drwx 2 student student 24 Feb 22 15:33 .ssh  
drwx 2 student student 6 Feb 16 11:29 Templates  
drwx 2 student student 4096 Feb 23 16:35 Videos  
-rw- 1 student student 1020 Feb 21 21:14 .viminfo  
~  
~  
~  
~  
~  
~  
-- VISUAL BLOCK -- 16,23 All
```

7. Elimine la columna de tiempo, pero deje el mes y el día en todas las líneas. Una vez más, use el modo visual de selección de bloque.

Use las teclas de flecha para ubicar el cursor en el primer carácter. Ingrese al modo visual con **Ctrl+v**. Use las teclas de flecha para ubicar el cursor en el último carácter y la última fila de la columna de la hora, como se muestra en la captura de pantalla. Elimine la selección con **x**.



```
student@desktop1:~  
File Edit View Search Terminal Help  
-rw- 1 student 7691 Mar 5 10:56 .bash_history  
-rw- 1 student 18 Jan 29 05:45 .bash_logout  
-rw- 1 student 193 Jan 29 05:45 .bash_profile  
-rw- 1 student 231 Jan 29 05:45 .bashrc  
drwx 12 student 4096 Feb 22 13:23 .cache  
drwx 18 student 4096 Feb 21 11:33 .config  
drwx 2 student 6 Feb 21 20:06 Desktop  
drwx 2 student 4096 Feb 23 17:46 Documents  
drwx 2 student 6 Feb 16 11:29 Downloads  
drwx 2 student 4096 Feb 23 14:06 Music  
drwx 2 student 6 Feb 23 16:23 Pictures  
drwx 2 student 6 Feb 16 11:29 Public  
drwx 2 student 24 Feb 22 15:33 .ssh  
drwx 2 student 6 Feb 16 11:29 Templates  
drwx 2 student 4096 Feb 23 16:35 Videos  
-rw- 1 student 1020 Feb 21 21:14 .viminfo  
~  
~  
~  
~  
~  
~  
-- VISUAL BLOCK -- 16,34 All
```

8. Elimine las filas **Desktop** y **Public**. Esta vez, ingrese el modo visual con la **V** mayúscula, que selecciona automáticamente las líneas completas.

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

```
student@desktop1:~$ ls -l
-rw- 1 student 7691 Mar  5 .bash_history
-rw- 1 student 18 Jan 29 .bash_logout
-rw- 1 student 193 Jan 29 .bash_profile
-rw- 1 student 231 Jan 29 .bashrc
drwx 12 student 4096 Feb 22 .cache
drwx 18 student 4096 Feb 21 .config
drwx 2 student 6 Feb 21 Desktop
drwx 2 student 4096 Feb 23 Documents
drwx 2 student 6 Feb 16 Downloads
drwx 2 student 4096 Feb 23 Music
drwx 2 student 6 Feb 23 Pictures
drwx 2 student 6 Feb 16 Public
drwx 2 student 24 Feb 22 .ssh
drwx 2 student 6 Feb 16 Templates
drwx 2 student 4096 Feb 23 Videos
-rw- 1 student 1020 Feb 21 .viminfo

```

-- VISUAL LINE -- 7,31 All

9. Guarde y salga. Realice una copia de seguridad con la fecha (en segundos) para crear un nombre de archivo único.

```
[student@serverX ~]$ cp editing_final_lab.txt editing_final_lab_$(date +%s).txt
```

10. Envíe los contenidos del archivo como mensaje y no como adjunto al usuario student.

```
[student@serverX ~]$ cat editing_final_lab.txt | mail -s "lab file" student
```

11. Incluya una línea de puntos al archivo para reconocer el inicio del contenido más nuevo.

```
[student@serverX ~]$ echo "-----" >> editing_final_lab.txt
```

12. Agregue un listado de procesos completo, pero solo de procesos que son propiedad del usuario **student** actual y que se estén ejecutando en el terminal utilizado actualmente. Visualice el listado de procesos y envíelo al archivo que tenga una línea de comandos.

```
[student@serverX ~]$ ps -f | tee -a editing_final_lab.txt
```

13. Confirme que el listado de procesos esté en la parte inferior del archivo de ejercicio de laboratorio.

```
[student@serverX ~]$ cat editing_final_lab.txt
-rw- 1 student 7691 Mar  5 .bash_history
-rw- 1 student 18 Jan 29 .bash_logout
-rw- 1 student 193 Jan 29 .bash_profile
-rw- 1 student 231 Jan 29 .bashrc
drwx 12 student 4096 Feb 22 .cache
drwx 18 student 4096 Feb 21 .config
drwx 2 student 4096 Feb 23 Documents
drwx 2 student 6 Feb 16 Downloads
drwx 2 student 4096 Feb 23 Music
drwx 2 student 6 Feb 23 Pictures
```

Capítulo 4. Creación, visualización y edición de archivos de texto

```
drwx 2 student 24 Feb 22 .ssh
drwx 2 student 6 Feb 16 Templates
drwx 2 student 4096 Feb 23 Videos
-rw- 1 student 1020 Feb 21 .viminfo

-----
UID      PID  PPID  C STIME TTY          TIME CMD
student  2005  2001  0 16:01 pts/0    00:00:00 /bin/bash
student  26923 2005  0 19:14 pts/0    00:00:00 ps -f
student  26924 2005  0 19:14 pts/0    00:00:00 tee -a editing_final_lab.txt
```

Resumen

Redireccionamiento de la salida a un archivo o programa

Descripción de cómo se visualiza, controla y guarda eficazmente la salida de un programa

Edición de archivos de texto desde el aviso de shell

Editar archivos usando Vim, un programa de edición basado en texto del administrador.

Edición de archivos de texto con un editor gráfico

Uso de un editor en un entorno de escritorio gráfico para cambiar el contenido de archivos y mover texto entre ventanas y archivos.



CAPÍTULO 5

ADMINISTRACIÓN DE USUARIOS Y GRUPOS DE LINUX LOCAL

Descripción general	
Meta	Administrar usuarios y grupos de Linux local y administrar directivas de contraseña locales.
Objetivos	<ul style="list-style-type: none">• Explicar la función de los usuarios y grupos en un sistema Linux y cómo son entendidos por la computadora.• Ejecutar comandos como superusuario para administrar el sistema Linux.• Crear, modificar, bloquear y eliminar cuentas de usuario definidas a nivel local.• Crear, modificar y eliminar cuentas de grupo definidas a nivel local.• Bloquear cuentas en forma manual o mediante la configuración de una directiva de antigüedad de contraseña en el archivo de contraseña shadow.
Secciones	<ul style="list-style-type: none">• Usuarios y grupos (y práctica)• Obtención de acceso de superusuario (y práctica)• Administración de cuentas de usuario local (y práctica)• Administración de cuentas de grupo local (y práctica)• Administración de contraseñas de usuario (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">• Administración de usuarios y grupos de Linux local

Usuarios y Grupos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder explicar el rol y cómo son entendidos, los usuarios y grupos en un sistema Linux.

¿Qué es un usuario?

Cada proceso (programa en ejecución) en el sistema se ejecuta como un usuario particular. Cada archivo es propiedad de un usuario particular. El acceso a los archivos y directorios está restringido por usuario. El usuario asociado con un proceso de ejecución determina los archivos y directorios accesibles para ese proceso.

El comando **id** se usa para mostrar información acerca del usuario con sesión iniciada actualmente. También se puede solicitar información básica de otro usuario pasando el nombre de usuario de dicho usuario como primer argumento al comando **id**.

```
[student@desktopX ~]$ id
uid=1000(student) gid=1000(student) groups=1000(student),10(wheel)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Para ver el usuario relacionado con un archivo o directorio, use el comando **ls -l**. La tercera columna muestra el nombre de usuario:

```
[student@serverX ~]$ ls -l /tmp
drwx----- 2 gdm      gdm      4096 Jan 24 13:05 orbit-gdm
drwx----- 2 student  student  4096 Jan 25 20:40 orbit-student
-rw-r--r-- 1 root     root    23574 Jan 24 13:05 postconf
```

Para ver la información del proceso, use el comando **ps**. La opción predeterminada es mostrar solo los procesos que están en la shell actual. Agregue la opción **a** para ver todos los procesos con un terminal. Para ver el usuario relacionado con un proceso, incluya la opción **u**. La primera columna muestra el nombre de usuario:

```
[student@serverX ~]$ ps au
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      428  0.0  0.7 152768 14400 tty1      Ss+ Feb03   0:04 /usr/bin/Xorg
root      511  0.0  0.0 110012  812  ttyp0      Ss+ Feb03   0:00 /sbin/agetty
root     1805  0.0  0.1 116040 2580  pts/0      Ss+ Feb03   0:00 -bash
root     2109  0.0  0.1 178468 2200  pts/0      S   Feb03   0:00 su - student
student   2110  0.0  0.1 116168 2864  pts/0      S   Feb03   0:00 -bash
student   3690  0.0  0.0 123368 1300  pts/0      R+  11:42   0:00 ps au
```

El resultado de los comandos anteriores muestra a los usuarios por nombre, pero internamente, el sistema operativo realiza el seguimiento de los usuarios por *número de UID*. La asignación de nombres a números se define en las bases de datos de la información de la cuenta. De forma predeterminada, los sistemas usan un "archivo plano o sin formato", el archivo **/etc/passwd**, para almacenar información sobre los usuarios locales. El formato de **/etc/passwd** es el siguiente (siete campos separados por dos puntos):

```
①username:②password:③UID:④GID:⑤GECOS:⑥/home/dir:⑦shell
```

- ① El *username* es una asignación de ID de usuario (UID) a un nombre para beneficio de los usuarios humanos.
- ② *password* es donde se guardaban las contraseñas en formato cifrado tradicionalmente. Actualmente, se guardan en un archivo aparte con el nombre **/etc/shadow**.
- ③ *UID* es una ID de usuario, un número que identifica al usuario en el nivel más básico.
- ④ *GID* es el número de ID de grupo principal del usuario. Los grupos se analizarán más adelante.
- ⑤ El campo *GECOS* es un texto arbitrario que, por lo general, incluye el nombre real del usuario.
- ⑥ */home/dir* es la ubicación donde se encuentran los datos personales del usuario y los archivos de configuración.
- ⑦ La *shell* es un programa que se ejecuta cuando el usuario inicia sesión. Para un usuario habitual, por lo general, este es el programa que proporciona el aviso de línea de comando del usuario.

¿Qué es un grupo?

Al igual que los usuarios, los grupos tienen un nombre y un número (GID). Los grupos locales están definidos en **/etc/group**.

Grupos principales

- Cada usuario tiene exactamente un *grupo principal*.
- Para los usuarios locales, el grupo principal está definido por el número de GID del grupo indicado en el cuarto campo de **/etc/passwd**.
- Generalmente, el grupo principal es propietario de los nuevos archivos creados por el usuario.
- Normalmente, el grupo principal de un usuario creado recientemente es un grupo creado con el mismo nombre que el del usuario. El usuario es el único miembro de este *grupo privado de usuarios* (UPG).

Grupos suplementarios

- Los usuarios pueden ser miembros de ninguno o más *grupos adicionales*.
- Los usuarios que son miembros adicionales de grupos locales se enumeran en el último campo de la entrada del grupo en **/etc/group**: Para grupos locales, la membresía del usuario se determina por una lista de usuarios separados por comas que se encuentran en el último campo de la entrada del grupo en **/etc/group**:

```
groupname:password:GID:list,of,users,in,this,group
```

- La membresía del grupo suplementario se utiliza para ayudar a asegurar que los usuarios tengan permisos para acceder a los archivos y a otros recursos en el sistema.



Referencias

Páginas del manual: **id(5)**, **passwd(5)** y **group(1)**

info libc (*Manual de referencia de la biblioteca GNU C*)

- Sección 29: Usuarios y grupos

(Tenga en cuenta que el paquete *glibc-devel* se debe haber instalado para que estos nodos de información estén disponibles).

Práctica: Conceptos de usuario y grupo

Une los siguientes elementos con sus equivalentes en la tabla.

/etc/group	/etc/passwd	GID	UID
directorio de inicio	grupo principal	shell de inicio de sesión	

Descripción	Palabra clave
Número que identifica al usuario en el nivel más fundamental	
Programa que proporciona el aviso de la línea de comando del usuario	
Ubicación de la información del grupo local	
Ubicación de los archivos personales del usuario	
Número que identifica al grupo en el nivel más fundamental	
Ubicación de la información de la cuenta de usuario local	
El cuarto campo de /etc/passwd	

Solución

Une los siguientes elementos con sus equivalentes en la tabla.

Descripción	Palabra clave
Número que identifica al usuario en el nivel más fundamental	UID
Programa que proporciona el aviso de la línea de comando del usuario	shell de inicio de sesión
Ubicación de la información del grupo local	/etc/group
Ubicación de los archivos personales del usuario	directorio de inicio
Número que identifica al grupo en el nivel más fundamental	GID
Ubicación de la información de la cuenta de usuario local	/etc/passwd
El cuarto campo de /etc/passwd	grupo principal

Obtención de acceso de superusuario

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder ejecutar comandos como superusuario para administrar un sistema Linux.

El usuario root

La mayoría de los sistemas operativos tienen una especie de *superusuario*, un usuario que tiene todo el poder sobre el sistema. Este usuario en Red Hat Enterprise Linux es el usuario **root**. Este usuario tiene el poder de anular los privilegios normales del sistema de archivos y se utiliza para manejar y administrar el sistema. Para poder realizar tareas, como la instalación o eliminación de software, y para administrar los directorios y los archivos del sistema, debe aumentar los privilegios al usuario **root**.

La mayoría de los dispositivos solo pueden ser controlados por el usuario **root**, pero existen algunas excepciones. Por ejemplo, los dispositivos desmontables, como los dispositivos USB, pueden controlarse mediante un usuario normal. Por lo tanto, se le permite a un usuario que no sea root que agregue y elimine archivos, y administre de otro modo un dispositivo desmontable, pero solo el usuario root puede administrar los discos duros "fijos" de manera predeterminada.

Sin embargo, este privilegio ilimitado viene acompañado de una responsabilidad. El usuario **root** tiene poder ilimitado para dañar el sistema: eliminar archivos y directorios, eliminar cuentas de usuarios, agregar puertas traseras, etc. Si la cuenta **root** está comprometida, alguien más tendrá control administrativo del sistema. A lo largo de este curso, se les indicará a los administradores que inicien sesión como usuario normal y que escalen los privilegios a **root** solo cuando sea necesario.

La cuenta **root** en Linux es casi equivalente a la cuenta de administrador local en Windows. En Linux, la mayoría de los administradores del sistema inicia sesión en una cuenta de usuario sin privilegios y utiliza distintas herramientas para obtener privilegios de usuario root temporalmente.



Advertencia

Una práctica habitual en Windows en el pasado es que el usuario administrador inicie sesión en forma directa para que realice las tareas de administrador del sistema. Sin embargo, en Linux se recomienda que los administradores de sistema no inicien sesión directamente como **root**. En su lugar, los administradores de sistema deben iniciar sesión como usuario no root y utilizar otros mecanismos (**su**, **sudo** o **PolicyKit**, por ejemplo) para obtener privilegios de superusuario temporalmente.

Mediante el inicio de sesión como usuario administrativo, todo el entorno de escritorio se ejecuta sin necesidad con privilegios administrativos. En esa situación, cualquier vulnerabilidad de la seguridad, que normalmente pudiera comprometer solo la cuenta del usuario, tiene el potencial de comprometer a todo el sistema.

En versiones recientes de Microsoft Windows, el administrador está inhabilitado de manera predeterminada y se usan funciones como el control de cuenta de usuario (UAC) para limitar los privilegios administrativos de los usuarios hasta que se necesiten. En Linux, el sistema **PolicyKit** es el equivalente más cercano a UAC.

Intercambio de usuarios con su

El comando **su** le permite al usuario cambiar a una cuenta de usuario diferente. Si no se especifica el nombre de usuario, se supone que es la cuenta de usuario *root*. Al ser invocado como usuario común, aparecerá un aviso que le solicitará la contraseña de la cuenta a la que cambiará, mientras que al ser invocado como usuario *root*, no deberá ingresar la contraseña de la cuenta.

su [-] <username>

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

El comando **su username** inicia una *shell de no inicio de sesión*, mientras que el comando **su - username** inicia una shell de *inicio de sesión*. La diferencia principal es que **su -** establece el entorno de la shell como si iniciara la sesión como ese usuario, mientras que **su** simplemente inicia una shell como ese usuario con la configuración de entorno actual.

En la mayoría de los casos, los administradores quieren ejecutar **su -** para obtener la configuración normal del usuario. Si desea obtener más información, consulte la página del manual **bash(1)**.



nota

El comando **su** se utiliza frecuentemente para obtener una interfaz de línea de comandos (aviso de shell) que se ejecuta como otro usuario, generalmente **root**. Sin embargo, con la opción **-c**, se puede usar como la utilidad de Windows **runas** para ejecutar un programa arbitrario como otro usuario. Vea **info su** para obtener más detalles.

Ejecución de comandos como usuario **root** con **sudo**

Fundamentalmente, Linux implementa un modelo de permisos muy general: los usuarios **root** pueden realizar todo, mientras que los demás usuarios no pueden realizar nada (relacionado con el sistema). Una solución común es permitir que los usuarios estándares “se conviertan en usuarios **root**” temporalmente con el comando **su**. La desventaja es que, mientras sea un usuario **root**, se otorgan todos los privilegios (y las responsabilidades) de un usuario **root**. El usuario no solo puede reiniciar el servidor web, sino que también puede eliminar el directorio **/etc** completo. Además, todos los usuarios que requieran privilegios de superusuario de esta manera deben conocer la contraseña de usuario **root**.

El comando **sudo** permite al usuario ejecutar un comando como usuario **root** o como otro usuario, en función de la configuración del archivo **/etc/sudoers**. A diferencia de otras herramientas, como **su**, **sudo** requiere que un usuario ingrese su propia contraseña para la autenticación y no la contraseña de la cuenta a la que intenta acceder. Esto le permite a un administrador repartir los permisos específicos a los usuarios para delegar las tareas de administración del sistema sin tener que repartir la contraseña **root**.

Por ejemplo, cuando **sudo** se configura para permitir al usuario *student* ejecutar el comando **usermod** como **root**, el usuario *student* puede ejecutar el siguiente comando a fin de bloquear una cuenta de usuario:

```
[student@serverX ~]$ sudo usermod -L username
[sudo] password for student: password
```

Un beneficio adicional de usar **sudo** es que todos los comandos ejecutados con **sudo** se registran de manera predeterminada en **/var/log/secure**.

```
[student@serverX ~]$ sudo tail /var/log/secure
...
Feb 19 15:23:36 localhost sudo: student : TTY=pts/0 ; PWD=/home/student ; USER=root ;
COMMAND=/sbin/usermod -L student
Feb 19 15:23:36 localhost usermod[16325]: lock user 'student' password
Feb 19 15:23:47 localhost sudo: student : TTY=pts/0 ; PWD=/home/student ; USER=root ;
COMMAND=/bin/tail /var/log/secure
```

En Red Hat Enterprise Linux 7, todos los miembros del grupo **wheel** pueden usar **sudo** para ejecutar comandos como cualquier usuario, que incluye al usuario **root**. Se le pedirá al usuario que ingrese su propia contraseña. Este es un cambio con respecto a Red Hat Enterprise Linux 6 y las versiones anteriores. Los usuarios que fueron miembros del grupo **wheel** no obtuvieron este acceso administrativo de manera predeterminada en RHEL 6 y en versiones anteriores.

Para habilitar comportamientos similares en versiones anteriores de Red Hat Enterprise Linux, use **visudo** a fin de editar el archivo de configuración y eliminar el comentario de la línea que permite al grupo **wheel** ejecutar todos los comandos.

```
[root@desktopX ~]# cat /etc/sudoers
...Output omitted...
## Allows people in group wheel to run all commands
%wheel          ALL=(ALL)        ALL
```

```
## Same thing without a password
# %wheel  ALL=(ALL)      NOPASSWD: ALL
...Output omitted...
```



Advertencia

RHEL 6 no otorgó ningún privilegio especial al grupo **wheel** de manera predeterminada. Es probable que los sitios que estuvieron usando este grupo se sorprendan cuando RHEL 7 otorgue en forma automática y a todos los miembros de **wheel** privilegios totales de **sudo**. Esto podría provocar que usuarios no autorizados obtengan acceso de superusuario a los sistemas RHEL 7.

Históricamente, la membresía en el grupo **wheel** se ha usado por sistemas parecidos a Unix para otorgar o controlar el acceso como superusuario.

La mayoría de las aplicaciones de administración del sistema con un GUI usan **PolicyKit** para solicitar autenticación a los usuarios y administrar el acceso como usuario root. En Red Hat Enterprise Linux 7, **PolicyKit** también puede pedir a los miembros del grupo **wheel** su propia contraseña para obtener privilegios como **root** cuando usen herramientas gráficas. Esto es parecido a la forma en que pueden usar **sudo** para obtener esos privilegios en el aviso de la shell. **PolicyKit** otorga estos privilegios según sus propios parámetros de configuración, aparte de **sudo**. Es posible que los estudiantes avanzados estén interesados en las páginas del manual **pkexec(1)** y **polkit(8)** para obtener detalles sobre cómo funciona este sistema, pero eso está fuera del alcance de este curso.



Referencias

Páginas del manual: **su** (1), **visudo** (8) y **sudo** (8)

info libc (*Manual de referencia de la biblioteca GNU C*)

- Sección 29.2: "The Persona of a Process"

(Tenga en cuenta que el paquete *glibc-devel* se debe haber instalado para que estos nodos de información estén disponibles).

Práctica: Ejecución de comandos como usuario root

En este ejercicio de laboratorio, practicará la ejecución de comandos como usuario **root**.

Resultados

Use **su** con y sin secuencias de comandos de inicio de sesión para cambiar de usuarios. Use **sudo** para ejecutar comandos con privilegios.

Antes de comenzar

Restablezca su sistema serverX.

1. Inicie sesión en el escritorio GNOME en serverX como **student** con la contraseña **student**.
2. Abra una ventana con una señal BASH.
Seleccione **Applications > Utilities > Terminal**.
3. Explore las características del entorno de inicio de sesión del estudiante actual.
 - 3.1. Visualice la información del usuario y del grupo, y muestre el directorio de trabajo actual.

```
[student@serverX ~]$ id  
uid=1000(student) gid=1000(student) groups=1000(student),10(wheel)  
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[student@serverX ~]$ pwd  
/home/student
```

- 3.2. Visualice las variables que especifican el directorio de inicio y las ubicaciones que se buscaron de los archivos ejecutables.

```
[student@serverX ~]$ echo $HOME  
/home/student  
[student@serverX ~]$ echo $PATH  
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/home/student/.local/bin:/  
home/student/bin
```

4. Cambie a root sin guión y explore las características del entorno nuevo.
 - 4.1. Convírtase en el usuario **root** en el aviso de shell.
- 4.2. Visualice la información del usuario y del grupo, y muestre el directorio de trabajo actual. Observe que la identidad haya cambiado, pero que no se haya modificado el directorio de trabajo actual.

```
[root@serverX student]# id
```

Capítulo 5. Administración de usuarios y grupos de Linux local

```
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@serverX student]# pwd
/home/student
```

- 4.3. Visualice las variables que especifican el directorio de inicio y las ubicaciones que se buscaron de los archivos ejecutables. Busque las referencias en las cuentas de **student** y **root**.

```
[root@serverX student]# echo $HOME
/root
[root@serverX student]# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/home/student/.local/bin:/
/home/student/bin
```

- 4.4. Salga de la shell para regresar al usuario **student**.

```
[root@serverX student]# exit
exit
```

5. Cambie a **root** con guión y explore las características del entorno nuevo.

- 5.1. Convírtase en el usuario **root** en el aviso de shell. Asegúrese de que también se ejecuten todas las secuencias de comandos de inicio de sesión.

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

- 5.2. Visualice la información del usuario y del grupo, y muestre el directorio de trabajo actual.

```
[root@serverX ~]# id
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@serverX ~]# pwd
/root
```

- 5.3. Visualice las variables que especifican el directorio de inicio y las ubicaciones que se buscaron de los archivos ejecutables. Busque las referencias en las cuentas de **student** y **root**.

```
[root@serverX ~]# echo $HOME
/root
[root@serverX ~]# echo $PATH
/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin
```

- 5.4. Salga de la shell para regresar al usuario **student**.

```
[root@serverX ~]# exit
logout
```

6. Ejecute varios comandos como estudiante que requieran de acceso **root**.

6.1. Visualice las 5 últimas líneas de **/var/log/messages**.

```
[student@serverX ~]$ tail -5 /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[student@serverX ~]$ sudo tail -5 /var/log/messages
Feb  3 15:07:22 localhost su: (to root) root on pts/0
Feb  3 15:10:01 localhost systemd: Starting Session 31 of user root.
Feb  3 15:10:01 localhost systemd: Started Session 31 of user root.
Feb  3 15:12:05 localhost su: (to root) root on pts/0
Feb  3 15:14:47 localhost su: (to student) root on pts/0
```

6.2. Realice una copia de seguridad de un archivo de configuración en el directorio **/etc**.

```
[student@serverX ~]$ cp /etc/motd /etc/motdOLD
cp: cannot create regular file '/etc/motdOLD': Permission denied
[student@serverX ~]$ sudo cp /etc/motd /etc/motdOLD
```

6.3. Elimine el archivo **/etc/motdOLD** que se acaba de crear.

```
[student@serverX ~]$ rm /etc/motdOLD
rm: remove write-protected regular empty file '/etc/motdOLD'? y
rm: cannot remove '/etc/motdOLD': Permission denied
[student@serverX ~]$ sudo rm /etc/motdOLD
```

6.4. Edite un archivo de configuración en el directorio **/etc**.

```
[student@serverX ~]$ echo "Welcome to class" >> /etc/motd
-bash: /etc/motd: Permission denied
[student@serverX ~]$ sudo vim /etc/motd
```

Administración de cuentas de usuarios locales

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder crear, modificar, bloquear y eliminar cuentas de usuarios definidas localmente.

Administración de usuarios locales

Se puede utilizar una serie de herramientas de la línea de comandos para administrar cuentas de usuarios locales.

useradd permite crear usuarios.

- **useradd username** define valores predeterminados razonables para todos los campos en **/etc/passwd** cuando se ejecuta sin opciones. El comando **useradd** no permite definir ninguna contraseña válida de manera predeterminada, y el usuario no puede iniciar sesión hasta que se defina una.
- **useradd --help** permite ver las opciones básicas que pueden usarse para anular los valores predeterminados. En la mayoría de los casos, las mismas opciones pueden usarse con el comando **usermod** para modificar un usuario existente.
- Algunos valores predeterminados, como el rango de números UID válidos y las reglas de vigencia de contraseñas predeterminadas, se leen desde el archivo **/etc/login.defs**. Los valores incluidos en este archivo solo se utilizan durante la creación de usuarios nuevos. Si se modifica dicho archivo, ningún usuario existente se verá afectado.

usermod permite modificar usuarios existentes.

- **usermod --help** mostrará las opciones básicas que pueden usarse para modificar una cuenta. Algunas opciones comunes incluyen las siguientes:

usermod opciones:	
-c, --comment COMMENT	Añadir un valor, como un nombre completo, al campo GECOS.
-g, --gid GROUP	Especificar el grupo principal para la cuenta del usuario.
-G, --groups GROUPS	Especificar una lista de grupos complementarios para la cuenta de usuario.
-a, --append	Se utiliza con la opción -G para anexar el usuario a los grupos complementarios mencionados sin quitarlo de otros grupos.
-d, --home HOME_DIR	Especificar un nuevo directorio de inicio para la cuenta de usuario.
-m, --move-home	Mover un nuevo directorio de inicio de usuario a una nueva ubicación. Debe usarse con la opción -d .
-s, --shell SHELL	Especificar una nueva shell de inicio de sesión para la cuenta de usuario.

usermod opciones:	
-L, --lock	Bloquear una cuenta de usuario.
-U, --unlock	Desbloquear una cuenta de usuario.

userdel permite eliminar usuarios.

- **userdel username** elimina el usuario de **/etc/passwd**, pero de manera predeterminada, no modifica el directorio principal.
- **userdel -r username** elimina el usuario y el directorio de inicio del usuario.



Advertencia

Cuando se elimina un usuario con **userdel** sin la opción **-r** especificada, el sistema tendrá archivos que pertenecen a un número de ID de usuario no asignado. Esto también puede suceder cuando los archivos creados por un usuario eliminado existen fuera de su directorio de inicio. Esta situación puede hacer que se filtre información y causar otros problemas de seguridad.

En Red Hat Enterprise Linux 7, el comando **useradd** asigna a los usuarios nuevos el primer número de UID disponible en el rango, a partir de la UID 1000 en adelante (a menos que se especifique uno explícitamente con la opción **-u *UID***). Es así como puede filtrarse información: si el primer número UID disponible ha sido asignado previamente a una cuenta de usuario que ha sido eliminada del sistema, el número de UID del usuario anterior se reasignará al nuevo usuario y le dará la propiedad de los archivos restantes del usuario anterior. A continuación se demuestra esta situación:

```
[root@serverX ~]# useradd prince
[root@serverX ~]# ls -l /home
drwx----- 3 prince prince 74 Feb 4 15:22 prince
[root@serverX ~]# userdel prince
[root@serverX ~]# ls -l /home
drwx----- 3 1000 1000 74 Feb 4 15:22 prince
[root@serverX ~]# useradd bob
[root@serverX ~]# ls -l /home
drwx----- 3 bob bob 74 Feb 4 15:23 bob
drwx----- 3 bob bob 74 Feb 4 15:22 prince
```

Observe que **bob** es ahora propietario de todos los archivos que, en otra ocasión, pertenecían a **prince**. Según la situación, una solución a este problema es eliminar todos los archivos "que no pertenecen a nadie" del sistema cuando se elimina el usuario que los creó. Otra solución es asignar manualmente los archivos "que no pertenecen a nadie" a otro usuario. El usuario root puede encontrar los archivos y directorios "que no pertenecen a nadie" al ejecutar:

find / -nouser -o -nogroup 2> /dev/null.

passwd permite definir las contraseñas.

- **passwd username** se puede usar para establecer la contraseña inicial o cambiar la contraseña del usuario.

Capítulo 5. Administración de usuarios y grupos de Linux local

- El usuario *root* puede definir una contraseña en cualquier valor. Aparecerá un mensaje si la contraseña no cumple con los criterios mínimos recomendados, seguido de un aviso para que vuelva a ingresar la contraseña nueva y todos los símbolos se actualizarán correctamente.

```
[root@serverX ~]# passwd student
Changing password for user student.
New password: redhat123
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary
word
Retype new password: redhat123
passwd: all authentication tokens updated successfully.
```

- Un usuario regular debe elegir una contraseña que tenga al menos 8 caracteres y que no sea una palabra que figure en el diccionario, el nombre de usuario ni la contraseña anterior.

Rangos de UID

Red Hat Enterprise Linux utiliza números y rangos de números de UID específicos con fines específicos.

- *UID 0* siempre se asigna a la cuenta de superusuario: **root**.
- *UID 1-200* es un rango de "usuarios del sistema" que Red Hat asignó estadísticamente a procesos del sistema.
- *UID 201-999* es un rango de "usuarios del sistema" utilizado por procesos del sistema que no tienen archivos en el sistema de archivos. Por lo general, se asignan dinámicamente de la agrupación disponible cuando el software que los necesita está instalado. Los programas se ejecutan como estos usuarios del sistema "sin privilegios" para limitar el acceso que tienen a solo los recursos que necesitan para funcionar.
- *UID 1000+* es el rango disponible para la asignación a usuarios regulares.



nota

Antes de Red Hat Enterprise Linux 7, la convención consistía en que UID 1-499 se utilizaba para usuarios del sistema y UID 500+ para usuarios regulares. Los rangos predeterminados utilizados por **useradd** y **groupadd** pueden modificarse en el archivo **/etc/login.defs**.



Referencias

Páginas del manual: **useradd(8)**, **usermod (8)**, **userdel (8)**

Práctica: Creación de usuarios usando herramientas de la línea de comandos

En este ejercicio de laboratorio, creará una serie de usuarios en su sistema serverX, y configurará y registrará una contraseña inicial para cada uno de ellos.

Resultados

Un sistema con cuentas de usuario adicionales.

Antes de comenzar

Restablezca su sistema serverX.

1. Inicie sesión en el escritorio GNOME en serverX como **student** con la contraseña **student**.
2. Abra una ventana con una señal BASH.
Seleccione **Applications > Utilities > Terminal**.
3. Conviértase en el usuario **root** en el aviso de shell.

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

4. Agregue el usuario *juliet*.

```
[root@serverX ~]# useradd juliet
```

5. Confirme que *juliet* se haya agregado examinando el archivo **/etc/passwd**.

```
[root@serverX ~]# tail -2 /etc/passwd  
tcpdump:x:72:72:::/sbin/nologin  
juliet:x:1001:1001::/home/juliet:/bin/bash
```

6. Utilice el comando **passwd** para inicializar la contraseña de *juliet*.

```
[root@serverX ~]# passwd juliet  
Changing password for user juliet.  
New password: juliet  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password: juliet  
passwd: all authentication tokens updated successfully.
```

7. Continúe con los siguientes pasos para añadir los usuarios restantes y configurar contraseñas iniciales.

7.1. romeo

```
[root@serverX ~]# useradd romeo
```

```
[root@serverX ~]# passwd romeo
Changing password for user romeo.
New password: romeo
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: romeo
passwd: all authentication tokens updated successfully.
```

7.2. hamlet

```
[root@serverX ~]# useradd hamlet
[root@serverX ~]# passwd hamlet
```

7.3. reba

```
[root@serverX ~]# useradd reba
[root@serverX ~]# passwd reba
```

7.4. dolly

```
[root@serverX ~]# useradd dolly
[root@serverX ~]# passwd dolly
```

7.5. elvis

```
[root@serverX ~]# useradd elvis
[root@serverX ~]# passwd elvis
```

Administración de cuentas de grupos locales

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder crear, modificar y eliminar cuentas de grupos definidas localmente.

Administración de grupos adicionales

Para que un usuario pueda agregarse a un grupo, primero debe crearse el grupo. Se emplean diversas herramientas de la línea de comandos para administrar cuentas de grupos locales.

El comando crea grupos.**groupadd**

- **groupadd groupname** sin opciones emplea la siguiente GID disponible de un rango especificado en el archivo **/etc/login.defs**.
- La opción **-g GID** se utiliza para especificar una GID particular.

```
[student@serverX ~]$ sudo groupadd -g 5000 ateam
```



nota

Dada la creación automática de grupos privados de usuarios (GID 1000+), generalmente se recomienda establecer aparte un rango de números de GID para su uso con los grupos adicionales. Un rango más alto evitará una colisión con un grupo del sistema (GID 0-999).

- La opción **-r** creará un grupo del sistema usando una GID del rango de números de GID del sistema válido incluidos en el archivo **/etc/login.defs**.

```
[student@serverX ~]$ sudo groupadd -r appusers
```

El comando **groupmod** modifica grupos existentes.

- El comando **groupmod** se utiliza para cambiar el nombre de un grupo por una asignación de GID. La opción **-n** se usa para especificar un nombre nuevo.

```
[student@serverX ~]$ sudo groupmod -n javaapp appusers
```

- La opción **-g** se usa para especificar una GID nueva.

```
[student@serverX ~]$ sudo groupmod -g 6000 ateam
```

El comando **groupdel** elimina un grupo.

- El comando **groupdel** quita un grupo.

```
[student@serverX ~]$ sudo groupdel javaapp
```

- Es posible que un grupo no se quite si es el grupo principal de cualquier usuario existente. Como en el caso de **userdel**, controle todos los sistemas de archivos para asegurarse de que ningún archivo siga siendo propiedad del grupo.

El comando **usermod** modifica la pertenencia a grupos.

- La pertenencia a un grupo se controla con la administración de usuarios. Cambie el grupo principal de un usuario con **usermod -g groupname**.

```
[student@serverX ~]$ sudo usermod -g student student
```

- Añada un usuario a un grupo adicional con **usermod -aG groupname username**.

```
[student@serverX ~]$ sudo usermod -aG wheel elvis
```



Importante

El uso de la opción **-a** hace que **usermod** funcione en modo "adición". Sin esta, el usuario se eliminaría de *todos los demás* grupos adicionales.

Referencias

Páginas del manual: **group(5)**, **groupadd(8)**, **groupdel(8)** y **usermod(8)**



Práctica: Administración de grupos utilizando herramientas de línea de comandos

En este ejercicio de laboratorio, agregará usuarios a grupos adicionales creados recientemente.

Resultados

El grupo **shakespeare** está formado por **juliet**, **romeo** y **hamlet**. El grupo **artists** está formado por **reba**, **dolly** y **elvis**.

Andes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario.

1. Conviéntase en el usuario **root** en el aviso de shell.

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

2. Cree un grupo suplementario con el nombre **shakespeare** y con la ID de grupo **30000**.

```
[root@serverX ~]# groupadd -g 30000 shakespeare
```

3. Cree un grupo suplementario con el nombre **artists**.

```
[root@serverX ~]# groupadd artists
```

4. Confirme que *shakespeare* y *artists* se hayan agregado al examinar el archivo **/etc/group**.

```
[root@serverX ~]# tail -5 /etc/group  
reba:x:1004:  
dolly:x:1005:  
elvis:x:1006:  
shakespeare:x:30000:  
artists:x:30001:
```

5. Agregue el usuario *juliet* al grupo *shakespeare* como grupo suplementario.

```
[root@serverX ~]# usermod -G shakespeare juliet
```

6. Confirme que *juliet* se haya agregado mediante el uso del comando **id**.

```
[root@serverX ~]# id juliet  
uid=1001(juliet) gid=1001(juliet) groups=1001(juliet),30000(shakespeare)
```

7. Continúe agregando el resto de los usuarios a los grupos como se indica a continuación:

7.1. Agregue *romeo* y *hamlet* al grupo *shakespeare*.

```
[root@serverX ~]# usermod -G shakespeare romeo
[root@serverX ~]# usermod -G shakespeare hamlet
```

7.2. Agregue *reba*, *dolly* y *elvis* al grupo *artists*.

```
[root@serverX ~]# usermod -G artists reba
[root@serverX ~]# usermod -G artists dolly
[root@serverX ~]# usermod -G artists elvis
```

7.3. Compruebe las membresías del grupo complementario mediante el archivo **/etc/group**.

```
[root@serverX ~]# tail -5 /etc/group
reba:x:1004:
dolly:x:1005:
elvis:x:1006:
shakespeare:x:30000:juliet,romeo,hamlet
artists:x:30001:reba,dolly,elvis
```

Administración de contraseñas de usuarios

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder bloquear cuentas manualmente o definiendo una política de vigencia de contraseñas en el archivo de contraseña "shadow".

Contraseñas shadow y política de contraseñas

Hace muchos años, las contraseñas cifradas se almacenaban en el archivo /etc/passwd de lectura global. Se pensaba que esta ubicación era bastante segura hasta que los ataques de diccionarios a contraseñas cifradas se volvieron frecuentes. En ese momento, las contraseñas cifradas o "hashes de contraseña", se trasladaron al archivo /etc/shadow más seguro. Este nuevo archivo también permitió la implementación de características de vigencia y caducidad de la contraseña.

Un hash de contraseña moderno almacena tres datos:

\$1\$gCjLa2/Z\$6Pu0EK0AzfCjxjv2hoL0B/

1. **1**: el algoritmo hash. El número 1 indica un hash MD5. El número 6 aparece cuando se usa un hash SHA-512.
2. **gCjLa2/Z**: el valor *aleatorio* utilizado para cifrar el hash. Originalmente, se elige al azar. El valor aleatorio y la contraseña no cifrada se combinan y se cifran para crear el hash de contraseña cifrado. El uso del valor aleatorio evita que dos usuarios con la misma contraseña tengan entradas idénticas en el archivo **/etc/shadow**.
3. **6Pu0EK0AzfCjxjv2hoL0B/**: el hash cifrado.

Cuando un usuario intenta iniciar sesión, el sistema busca la entrada correspondiente al usuario en **/etc/shadow**, combina el valor aleatorio del usuario con la contraseña sin cifrar que se ingresó y los cifra usando el algoritmo de hash especificado. Si el resultado coincide con el hash cifrado, el usuario ingresó la contraseña correcta. Si el resultado no coincide con el hash cifrado, el usuario ingresó una contraseña incorrecta y el intento de inicio de sesión falla. Este método permite que el sistema determine si el usuario ingresó la contraseña correcta sin almacenarla en una forma que se puede usar en el inicio de sesión.



nota

Red Hat Enterprise Linux 6 y 7 admiten dos nuevos algoritmos de hash de contraseñas sólidos: SHA-256 (algoritmo **5**) y SHA-512 (algoritmo **6**). Tanto la cadena del valor aleatorio como el hash cifrado son más extensos para estos algoritmos. El usuario **root** puede cambiar el algoritmo predeterminado que se utiliza para hashes de contraseñas ejecutando el comando **authconfig --passalgo** con alguno de los argumentos **md5**, **sha256** o **sha512**, según corresponda.

Red Hat Enterprise Linux 7 utiliza el cifrado SHA-512 de manera predeterminada.

/etc/shadow formato

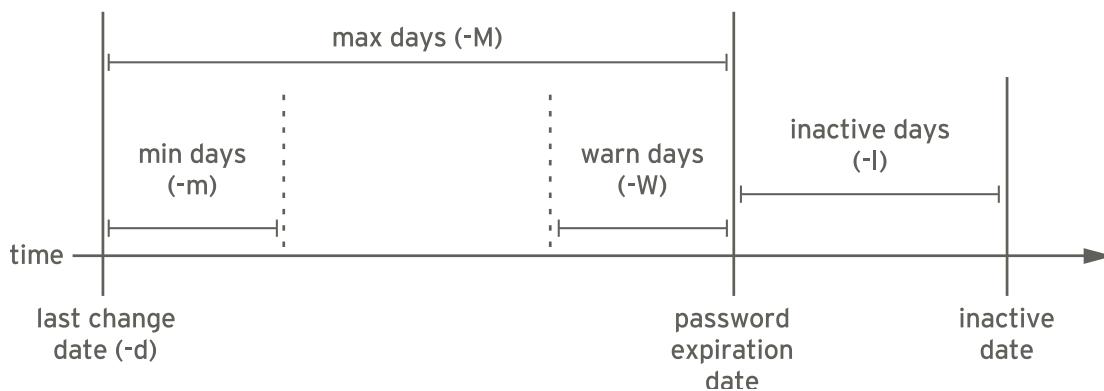
El formato de **/etc/shadow** es el siguiente (nueve campos separados por dos puntos):

① name: ② password: ③ lastchange: ④ minage: ⑤ maxage: ⑥ warning: ⑦ inactive: ⑧ expire: ⑨ blank

- ① El *nombre* de inicio de sesión. Debe ser un nombre de cuenta válido en el sistema.
- ② La *contraseña* cifrada. Si un campo de contraseña comienza con un signo de admiración, la contraseña está bloqueada.
- ③ La fecha de la última *modificación de la contraseña*, que se representa como la cantidad de días desde 1970.01.01.
- ④ La cantidad *mínima* de días que deben transcurrir para que una contraseña pueda modificarse; 0 significa "ningún requisito mínimo de vigencia".
- ⑤ La cantidad *máxima* de días que deben transcurrir para que una contraseña deba modificarse.
- ⑥ El período de *advertencia* de que una contraseña está a punto de caducar. Se representa en días; 0 significa que "no se proporciona ninguna advertencia".
- ⑦ La cantidad de días que una cuenta permanece activa después de que una contraseña caduca. Un usuario aún puede iniciar sesión en el sistema y modificar la contraseña durante ese período. Una vez transcurridos los días especificados, la cuenta se bloquea y se vuelve *inactiva*.
- ⑧ La fecha de *caducidad* de la cuenta, que se representa como la cantidad de días desde el 1970.01.01.
- ⑨ Este campo en *blanco* se reserva para su uso en el futuro.

Vigencia de contraseñas

En el siguiente diagrama, se indican los parámetros de vigencia de contraseñas relevantes que pueden ajustarse mediante **chage** para implementar una política de vigencia de contraseñas.



```
[root@serverX ~]# chage -m 0 -M 90 -W 7 -I 14 username
```

chage -d 0 username forzará que se actualice la contraseña en el próximo inicio de sesión.

chage -l username enumerará los valores de configuración actuales del nombre de usuario.

chage -E YYYY-MM-DD username expirá una cuenta un día específico.



nota

El comando **date** puede usarse para calcular una fecha en el futuro.

```
[student@serverX ~]$ date -d "+45 days"
Sat Mar 22 11:47:06 EDT 2014
```

Restricción del acceso

Con el comando **chage**, puede definirse la caducidad de una cuenta. Cuando se alcanza la fecha, el usuario no puede iniciar sesión en el sistema de manera interactiva. El comando **usermod** puede "bloquear" una cuenta con la opción **-L**.

```
[student@serverX ~]$ sudo usermod -L elvis
[student@serverX ~]$ su - elvis
Password: elvis
su: Authentication failure
```

Cuando un usuario se va de una empresa, el administrador puede bloquear una cuenta y determinar su caducidad con el comando **usermod** solamente. La fecha debe indicarse como la cantidad de días desde 1970.01.01.

```
[student@serverX ~]$ sudo usermod -L -e 1 elvis
```

El bloqueo de la cuenta evita que el usuario logre la autenticación con una contraseña en el sistema. Esta es la forma recomendada de evitar que un empleado que se fue de la empresa acceda a su cuenta. Si el empleado regresa, la cuenta puede desbloquearse con **usermod -U USERNAME**. Si la cuenta también caducó, asegúrese de modificar, además, la fecha de caducidad.

La shell **nologin**

En ocasiones, un usuario necesita una cuenta con una contraseña para realizar la autenticación en un sistema, pero no necesita una shell interactiva en el sistema. Por ejemplo, un servidor de correo puede necesitar una cuenta para el almacenamiento de correo y una contraseña para que el usuario realice la autenticación con un cliente de correo utilizado para recuperar correo. Dicho usuario no debe iniciar sesión directamente en el sistema.

Ante una situación como la anterior, una solución común es definir la shell de inicio de sesión del usuario en **/sbin/nologin**. Si el usuario intenta iniciar sesión en el sistema directamente, la "shell" **nologin** simplemente cerrará la conexión.

```
[root@serverX ~]# usermod -s /sbin/nologin student
[root@serverX ~]# su - student
Last login: Tue Feb  4 18:40:30 EST 2014 on pts/0
This account is currently not available.
```



Importante

El uso de la shell **nologin** evita el uso interactivo del sistema, pero no evita todo el acceso. Un usuario puede, de todas maneras, realizar la autenticación y cargar o recuperar archivos a través de aplicaciones, como aplicaciones web, programas de transferencia de archivos o lectores de correo.



Referencias

Páginas del manual: **chage(8)**, **usermod(5)**, **shadow(3)**, **crypt(1)**

Práctica: Administración de la antigüedad de la contraseña de usuario

En este ejercicio de laboratorio, configurará directivas de contraseña únicas para los usuarios.

Resultados

La contraseña para **romeo** debe cambiarse cuando el usuario inicie sesión por primera vez en el sistema y cada 90 días en lo sucesivo; la cuenta vence a los 180 días.

Antes de comenzar

Realice los siguientes pasos en serverX, a menos que se le indique lo contrario.

1. Explore la opción de bloquear y desbloquear cuentas.

- 1.1. Bloquee la cuenta **romeo**.

```
[student@serverX ~]$ sudo usermod -L romeo
```

- 1.2. Intente iniciar sesión como **romeo**.

```
[student@serverX ~]$ su - romeo  
Password: romeo  
su: Authentication failure
```

- 1.3. Desbloquee la cuenta **romeo**.

```
[student@serverX ~]$ sudo usermod -U romeo
```

2. Cambie la directiva de contraseña para **romeo** a fin de solicitar una contraseña nueva cada 90 días.

```
[student@serverX ~]$ sudo chage -M 90 romeo  
[student@serverX ~]$ sudo chage -l romeo  
Last password change : Feb 03, 2014  
Password expires : May 04, 2014  
Password inactive : never  
Account expires : never  
Minimum number of days between password change : 0  
Maximum number of days between password change : 90  
Number of days of warning before password expires : 7
```

3. Además, establezca que el cambio de contraseña sea obligatorio en el primer inicio de sesión en la cuenta **romeo**.

```
[student@serverX ~]$ sudo chage -d 0 romeo
```

4. Inicie sesión como **romeo** y cambie la contraseña a **forsooth123**.

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

```
Password: romeo
You are required to change your password immediately (root enforced)
Changing password for romeo.
(current) UNIX password: romeo
New password: forsooth123
Retype new password: forsooth123
[romeo@serverX ~]$ exit
```

5. Vencimiento futuro de las cuentas

5.1. Determine la fecha de vencimiento en 180 días.

```
[student@serverX ~]$ date -d "+180 days"
Sat Aug 2 17:05:20 EDT 2014
```

5.2. Configure el vencimiento de las cuentas en esa fecha.

```
[student@serverX ~]$ sudo chage -E 2014-08-02 romeo
[student@serverX ~]$ sudo chage -l romeo
Last password change : Feb 03, 2014
Password expires      : May 04, 2014
Password inactive     : never
Account expires        : Aug 02, 2014
Minimum number of days between password change : 0
Maximum number of days between password change : 90
Number of days of warning before password expires : 7
```

Ejercicio de laboratorio: Administración de usuarios y grupos locales de Linux

En este ejercicio de laboratorio, definirá una política de contraseña predeterminada, creará un grupo adicional de tres usuarios nuevos y modificará la política de contraseña de un usuario.

Resultados

- Un nuevo grupo en serverX denominado **consultants**, que incluye tres cuentas de usuario nuevas para Sam Spade, Betty Boop y Dick Tracy.
- Todas las cuentas nuevas deben solicitar que se cambien las contraseñas al iniciar sesión por primera vez y, luego, cada 30 días.
- Las cuentas nuevas de estos consultores deben tener vencimiento al final del contrato por 90 días y Betty Boop debe cambiar su contraseña cada 15 días.

Andes de comenzar

Restablezca su sistema serverX.

1. Asegúrese de que los usuarios creados recientemente tengan contraseñas que se deben cambiar cada 30 días.
2. Cree un grupo nuevo llamado **consultants** con GID de 40000.
3. Cree tres usuarios nuevos: **ssspade**, **bboop** y **dtracy**, con una contraseña **predeterminada** y agréguelos al grupo adicional **consultants**. El grupo principal debería permanecer como el grupo privado del usuario.
4. Determine la fecha en 90 días en el futuro y establezca esa fecha como fecha de vencimiento de cada una de las tres cuentas de usuario nuevas.
5. Cambie la política de contraseña para la cuenta **bboop**, para que se le solicite una contraseña nueva cada 15 días.
6. Además, exija a los usuarios que cambien la contraseña al iniciar sesión por primera vez.
7. Cuando termine, ejecute el script de evaluación **lab localusers grade** para confirmar que se hayan realizado todos los pasos de forma correcta.

Solución

En este ejercicio de laboratorio, definirá una política de contraseña predeterminada, creará un grupo adicional de tres usuarios nuevos y modificará la política de contraseña de un usuario.

Resultados

- Un nuevo grupo en serverX denominado **consultants**, que incluye tres cuentas de usuario nuevas para Sam Spade, Betty Boop y Dick Tracy.
- Todas las cuentas nuevas deben solicitar que se cambien las contraseñas al iniciar sesión por primera vez y, luego, cada 30 días.
- Las cuentas nuevas de estos consultores deben tener vencimiento al final del contrato por 90 días y Betty Boop debe cambiar su contraseña cada 15 días.

Andes de comenzar

Restablezca su sistema serverX.

1. Asegúrese de que los usuarios creados recientemente tengan contraseñas que se deben cambiar cada 30 días.

```
[student@serverX ~]$ sudo vim /etc/login.defs
[student@serverX ~]$ cat /etc/login.defs
...Output omitted...
PASS_MAX_DAYS 30
PASS_MIN_DAYS 0
PASS_MIN_LEN 5
PASS_WARN_AGE 7
...Output omitted...
```

2. Cree un grupo nuevo llamado **consultants** con GID de 40000.

```
[student@serverX ~]$ sudo groupadd -g 40000 consultants
[student@serverX ~]$ tail -5 /etc/group
stapdev:x:158:
pesign:x:989:
tcpdump:x:72:
slocate:x:21:
consultants:x:40000:
```

3. Cree tres usuarios nuevos: **sspad**, **bboop** y **dtracy**, con una contraseña **predeterminada** y agréguelos al grupo adicional **consultants**. El grupo principal debería permanecer como el grupo privado del usuario.

```
[student@serverX ~]$ sudo useradd -G consultants spade
[student@serverX ~]$ sudo useradd -G consultants bboop
[student@serverX ~]$ sudo useradd -G consultants dtracy
[student@serverX ~]$ tail -5 /etc/group
slocate:x:21:
consultants:x:40000:sspad,bboop,dtracy
sspad:x:1001:
bboop:x:1002:
dtracy:x:1003:
[student@serverX ~]$ sudo passwd spade
```

```
Changing password for user sspade.
New password: default
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: default
passwd: all authentication tokens updated successfully.
[student@serverX ~]$ sudo passwd bboop
[student@serverX ~]$ sudo passwd dtracy
```

4. Determine la fecha en 90 días en el futuro y establezca esa fecha como fecha de vencimiento de cada una de las tres cuentas de usuario nuevas.

```
[student@serverX ~]$ date -d "+90 days"
Mon May  5 11:49:24 EDT 2014
[student@serverX ~]$ sudo chage -E 2014-05-05 sspade
[student@serverX ~]$ sudo chage -E 2014-05-05 bboop
[student@serverX ~]$ sudo chage -E 2014-05-05 dtracy
```

5. Cambie la política de contraseña para la cuenta **bboop**, para que se le solicite una contraseña nueva cada 15 días.

```
[student@serverX ~]$ sudo chage -M 15 bboop
[student@serverX ~]$ sudo chage -l bboop
Last password change : Feb 04, 2014
Password expires       : Feb 19, 2014
Password inactive     : never
Account expires        : May 05, 2014
Minimum number of days between password change : 0
Maximum number of days between password change : 15
Number of days of warning before password expires : 7
```

6. Además, exija a los usuarios que cambien la contraseña al iniciar sesión por primera vez.

```
[student@serverX ~]$ sudo chage -d 0 sspade
[student@serverX ~]$ sudo chage -d 0 bboop
[student@serverX ~]$ sudo chage -d 0 dtracy
```

7. Cuando termine, ejecute el script de evaluación **lab localusers grade** para confirmar que se hayan realizado todos los pasos de forma correcta.

```
[student@serverX ~]$ lab localusers grade
```

Resumen

Usuarios y Grupos

Enumere las funciones de los usuarios y grupos en un sistema Linux y visualice los archivos de configuración locales.

Obtención de acceso de superusuario

Escale los privilegios para ejecutar comandos como superusuario.

Administración de cuentas de usuarios locales

Añadir, quitar y modificar usuarios locales con herramientas de la línea de comandos.

Administración de cuentas de grupos locales

Administre grupos locales con herramientas de la línea de comandos.

Administración de contraseñas de usuarios

Administrar políticas de vigencia de contraseñas de usuarios y bloquear, desbloquear y determinar la caducidad de cuentas de manera manual.



CAPÍTULO 6

CONTROL DE ACCESO A ARCHIVOS CON PERMISOS DEL SISTEMA DE ARCHIVOS LINUX

Descripción general	
Meta	Configurar los permisos del sistema de archivos Linux en los archivos e interpretar los efectos de seguridad de los distintos parámetros de configuración de permisos.
Objetivos	<ul style="list-style-type: none">• Explicar cómo funciona el modelo de permisos de archivo Linux.• Cambiar los permisos y la propiedad de los archivos con las herramientas de línea de comando.• Configurar un directorio en el que los archivos creados recientemente puedan ser escritos en forma automática por los miembros del grupo propietario del directorio, usando permisos especiales y configuración de default umask.
Secciones	<ul style="list-style-type: none">• Permisos del sistema de archivos Linux (y práctica)• Administración de los permisos del sistema de archivos desde la línea de comando (y práctica)• Administración de permisos predeterminados y acceso a archivos (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">• Control de acceso a archivos con permisos del sistema de archivos Linux

Permisos del sistema de archivos Linux

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder explicar cómo funciona el modelo de permisos de archivo de Linux.

Permisos del sistema de archivos Linux

El acceso a los archivos por parte de los usuarios es controlado por *permisos de archivos*. El sistema de permisos de archivos de Linux es simple pero flexible, lo que hace que sea fácil de comprender y de aplicar, y aún así poder manejar fácilmente los casos más normales de permisos.

Los archivos tienen solo tres categorías de usuario a las que se le aplican permisos. El archivo pertenece a un *usuario*, que generalmente es quien creó el archivo. El archivo también pertenece a un solo *grupo*, generalmente el grupo primario del usuario que creó el archivo, pero esto se puede cambiar. Se pueden establecer diferentes permisos para el usuario propietario y el grupo propietario, así como para todos los *otros* usuarios en el sistema que no sean el usuario o un miembro del grupo propietario.

Se aplicarán los permisos más específicos. Por lo tanto, los permisos de *usuario* anulan los permisos de *grupo*, que anulan *otros* permisos.

En el siguiente gráfico, joshua es un integrante de los grupos joshua y web, mientras que allison integra los grupos allison, wheel y web. Cuando joshua y allison necesitan colaborar, los archivos deben asociarse con el grupo web y los permisos del grupo deben permitir el acceso deseado.

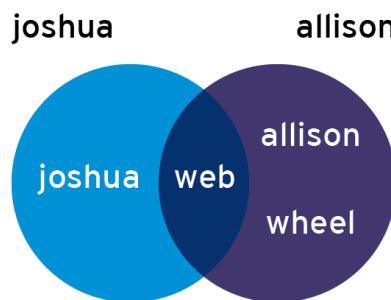


Figura 6.1: Ilustración de la membresía de grupo

También existen tres categorías de permisos que se aplican: *leer, escribir y ejecutar*. Estos permisos afectan el acceso a archivos y directorios de la siguiente forma:

Efectos de los permisos en archivos y directorios

Permiso	Efecto en los archivos	Efecto en los directorios
r (read)	Pueden leerse los contenidos del archivo.	Los contenidos del directorio (nombres de archivos) pueden detallarse.
w (write)	Los contenidos del archivo pueden cambiarse.	Cualquier archivo en el directorio puede crearse o eliminarse.

Permiso	Efecto en los archivos	Efecto en los directorios
x (exec)	Los archivos pueden ejecutarse como comandos.	Es posible acceder al contenido del directorio (según los permisos de los archivos en el directorio).

Tenga en cuenta que los usuarios normalmente poseen privilegios tanto de **read** como de **exec** en los directorios de solo lectura, por lo que pueden listar el directorio y acceder a su contenido. Si un usuario solo posee acceso de **read** en un directorio, los nombres de los archivos dentro de este pueden detallarse, pero no estará disponible otra información, incluidos permisos o marcas de tiempo, y tampoco se podrá acceder a ellos. Si un usuario solo posee acceso **exec** en un directorio, no podrá enumerar los nombres de los archivos en este, pero sí podrá acceder a su contenido en caso de que ya conozca el nombre de un archivo del que posee permiso para leer. Así, podrá acceder al contenido del archivo especificando su nombre.

Todo usuario que cuente con permisos de escritura para el directorio donde se encuentra el archivo puede quitar un archivo, sin importar la propiedad ni los permisos del archivo en sí. (Esto se puede anular con un permiso especial, el *sticky bit*, el cual abordaremos al finalizar la unidad).

Visualizar permisos y propiedades de archivos o directorios

La opción **-l** del comando **ls** expandirá los detalles de los archivos para incluir tanto los permisos de un archivo como su propiedad:

```
[student@desktopX ~]$ ls -l test
-rw-rw-r--. 1 student student 0 Feb  8 17:36 test
```

El comando **ls -l directoryname** mostrará el listado ampliado de todos los archivos que están dentro del directorio. Si desea evitar el descenso al directorio y ver los detalles expandidos de dicho directorio, agregue la opción **-d** a ls:

```
[student@desktopX ~]$ ls -ld /home
drwxr-xr-x. 5 root root 4096 Jan 31 22:00 /home
```



nota

A diferencia de los permisos NTFS, los permisos de Linux solo se aplican al directorio o archivo en el que están establecidos. Los permisos en un directorio no se heredan de forma automática por los subdirectorios o los archivos que se encuentran en él. (No obstante, los permisos en un directorio *pueden* efectivamente bloquear el acceso a su contenido). Todos los permisos en Linux se establecen directamente en cada archivo o directorio.

El permiso para **leer** en un directorio de Linux es casi equivalente a **List folder contents** en Windows.

El permiso para **escribir** en un directorio de Linux es equivalente a **Modify** en Windows. Esto implica la posibilidad de eliminar archivos y subdirectorios. En Linux, si **write** y el **sticky bit** están establecidos en un directorio, solo el usuario que sea propietario de un archivo o de un subdirectorio del directorio puede eliminarlo, lo que se asemeja al comportamiento del permiso **Write** de Windows.

El usuario root posee los permisos equivalentes a **Full Control** de Windows en todos los archivos de Linux. Sin embargo, el usuario root aún puede tener acceso restringido por la política de SELinux del sistema y el contexto de seguridad del proceso y de los archivos en cuestión. SELinux se analizará en un curso posterior.

Ejemplos: usuario, grupo y otros conceptos de Linux

Users and their groups:

```
lucy      lucy,ricardo
ricky    ricky,ricardo
ethel    ethel,mertz
fred     fred,mertz
```

File attributes (permissions, user & group ownership, name):

```
drwxrwxr-x  ricky  ricardo  dir (which contains the following files)
 -rw-rw-r--  lucy   lucy     lfile1
 -rw-r--rw-  lucy   ricardo  lfile2
 -rw-rw-r--  ricky  ricardo  rfile1
 -rw-r----- ricky  ricardo  rfile2
```

Comportamiento permitido o denegado	Control de permisos
lucy es la única persona que puede cambiar el contenido de lfile1 .	lucy tiene permisos de escritura en el archivo lfile1 como propietaria. No hay personas registradas como miembros del grupo de lucy . Los permisos para <i>otros</i> no incluyen permisos de escritura.
ricky puede ver el contenido de lfile2 , pero no puede modificar el contenido de lfile2 .	ricky es miembro del grupo ricardo y ese grupo posee permisos de solo lectura para lfile2 . Si bien <i>otro</i> tiene permisos de escritura, los permisos del grupo tienen prioridad.

Comportamiento permitido o denegado	Control de permisos
ricky puede eliminar lfile1 y lfile2 .	ricky tiene permisos de escritura en el directorio que contiene ambos archivos y, como tal, puede eliminar cualquier archivo de ese directorio.
ethel puede cambiar el contenido de lfile2 .	Dado que ethel no es lucy y no es miembro del grupo ricardo , los permisos relacionados con otros la rigen, y estos incluyen permiso de escritura.
lucy puede cambiar el contenido de rfile1 .	lucy es miembro del grupo ricardo y ese grupo tiene permisos de lectura y escritura respecto de rfile1 .
ricky puede ver y modificar el contenido de rfile2 . lucy puede ver, pero no modificar el contenido de rfile2 . ethel y fred no tienen ningún acceso al contenido de rfile2 .	ricky es propietario del archivo y tiene acceso de lectura y de escritura a rfile2 . lucy es miembro del grupo ricardo y ese grupo tiene acceso de solo lectura a rfile2 . Rigen otros permisos para ethel y fred , y dichos permisos no incluyen permiso de lectura ni escritura.



Referencias

Página del manual (1)**ls**

info coreutils (GNU Coreutils)

- Sección 13: Cambiar atributos de archivos

Práctica: Interpretación de permisos de archivos y directorios

Usando el listado de directorios presentado, relacione los elementos que se muestran a continuación con el elemento correspondiente en la tabla.

Users and their groups:

```
wilma  wilma, flintstone
fred   fred, flintstone
betty  betty, rubble
barney barney, rubble
```

File attributes (permissions, user & group ownership, name):

```
drwxrwxr-x  fred   flintstone  dir (which contains the following files)
-rw-rw-r--  wilma wilma      lfile1
-rw-r--rw-  wilma flintstone lfile2
-rw-rw-r--  fred   flintstone rfile1
-rw-r----- fred   flintstone rfile2
```

all

lfile1

lfile2

none (ninguno)

rfile1

rfile2

Descripción	Nombre del archivo
Es propiedad de fred y lo pueden leer todos los usuarios.	
El usuario betty puede modificar el contenido.	
El usuario fred puede eliminarlo.	
El usuario barney no puede leerlo.	
Tiene la propiedad de un grupo de wilma .	
El usuario barney puede eliminarlo.	

Solución

Usando el listado de directorios presentado, relacione los elementos que se muestran a continuación con el elemento correspondiente en la tabla.

Users and their groups:
wilma wilma,flintstone
fred fred,flintstone
betty betty,rubble
barney barney,rubble
File attributes (permissions, user & group ownership, name):
drwxrwxr-x fred flintstone dir (which contains the following files)
-rw-rw-r-- wilma wilma lfile1
-rw-rw-rw- wilma flintstone lfile2
-rw-rw-r-- fred flintstone rfile1
-rw-r----- fred flintstone rfile2

Descripción	Nombre del archivo
Es propiedad de fred y lo pueden leer todos los usuarios.	rfile1
El usuario betty puede modificar el contenido.	lfile2
El usuario fred puede eliminarlo.	all
El usuario barney no puede leerlo.	rfile2
Tiene la propiedad de un grupo de wilma .	lfile1
El usuario barney puede eliminarlo.	none (ninguno)

Administración de permisos del sistema de archivos desde la línea de comandos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder cambiar los permisos y la propiedad de los archivos usando herramientas de la línea de comandos.

Cambio de permisos de archivo o directorio

El comando usado para cambiar los permisos desde la línea de comandos es **chmod**, que significa "change mode" (cambiar modo) (los permisos también se conocen como el *mode* de un archivo). El comando **chmod** tiene una instrucción de permiso seguida de una lista de archivos o directorios para cambio. La instrucción de permiso puede ser emitida simbólicamente (el método simbólico) o numéricamente (el método numérico).

Palabras clave de métodos simbólicos:

```
chmod WhoWhatWhich file|directory
```

- *Who* es u, g, o, a (*para usuario, grupo, otros, todos*)
- *What* es +, -, = (*para agregar, eliminar, establecer exactamente*)
- *Which* es br, w, x (*para leer, escribir, ejecutar*)

El método *simbólico* de cambiar los permisos del archivo usa letras para representar los distintos grupos de permisos: **u** para usuario, **g** para grupo, **o** para otros y **a** para todos.

Con el método simbólico, no es necesario establecer un grupo completamente nuevo de permisos. En su lugar, se puede cambiar uno o más permisos existentes. Para lograrlo, puede usar tres símbolos: **+** para agregar permisos a un conjunto, **-** para eliminar permisos de un conjunto e **=** para reemplazar el conjunto completo por un grupo de permisos.

Los permisos en sí están representados por una única letra: **r** para leer, **w** para escribir y **x** para ejecutar. Cuando utilice **chmod** para cambiar los permisos con el método simbólico, el uso de una **X** mayúscula como indicador de permiso agregará permiso de ejecución únicamente si el archivo es un directorio o si ya tiene el permiso de ejecución establecido para usuario, grupo u otros.

Método numérico:

```
chmod ### file|directory
```

- Cada dígito representa un nivel de acceso: usuario, grupo, otros.
- # es la suma de r = 4, w = 2 y x = 1.

Al utilizar el método *numérico*, los permisos son representados por un número *octal* de tres dígitos (o cuatro, al establecer permisos avanzados). Un único dígito **octal** puede

representar los números 0-7, exactamente la cantidad de posibilidades para un número de tres bits.

Para realizar conversiones entre una representación simbólica y numérica de permisos, debemos saber cómo se realiza la asignación. En la representación octal (numérica) de tres dígitos, cada dígito representa un grupo de permisos, de izquierda a derecha: usuario, grupo y otros. En cada uno de estos grupos, se comienza con **0**. Si se encuentra el permiso de lectura, agregue **4**. Agregue **2** si se encuentra el permiso de escritura y **1** para ejecutar.

Los permisos numéricos a menudo son usados por administradores avanzados, ya que son más breves para escribir y pronunciar, y al mismo tiempo, le proporcionan el control total de todos los permisos.

Examinar los permisos **-rwxr-x---**. Para usuario, **rwx** se calcula como **4+2+1=7**. Para grupo, **r-x** se calcula como **4+0+1=5**, y para otros usuarios, **---** se representa con **0**. Con estos tres en conjunto, la representación numérica de dichos permisos es **750**.

Este cálculo también se puede realizar en dirección opuesta. Veamos los permisos **640**. Para los permisos de usuario, **6** representa leer (4) y escribir (2), que se ve como **rw-**. Para la parte de grupo, **4** solo incluye leer (4) y se ve como **r--**. El **0** para otros no nos proporciona permisos (**---**), por lo que el conjunto final de permisos simbólicos para este archivo es **-rw-r----**.

Ejemplos

- Elimine el permiso de lectura y escritura para el grupo y otros respecto de **file1**:

```
[student@desktopX ~]$ chmod go-rw file1
```

- Agregue un permiso de ejecución para todos respecto de **file2**:

```
[student@desktopX ~]$ chmod a+x file2
```

- Establezca un permiso de lectura, escritura y ejecución para usuario, lectura y escritura para grupo y ningún permiso para otros respecto de **sampledir**:

```
[student@desktopX ~]$ chmod 750 sampledir
```



nota

El comando **chmod** admite la opción **-R** para establecer permisos de manera recursiva en los archivos, en todo el árbol de directorios. Cuando utiliza la opción **-R**, puede ser útil establecer permisos de manera simbólica mediante el uso del indicador **X**. Esto permitirá ejecutar (buscar) permisos para establecer en los directorios de modo que se pueda acceder a su contenido, sin cambiar los permisos en la mayoría de los archivos. Pero tenga cuidado. Si un archivo tiene un permiso de ejecución establecido, **X** establecerá el permiso de ejecución especificado en ese archivo también. Por ejemplo, el siguiente comando establecerá de manera recursiva el acceso de lectura y de escritura en **demodir** y todos sus procesos secundarios para el propietario del grupo, pero solo aplicará permisos de ejecución de grupo a directorios y archivos que ya tienen permisos de ejecución establecidos para usuario, grupo u otros.

```
[student@desktopX ~]# chmod -R g+rwx demodir
```

Cambio de la propiedad de grupo o de usuario de un archivo o directorio

Un archivo creado recientemente es propiedad del usuario que lo crea. De manera predeterminada, el archivo nuevo es propiedad del grupo, que es el grupo principal del usuario que crea el archivo. Dado que Red Hat Enterprise Linux utiliza grupos privados de usuarios, este grupo a menudo es un grupo con ese único usuario como miembro. Para garantizar el acceso basado en membresía de grupo, es posible que se deban cambiar el propietario o el grupo de un archivo.

La propiedad del archivo se puede cambiar con el comando **chown** (change owner). Por ejemplo, para otorgarle propiedad del archivo **foofile** a **student**, se podría usar el siguiente comando:

```
[root@desktopX ~]# chown student foofile
```

Se puede utilizar **chown** con la opción **-R** para cambiar recursivamente la propiedad de un árbol de directorios completo. El siguiente comando otorgaría propiedad de **foodir** y de todos los archivos y subdirectorios incluidos dentro a **student**:

```
[root@desktopX ~]# chown -R student foodir
```

El comando **chown** también se puede utilizar para cambiar el propietario del grupo de un archivo, anteponiendo el nombre del grupo con dos puntos (:). Por ejemplo, el siguiente comando cambiará el grupo de **foodir** a **admins**:

```
[root@desktopX ~]# chown :admins foodir
```

El comando **chown** también se puede usar para cambiar el propietario y el grupo al mismo tiempo. Para ello, puede usar la sintaxis **owner:group**. Por ejemplo, para cambiar la propiedad de **foodir** a **visitor** y el grupo a **guests**, puede usar:

```
[root@desktopX ~]# chown visitor:guests foodir
```

Solo el usuario **root** puede cambiar la propiedad de un archivo. No obstante, la propiedad del grupo puede establecerla el usuario **root** o el propietario del archivo. **root** puede otorgar propiedad a cualquier grupo, mientras que los usuarios que no son **root** pueden otorgar propiedad solo a los grupos a los que pertenecen.



nota

En lugar de usar **chown**, algunos usuarios cambian el propietario del grupo con el comando **chgrp**; este comando realiza exactamente lo mismo que cambiar la propiedad con **chown**, e incluye el uso de **-R** para que afecte la totalidad de árboles de directorio.



Referencias

Páginas del manual: **ls(1)**, **chmod(1)**, **chown(1)** y **chgrp(1)**

Práctica: Administrar la seguridad de los archivos desde la línea de comandos

En este ejercicio de laboratorio, creará un directorio de colaboración para los usuarios preexistentes.

Resultados

Un directorio al que pueden acceder todos los miembros del grupo **ateam** y un archivo creado por Andy que puede ser modificado por Alice.

Antes de comenzar

Restablezca su sistema serverX.

1. Inicie sesión en el escritorio GNOME en serverX como **student** con la contraseña **student**.
2. Abra una ventana con una señal BASH.
Seleccione Applications > Utilities > Terminal.
3. Conviértase en el usuario **root** en el aviso de shell.

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

4. Ejecute **lab permissions setup**, que creará un grupo compartido, **ateam**, con dos usuarios nuevos, **andy** y **alice**. La contraseña para estas cuentas es **password**.

```
[root@serverX ~]# lab permissions setup
```

5. Cree un directorio en **/home** con el nombre **ateam-text**.

```
[root@serverX ~]# mkdir /home/ateam-text
```

6. Cambie la propiedad de grupo del directorio **ateam-text** a **ateam**.

```
[root@serverX ~]# chown :ateam /home/ateam-text
```

7. Asegúrese de que los permisos de **ateam-text** permitan que los miembros del grupo creen y eliminen archivos.

```
[root@serverX ~]# chmod g+w /home/ateam-text
```

8. Asegúrese de que los permisos de **ateam-text** impidan que otros accedan a sus archivos.

```
[root@serverX ~]# chmod 770 /home/ateam-text
```

```
[root@serverX ~]$ ls -ld /home/ateam-text  
drwxrwx---. 2 root ateam 6 Jan 23 12:50 /home/ateam-text
```

9. Salga de la shell de root y cambie al usuario **andy** con la contraseña **password**.

```
[root@serverX ~]# exit  
[student@serverX ~]$ su - andy  
Password: password
```

10. Navegue hacia la carpeta **/home/ateam-text** (recuerde abrir una ventana de terminal primero).

```
[andy@serverX ~]$ cd /home/ateam-text
```

11. Cree un archivo vacío con el nombre **andyfile3**.

```
[andy@serverX ateam-text]$ touch andyfile3
```

12. Registre las propiedades de grupo y de usuario predeterminadas del nuevo archivo y sus permisos.

```
[andy@serverX ateam-text]$ ls -l andyfile3  
-rw-rw-r--. 1 andy andy 0 Jan 23 12:59 andyfile3
```

13. Cambie la propiedad del grupo del archivo nuevo por **ateam** y registre la nueva propiedad y los permisos.

```
[andy@serverX ateam-text]$ chown :ateam andyfile3  
[andy@serverX ateam-text]$ ls -l andyfile3  
-rw-rw-r--. 1 andy ateam 0 Jan 23 12:59 andyfile3
```

14. Salga de la shell y cambie al usuario **alice** con la contraseña **password**.

```
[andy@serverX ateam-text]$ exit  
[student@serverX ~]$ su - alice  
Password: password
```

15. Navegue hasta la carpeta **/home/ateam-text**.

```
[alice@serverX ~]$ cd /home/ateam-text
```

16. Determine los privilegios de **alice** para acceder o modificar **andyfile3**.

```
[alice@serverX ateam-text]$ echo "text" >> andyfile3  
[alice@serverX ateam-text]$ cat andyfile3  
text
```

Administración de permisos predeterminados y acceso a archivos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder configurar un directorio en el que los miembros del grupo que posee el directorio puedan escribir automáticamente los archivos creados recientemente, mediante el uso de permisos especiales y configuraciones de umask predeterminadas.

Permisos especiales

El permiso **setuid** (o **setgid**) en un archivo ejecutable significa que el comando se ejecutará como **usuario** (o **grupo**) del archivo, no como el usuario que ejecutó el comando. Un ejemplo de este caso es el comando **passwd**:

```
[student@desktopX ~]$ ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 35504 Jul 16 2010 /usr/bin/passwd
```

En una larga lista, puede detectar los permisos **setuid** con una **s** minúscula, donde normalmente esperaría ver la **x** (permisos de ejecución del propietario). Si el propietario no posee permisos de ejecución, será reemplazada por una **S** mayúscula.

El **sticky bit** para un directorio establece una restricción especial sobre la eliminación de archivos: solo el propietario del archivo (y **root**) puede eliminar archivos del directorio. Un ejemplo es **/tmp**:

```
[student@desktopX ~]$ ls -ld /tmp
drwxrwxrwt. 39 root root 4096 Feb 8 20:52 /tmp
```

En una lista larga, puede detectar los permisos **sticky** con una **t** minúscula, donde normalmente esperaría ver la **x** (otros permisos de ejecución). Si el otro no posee permisos de ejecución, será reemplazada por una **T** mayúscula.

Por último, **setgid** en un directorio significa que los archivos creados en el directorio heredarán la afiliación de grupos del directorio, en lugar de heredarla del usuario que la creó. Esto generalmente se usa en directorios colaborativos grupales para poder cambiar automáticamente un archivo del grupo privado predeterminado al grupo compartido.

En una larga lista, puede detectar los permisos **setgid** con una **s** minúscula, donde normalmente esperaría ver la **x** (permisos de ejecución del grupo). Si el grupo no posee permisos de ejecución, será reemplazada por una **S** mayúscula.

Efectos de los permisos especiales en archivos y directorios

Permiso especial	Efecto en los archivos	Efecto en los directorios
u+s (suid)	El archivo se ejecuta como el usuario propietario, no como el usuario que lo ejecutó.	No hay efectos.

Permiso especial	Efecto en los archivos	Efecto en los directorios
g+s (sgid)	El archivo se ejecuta como el grupo propietario.	Los archivos creados recientemente en el directorio han establecido al propietario del grupo para que coincida con el propietario del grupo del directorio.
o+t (sticky)	No hay efectos.	Los usuarios con escribir en el directorio solo pueden eliminar los archivos de los que son propietarios, pero no pueden eliminar ni forzar el guardado de archivos cuyos propietarios sean otros usuarios.

Establecer permisos especiales

- Simbólicamente: setuid = **u+s**; setgid = **g+s**; sticky = **o+t**
- Numéricamente (cuarto dígito precedente): setuid = 4 ; setgid = 2 ; sticky = 1

Ejemplos

- Agregue el setgid bit en **directory**:

```
[root@desktopX ~]# chmod g+s directory
```

- Establezca el setgid bit y los permisos de lectura/escritura/ejecución para el usuario y el grupo en **directory**:

```
[root@desktopX ~]# chmod 2770 directory
```

Permisos de archivos predeterminados

Los permisos predeterminados para archivos se establecen mediante el proceso que los crea. Por ejemplo, los editores de texto crean archivos para que sean de lectura y escritura, pero no ejecutables para cualquiera. Lo mismo ocurre con el redireccionamiento de shell. Además, son los compiladores quienes crean los ejecutables binarios como ejecutables. El comando **mkdir** crea directorios nuevos con todos los permisos establecidos: de lectura, escritura y ejecución.

La experiencia indica que estos permisos por lo general no se establecen cuando se crean los directorios y archivos nuevos. Esto ocurre porque algunos permisos son borrados por el umask del proceso de shell. El comando **umask** sin argumentos mostrará el valor actual del umask de shell:

```
[student@desktopX ~]$ umask  
0002
```

Capítulo 6. Control de acceso a archivos con permisos del sistema de archivos Linux

Cada proceso en el sistema tiene un umask, que es una máscara de bits octal utilizada para borrar los permisos de archivos y directorios nuevos creados por el proceso. Si se establece un bit en el umask, el permiso correspondiente se elimina en los archivos nuevos. Por ejemplo, el umask anterior, 0002, borra el bit de escritura para otros usuarios. Los ceros iniciales indican que los permisos especiales, de usuario y de grupo no están borrados. Un umask de 077 borra los permisos de todo el grupo y de otros de los archivos creados recientemente.

Utilice el comando **umask** con un argumento numérico único para cambiar el umask de la shell actual. El argumento numérico debe ser un valor octal que se corresponda con el valor del umask nuevo. Si tiene menos de 3 dígitos, se suponen ceros iniciales.

Los valores de umask predeterminados del sistema para usuarios de shell Bash se definen en los archivos **/etc/profile** y **/etc/bashrc**. Los usuarios pueden omitir los valores predeterminados del sistema en sus archivos **.bash_profile** y **.bashrc**.

En este ejemplo, siga los pasos a continuación mientras el instructor demuestra los efectos de **umask** en directorios y archivos nuevos.

1. Cree un archivo y un directorio nuevos para ver cómo el umask predeterminado afecta los permisos.

```
[student@desktopX ~]$ touch newfile1
[student@desktopX ~]$ ls -l newfile1
-rw-rw-r--. 1 student student 0 May  9 01:54 newfile1
[student@desktopX ~]$ mkdir newdir1
[student@desktopX ~]$ ls -ld newdir1
drwxrwxr-x. 2 student student 0 May  9 01:54 newdir1
```

2. Establezca el valor de umask en 0. Esta configuración no enmascarará ninguno de los permisos de los archivos nuevos. Cree un archivo y un directorio nuevos para ver cómo este umask nuevo afecta los permisos.

```
[student@desktopX ~]$ umask 0
[student@desktopX ~]$ touch newfile2
[student@desktopX ~]$ ls -l newfile2
-rw-rw-rw-. 1 student student 0 May  9 01:54 newfile2
[student@desktopX ~]$ mkdir newdir2
[student@desktopX ~]$ ls -ld newdir2
drwxrwxrwx. 2 student student 0 May  9 01:54 newdir2
```

3. Establezca el valor del umask en 007. Esta configuración enmascarará todos los "otros" permisos de los archivos nuevos.

```
[student@desktopX ~]$ umask 007
[student@desktopX ~]$ touch newfile3
[student@desktopX ~]$ ls -l newfile3
-rw-rw----. 1 student student 0 May  9 01:55 newfile3
[student@desktopX ~]$ mkdir newdir3
[student@desktopX ~]$ ls -ld newdir3
drwxrwx---. 2 student student 0 May  9 01:54 newdir3
```

4. Establezca el valor del umask en 027. Esta configuración enmascarará el acceso de escritura para miembros del grupo y todos los "otros" permisos de los archivos nuevos.

```
[student@desktopX ~]$ umask 027
[student@desktopX ~]$ touch newfile4
[student@desktopX ~]$ ls -l newfile4
-rw-r----- 1 student student 0 May  9 01:55 newfile4
[student@desktopX ~]$ mkdir newdir4
[student@desktopX ~]$ ls -ld newdir4
drwxr-x--- 2 student student 0 May  9 01:54 newdir4
```

5. Inicie sesión como **root** para cambiar el umask predeterminado para usuarios sin privilegios a fin de evitar todo acceso de usuarios que no estén en su grupo.

Modifique **/etc/bashrc** y **/etc/profile** para cambiar el umask predeterminado para los usuarios de shell Bash. Dado que el umask predeterminado para usuarios sin privilegios es 0002, busque el comando **umask** en estos archivos que establezca el umask en ese valor. Cámbielos para establecer el umask en 007.

```
[root@desktopX ~]# less /etc/bashrc
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 002
else
    umask 022
fi

# Only display echos from profile.d scripts if we are no login shell
[root@desktopX ~]# vim /etc/bashrc
[root@desktopX ~]# less /etc/bashrc
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 007
else
    umask 022
fi

# Only display echos from profile.d scripts if we are no login shell
[root@desktopX ~]# less /etc/profile
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 002
else
    umask 022
fi

for i in /etc/profile.d/*.sh ; do
[root@desktopX ~]# vim /etc/profile
[root@desktopX ~]# less /etc/profile
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 007
else
    umask 022
fi

for i in /etc/profile.d/*.sh ; do
```

6. Vuelva a iniciar sesión como **student** y confirme que los cambios de umask que realizó sean persistentes.

```
[student@desktopX ~]$ umask  
0007
```



nota

Es posible que otros shells, como **tcs**, tengan distintos archivos de inicialización predeterminados del sistema en **/etc** y directorios principales de los usuarios.



Referencias

Páginas del manual: **bash(1)**, **ls(1)**, **chmod(1)** y **umask(1)**

Práctica: Control de permisos y propiedad de archivos nuevos

En este ejercicio de laboratorio, controlará los permisos predeterminados de archivos nuevos usando el comando **umask** y el permiso **setgid**.

Resultados

- Creación de un directorio compartido en el que los archivos nuevos pasan automáticamente a ser propiedad del grupo **ateam**.
- Prueba de diversos valores de configuración de umask.
- Ajuste de los permisos predeterminados para usuarios específicos.
- Confirmación de que el ajuste sea correcto.

Andes de comenzar

Restablezca su sistema serverX. Ejecute **lab permissions setup** para crear la cuenta **alice**. La contraseña de **alice** es **password**.

1. Inicie sesión con la cuenta **alice** en la máquina virtual **serverX** y abra una ventana con un aviso de Bash. Utilice el comando **umask** sin argumentos para ver el valor de umask predeterminado de Alice.

```
[alice@serverX ~]$ umask  
0002
```

2. Cree un directorio nuevo **/tmp/shared** y un archivo nuevo **/tmp/shared/defaults** para ver el modo en que el valor de umask predeterminado afecta los permisos.

```
[alice@serverX ~]$ mkdir /tmp/shared  
[alice@serverX ~]$ ls -ld /tmp/shared  
drwxrwxr-x. 2 alice alice 6 Jan 26 18:43 /tmp/shared  
[alice@serverX ~]$ touch /tmp/shared/defaults  
[alice@serverX ~]$ ls -l /tmp/shared/defaults  
-rw-rw-r--. 1 alice alice 0 Jan 26 18:43 /tmp/shared/defaults
```

3. Cambie la propiedad del grupo de **/tmp/shared** a **ateam** y registre la propiedad y los permisos nuevos.

```
[alice@serverX ~]$ chown :ateam /tmp/shared  
[alice@serverX ~]$ ls -ld /tmp/shared  
drwxrwxr-x. 2 alice ateam 21 Jan 26 18:43 /tmp/shared
```

4. Cree un archivo nuevo en **/tmp/shared** y registre la propiedad y los permisos.

```
[alice@serverX ~]$ touch /tmp/shared/alice3  
[alice@serverX ~]$ ls -l /tmp/shared/alice3  
-rw-rw-r--. 1 alice alice 0 Jan 26 18:46 /tmp/shared/alice3
```

Capítulo 6. Control de acceso a archivos con permisos del sistema de archivos Linux

5. Asegúrese de que los permisos de **/tmp/shared** permitan que los archivos que se creen en ese directorio hereden la propiedad de grupo de **ateam**.

```
[alice@serverX ~]$ chmod g+s /tmp/shared
[alice@serverX ~]$ ls -ld /tmp/shared
drwxrwsr-x. 2 alice ateam 34 Jan 26 18:46 /tmp/shared
[alice@serverX ~]$ touch /tmp/shared/alice4
[alice@serverX ~]$ ls -l /tmp/shared/alice4
-rw-rw-r--. 1 alice ateam 0 Jan 26 18:48 /tmp/shared/alice4
```

6. Cambie el umask de **alice** de modo que los archivos nuevos se creen con acceso de solo lectura para el grupo y sin acceso para otros usuarios. Cree un archivo nuevo y registre la propiedad y los permisos.

```
[alice@serverX ~]$ umask 027
[alice@serverX ~]$ touch /tmp/shared/alice5
[alice@serverX ~]$ ls -l /tmp/shared/alice5
-rw-r-----. 1 alice ateam 0 Jan 26 18:48 /tmp/shared/alice5
```

7. Abra una nueva shell Bash con la cuenta **alice** y vea el valor de umask.

```
[alice@serverX ~]$ umask
0002
```

8. Cambie el valor de umask predeterminado de **alice** para prohibir el acceso a los usuarios que no pertenezcan al grupo.

```
[alice@serverX ~]# echo "umask 007" >> ~/.bashrc
[alice@serverX ~]# cat ~/.bashrc
#
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
umask 007
```

9. Cierre sesión y regrese a **serverX** como **alice**, y confirme que los cambios efectuados en umask sean persistentes.

```
[alice@serverX ~]$ umask
0007
```

Ejercicio de laboratorio: Control de acceso a archivos con permisos del sistema de archivos Linux

En este ejercicio de laboratorio, configurará un sistema con directorios para la colaboración de los usuarios.

Resultados

- Un directorio en serverX llamado **/home/stooges** donde estos tres usuarios puedan trabajar en forma conjunta con los archivos.
- Solo el acceso de usuario y grupo crea y elimina archivos en **/home/stooges**. A los archivos creados en este directorio se les debe asignar automáticamente la propiedad de grupo **stooges**.
- No se podrá acceder a los archivos nuevos creados por los usuarios fuera del grupo.

Andes de comenzar

Restablezca su sistema serverX. Inicie sesión en su sistema servidor y configúrelo.

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

Su equipo serverX tiene tres cuentas: **curly**, **larry** y **moe**, cuyos usuarios son miembros de un grupo llamado **stooges**. La contraseña para cada cuenta es **password**.

1. Abra una ventana de terminal e ingrese como usuario root en serverX.
2. Cree el directorio **/home/stooges**.
3. Cambie los permisos en el directorio **/home/stooges** para que pertenezca al grupo **stooges**.
4. Establezca los permisos en el directorio **/home/stooges** para que se conviertan en un directorio GID bit (2), para que el propietario (7) y el grupo (7) tengan permisos totales para leer/escribir/ejecutar y otros usuarios no tengan permiso (0) al directorio.
5. Compruebe que los permisos hayan sido establecidos correctamente.
6. Modifique los login scripts globales para que los usuarios normales tengan una configuración de umask que evite que otros visualicen o modifiquen los archivos y directorios nuevos.
7. Cuando haya finalizado, abra una ventana de terminal en serverX y ejecute **lab permissions grade** para confirmar que haya completado todo en forma correcta.

Solución

En este ejercicio de laboratorio, configurará un sistema con directorios para la colaboración de los usuarios.

Resultados

- Un directorio en serverX llamado **/home/stooges** donde estos tres usuarios puedan trabajar en forma conjunta con los archivos.
- Solo el acceso de usuario y grupo crea y elimina archivos en **/home/stooges**. A los archivos creados en este directorio se les debe asignar automáticamente la propiedad de grupo **stooges**.
- No se podrá acceder a los archivos nuevos creados por los usuarios fuera del grupo.

Andes de comenzar

Restablezca su sistema serverX. Inicie sesión en su sistema servidor y configúrelo.

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

Su equipo serverX tiene tres cuentas: **curly**, **larry** y **moe**, cuyos usuarios son miembros de un grupo llamado **stooges**. La contraseña para cada cuenta es **password**.

1. Abra una ventana de terminal e ingrese como usuario root en serverX.

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

2. Cree el directorio **/home/stooges**.

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

3. Cambie los permisos en el directorio **/home/stooges** para que pertenezca al grupo **stooges**.

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

4. Establezca los permisos en el directorio **/home/stooges** para que se conviertan en un directorio GID bit (2), para que el propietario (7) y el grupo (7) tengan permisos totales para leer/escribir/ejecutar y otros usuarios no tengan permiso (0) al directorio.

```
[root@serverX ~]# chmod 2770 /home/stooges
```

5. Compruebe que los permisos hayan sido establecidos correctamente.

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

6. Modifique los login scripts globales para que los usuarios normales tengan una configuración de umask que evite que otros visualicen o modifiquen los archivos y directorios nuevos.

```
[root@serverX ~]# vim /etc/bashrc
[root@serverX ~]# vim /etc/profile
[root@serverX ~]# less /etc/bashrc
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 007
else
    umask 022
fi

for i in /etc/profile.d/*.sh ; do
```

7. Cuando haya finalizado, abra una ventana de terminal en serverX y ejecute **lab permissions grade** para confirmar que haya completado todo en forma correcta.

```
[student@serverX ~]$ lab permissions grade
```

Resumen

Permisos del sistema de archivos Linux

Interprete los permisos de archivos y directorio como se muestran con el comando **ls**.

Administración de permisos del sistema de archivos desde la línea de comandos

Modificar la propiedad y los permisos de archivos y directorios utilizando **chmod** y **chown**.

Administración de permisos predeterminados y acceso a archivos

Explicar cómo el sistema establece los permisos predeterminados y usar **umask** y **SGID** para controlar el acceso automático a los archivos.



CAPÍTULO 7

ADMINISTRACIÓN Y CONTROL DE PROCESOS LINUX

Descripción general	
Meta	Evaluar y controlar procesos que se ejecutan en un sistema Red Hat Enterprise Linux.
Objetivos	<ul style="list-style-type: none">• Enumerar e interpretar la información básica sobre los procesos que se ejecutan en el sistema.• Controlar procesos en la sesión de la shell utilizando el control de trabajo de Bash.• Finalizar y controlar los procesos utilizando señales.• Monitorear el uso de recursos y la carga del sistema debido a la actividad del proceso.
Secciones	<ul style="list-style-type: none">• Procesos (y práctica)• Control de trabajos (y práctica)• Finalizar procesos (y práctica)• Monitorear la actividad de procesos (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">• Administración y control de procesos Linux

Procesos

Objetivos

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

- Definir el ciclo de vida de un proceso.
- Definir los estados de un proceso.
- Ver e interpretar listas de procesos.

¿Qué es un proceso?

Un *proceso* es una instancia de un programa ejecutable que se inició y se encuentra en funcionamiento. Un proceso consta de lo siguiente:

- un espacio de direcciones que incluye la memoria asignada;
- características de seguridad, que incluyen credenciales y privilegios de propiedad;
- uno o más subprocesos de ejecución de código de programa; y
- el estado del proceso.

El *entorno* de un proceso incluye:

- variables locales y globales;
- un contexto de programación actual; y
- recursos asignados del sistema, como descriptores de archivos y puertos de red.

Un proceso (*principal*) existente duplica su espacio de dirección (**fork**) para crear una nueva estructura de proceso (*secundario*). A cada nuevo proceso se le asigna una *ID de proceso* (PID) única con fines de monitoreo y seguridad. La PID y la *ID del proceso principal* (PPID) son elementos del entorno del proceso nuevo. Cualquier proceso puede crear un proceso secundario. Todos los procesos derivan del primer proceso de sistemas, que es **systemd(1)** en un sistema Red Hat Enterprise Linux 7.

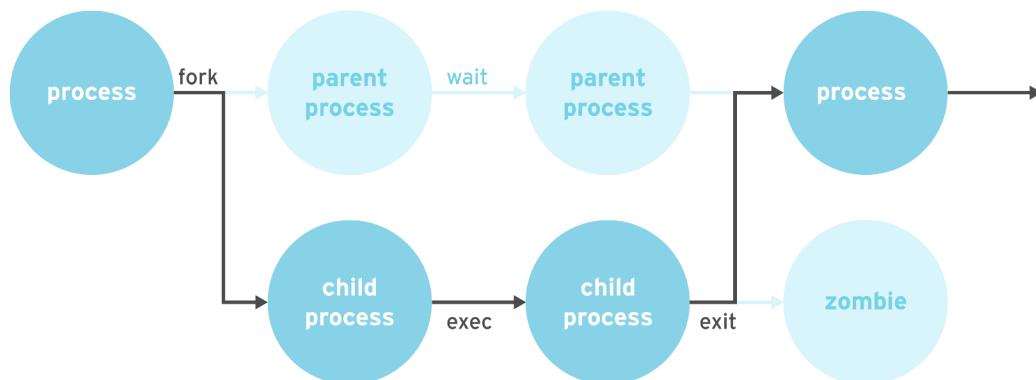


Figura 7.1: Ciclo de vida de un proceso

Mediante el procedimiento de **fork**, un proceso secundario hereda identidades de seguridad, descriptores de archivos actuales y anteriores, privilegios de recursos y puertos, variables de entorno y códigos de programa. Luego, un proceso secundario puede **exec** su propio código de programa. Normalmente, un proceso principal *duerme*, mientras se ejecuta el proceso secundario, lo que establece que una solicitud (**wait**) se señala cuando finalice el proceso secundario. Tras su finalización, el proceso secundario ya ha cerrado o descartado sus recursos y su entorno; el resto del proceso se conoce como *zombie*. El proceso principal, que se señala como activo una vez que finaliza el proceso secundario, limpia la estructura restante y continúa con la ejecución de su propio código de programa.

Estados de los procesos

En un sistema operativo de funciones múltiples, cada CPU (o núcleo de CPU) puede trabajar en un proceso en un momento dado. Mientras se ejecuta un proceso, sus requisitos inmediatos en cuanto a asignación de recursos y tiempo de la CPU cambian. A los procesos se les asigna un *estado*, el cual cambia según las circunstancias.

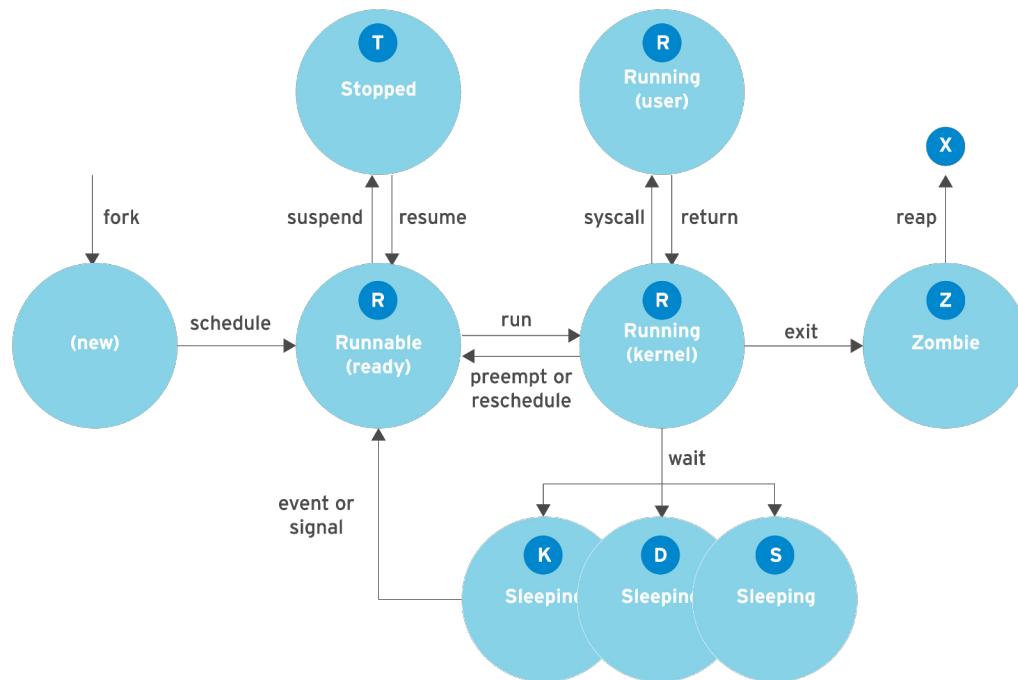


Figura 7.2: Estados de los procesos de Linux

Los estados de los procesos de Linux se ilustran en el diagrama anterior y se describen en la siguiente tabla.

Estados de los procesos de Linux

Nombre Bander	Nombre y descripción del estado definido por el kernel
En ejecución	R

TASK_RUNNING: El proceso se está ejecutando en una CPU o se encuentra en espera de su ejecución. El proceso puede estar ejecutando rutinas del usuario o rutinas del kernel (llamadas del sistema); también

Nombre Bander: Nombre y descripción del estado definido por el kernel		
		puede estar en cola y listo cuando esté en el estado <i>En ejecución</i> (o <i>Ejecutable</i>).
En espera	S	TASK_INTERRUPTIBLE: El proceso se encuentra en espera de que se dé cierta condición, como una solicitud de hardware, el acceso a un recurso del sistema o una señal. Cuando un evento o una señal cumple con la condición, el proceso regresa al estado <i>En ejecución</i> .
	D	TASK_UNINTERRUPTIBLE: Este proceso también se encuentra <i>En espera</i> , pero a diferencia del estado S , no responderá a las señales enviadas. Solo se utiliza en ciertas condiciones en las que la interrupción del proceso puede dar lugar a un estado imprevisto del dispositivo.
	K	TASK_KILLABLE: Igual al estado D ininterrumpido, solo que modificado para permitir que la tarea en espera responda a una señal de anulación (salida completa). Las utilidades con frecuencia muestran procesos <i>anulables</i> como procesos con estado D .
Detenido	T	TASK_STOPPED: El proceso se ha <i>detenido</i> (suspendido), generalmente porque otro usuario u otro proceso lo señalizó. Otra señal puede hacer que el proceso continúe (se reanude) y regrese al estado <i>En ejecución</i> .
	T	TASK_TRACED: Un proceso que se está depurando también se encuentra temporalmente <i>detenido</i> y comparte el mismo indicador de estado T .
Zombie	Z	EXIT_ZOMBIE: Un proceso secundario señala su proceso principal cuando finaliza. Se liberan todos los recursos, menos la identidad del proceso (PID).
	X	EXIT_DEAD: Cuando el proceso principal limpia (<i>obtiene</i>) la estructura del proceso secundario restante, el proceso se libera completamente. Este estado nunca se observará en utilidades de listas de procesos.

Listas de procesos

El comando **ps** se utiliza para elaborar una lista de los procesos actuales. El comando puede proporcionar información detallada de los procesos, que incluye:

- la identificación del usuario (UID) que determina los privilegios del proceso;
- la identificación del proceso (PID) única;
- la CPU y el tiempo real empleado;
- la cantidad de memoria que el proceso ha asignado en diversas ubicaciones;
- la ubicación del proceso **STDOUT**, conocido como *terminal de control*;
- el estado del proceso actual.



Importante

La versión de **ps** de Linux admite tres formatos de opciones, a saber:

- opciones UNIX (POSIX), que pueden agruparse y deben estar precedidas por un guión;
- opciones BSD, que pueden agruparse y no deben usarse con un guión; y
- opciones extensas GNU, que están precedidas por dos guiones.

Por ejemplo, **ps -aux** no es igual a **ps aux**.

Una lista de visualización común (opciones **aux**) muestra todos los procesos, con columnas que serán de interés para los usuarios, e incluye procesos sin un terminal de control. Una lista extensa (opciones **lax**) proporciona detalles más técnicos, pero puede visualizarse más rápidamente porque no realiza la búsqueda de nombre de usuario. La sintaxis de UNIX similar usa las opciones **-ef** para la visualización de todos los procesos.

```
[student@serverX ~]$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
root      1  0.1  0.1  51648  7504 ?        Ss   17:45  0:03 /usr/lib/systemd/syst
root      2  0.0  0.0     0     0 ?        S    17:45  0:00 [kthreadd]
root      3  0.0  0.0     0     0 ?        S    17:45  0:00 [ksoftirqd/0]
root      5  0.0  0.0     0     0 ?        S<  17:45  0:00 [kworker/0:0H]
root      7  0.0  0.0     0     0 ?        S    17:45  0:00 [migration/0]
-- output truncated --
[student@serverX ~]$ ps lax
F  UID      PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY      TIME COMMAND
4  0       1     0  20   0  51648  7504 ep_pol Ss   ?    0:03 /usr/lib/systemd/
1  0       2     0  20   0     0  kthrea S    ?    0:00 [kthreadd]
1  0       3     2  20   0     0  smpboo S    ?    0:00 [ksoftirqd/0]
1  0       5     2  0  -20   0  worker S<  ?    0:00 [kworker/0:0H]
1  0       7     2  -100  -    0  smpboo S    ?    0:00 [migration/0]
-- output truncated --
[student@serverX ~]$ ps -ef
UID      PID  PPID  C STIME TTY      TIME CMD
root      1     0  0 17:45 ?
root      2     0  0 17:45 ?
root      3     2  0 17:45 ?
root      5     2  0 17:45 ?
root      7     2  0 17:45 ?
-- output truncated --
```

De manera predeterminada, el comando **ps** sin opciones selecciona todos los procesos que tienen la misma *identificación de usuario efectivo* (EUID) que el usuario actual y que están asociados con la misma terminal en la que se invocó **ps**.

- Los procesos entre corchetes (normalmente en la parte superior) son subprocesos del kernel programados.
- Los procesos zombies aparecen en una lista ps como *finalizados u obsoletos*.
- **ps** se muestra una vez. Utilice la opción **top(1)** para una visualización de procesos de actualización repetitiva.
- **ps** puede mostrar los resultados en formato de árbol para ver las relaciones de procesos primarios y secundarios.

- El resultado predeterminado no está ordenado. El orden de visualización coincide con el de la tabla de procesos del sistema, que reutiliza las filas de la tabla, ya que ciertos procesos finalizan y otros nuevos se crean. Los resultados pueden aparecer en orden cronológico, pero esto no es seguro a menos que se usen las opciones explícitas **-o** o **--sort**.



Referencias

info libc signal (*Manual de referencia de la biblioteca GNU C*)

- Sección 24: Manejo de señales

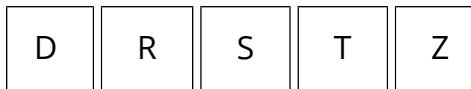
info libc processes (*Manual de referencia de la biblioteca GNU C*)

- Sección 26: Procesos

Páginas del manual: **ps(1)**, **signal(7)**

Práctica: Procesos

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



Descripción	Estado
El proceso se detuvo (se suspendió).	
El proceso ha liberado todos sus recursos, a excepción de su identificador de proceso.	
El proceso se está ejecutando o está esperando para ejecutarse en una CPU.	
El proceso está en espera hasta que se cumpla alguna condición.	
El proceso está esperando E/S o que se cumpla alguna condición y no debe responder a las señales.	

Solución

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

Descripción	Estado
El proceso se detuvo (se suspendió).	T
El proceso ha liberado todos sus recursos, a excepción de su identificador de proceso.	Z
El proceso se está ejecutando o está esperando para ejecutarse en una CPU.	R
El proceso está en espera hasta que se cumpla alguna condición.	S
El proceso está esperando E/S o que se cumpla alguna condición y no debe responder a las señales.	D

Control de trabajos

Objetivos

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

- Explicar los términos "primer plano", "segundo plano" y "terminal de control".
- Utilizar el control de trabajos para administrar múltiples tareas de la línea de comandos.

Trabajos y sesiones

Control de trabajos es una característica de la shell que permite ejecutar y administrar múltiples comandos desde una sola instancia de shell.

Un *trabajo* está asociado con cada tubería ingresada en un aviso de shell. Todos los procesos en esa tubería son parte del trabajo y son miembros del mismo *grupo de procesos*. (Si se ingresa solo un comando en un aviso de shell, puede considerarse como una "tubería" mínima de un comando. Ese comando sería el único miembro de ese trabajo).

Solo un trabajo puede leer entradas y señales generadas por el teclado desde una ventana de terminal específica por vez. Los procesos que sean parte de ese trabajo son procesos *en primer plano* de ese *terminal de control*.

Un proceso *en segundo plano* de dicho terminal de control es un miembro de cualquier otro trabajo asociado con ese terminal. Los procesos en segundo plano de un terminal no pueden leer entradas ni recibir interrupciones generadas por el teclado desde el terminal, pero pueden escribir en el terminal. Un trabajo en segundo plano puede detenerse (suspenderse) o puede estar ejecutándose. Si un trabajo que se está ejecutando en segundo plano intenta leer desde el terminal, se suspenderá automáticamente.

Cada terminal es su propia *sesión* y puede tener un proceso en primer plano y procesos en segundo plano independientes. Un trabajo es parte de exactamente una sesión, la que pertenece a su terminal de control.

El comando **ps** mostrará el nombre del dispositivo del terminal de control de un proceso en la columna **TTY**. Algunos procesos, como *demonios del sistema*, son iniciados por el sistema y no desde un aviso de shell. Estos procesos no tienen un terminal de control, no son miembros de un trabajo y no pueden colocarse en primer plano. El comando **ps** mostrará un signo de pregunta (?) en la columna **TTY** para estos procesos.

Realización de trabajos en segundo plano

Cualquier comando o tubería puede iniciarse en segundo plano si se anexa el signo ampersand (&) al final de la línea de comandos. La shell **bash** muestra un *número de trabajo* (exclusivo de la sesión) y el identificador de proceso del proceso secundario nuevo. La shell no espera al proceso secundario y vuelve a mostrar el aviso de shell.

```
[student@serverX ~]$ sleep 10000 &
[1] 5947
[student@serverX ~]$
```



nota

Cuando se coloca una tubería en segundo plano con un signo ampersand, el identificador de proceso del último comando en la tubería será el de salida. Todos los procesos de la tubería continúan siendo miembros de ese trabajo.

```
[student@serverX ~]$ example_command | sort | mail -s "Sort output" &
[1] 5998
```

La shell **bash** realiza un seguimiento de trabajos, por sesión, en una tabla que se muestra con el comando **jobs**.

```
[student@serverX ~]$ jobs
[1]+  Running                  sleep 10000 &
[student@serverX ~]$
```

Un trabajo en segundo plano se puede colocar en primer plano con el comando **fg** con su ID de trabajo (%*número de trabajo*).

```
[student@serverX ~]$ fg %1
sleep 10000
-
```

En el ejemplo anterior, el comando **sleep** se está ejecutando en primer plano en el terminal de control. La shell se encuentra nuevamente en espera de que se retire el proceso secundario.

Para enviar un proceso en primer plano a segundo plano, presione primero la solicitud de suspensión generada por el teclado (**Ctrl+z**) en el terminal.

```
sleep 10000
^Z
[1]+  Stopped                  sleep 10000
[student@serverX ~]$
```

El trabajo se colocará inmediatamente en segundo plano y se suspenderá.

El comando **ps j** mostrará información relacionada con los trabajos. El PGID es el identificador de proceso del *líder del grupo de procesos*, generalmente el primer proceso en la canalización del trabajo. El SID es el identificador de proceso del *líder de sesión*, que para un trabajo es generalmente la shell interactiva que se está ejecutando en su terminal de control. Dado que el comando **sleep** de ejemplo está suspendido actualmente, su estado de proceso es **T**.

```
[student@serverX ~]$ ps j
  PPID   PID  PGID   SID TTY      TPGID STAT    UID     TIME COMMAND
 2764  2768  2768  2768 pts/0      6377 Ss    1000    0:00 /bin/bash
 2768  5947  5947  2768 pts/0      6377 T     1000    0:00 sleep 10000
 2768  6377  6377  2768 pts/0      6377 R+    1000    0:00 ps j
[student@serverX ~]$
```

Para iniciar el proceso suspendido que se está ejecutando en segundo plano, utilice el comando **bg** con la misma ID de trabajo.

```
[student@serverX ~]$ bg %1  
[1]+ sleep 10000 &  
[student@serverX ~]$
```

La shell emitirá una advertencia al usuario que intente salir de una ventana de terminal (sesión) con trabajos suspendidos. Si el usuario vuelve a intentar salir de inmediato, los trabajos suspendidos se anulan.



Referencias

Es posible encontrar información adicional en el capítulo sobre visualización de procesos de sistemas en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

bash página de información de (*Manual de referencia de BASH para GNU*)

- Sección 7: Control de trabajos

libc página de información (*Manual de referencias de la biblioteca GNU C*)

- Sección 24: Manejo de señales

- Sección 26: Procesos

páginas de manual **bash(1)**, **builtins(1)**, **ps(1)**, **sleep(1)**

Práctica: Procesos de primer y segundo plano

En este ejercicio de laboratorio, los estudiantes iniciarán, suspenderán y se reconectarán a varios procesos con el control de trabajo.

Resultados:

Práctica de suspensión y reinicio de procesos de usuario

Antes de comenzar

Inicie sesión como student en serverX. Comience en el directorio de inicio del estudiante.

1. Abra las dos ventanas de terminal, una al lado de la otra, para que puedan identificarse como *izquierda* y *derecha*.
2. En la ventana izquierda, inicie un proceso que anexe constantemente la palabra "rock" y un espacio en el archivo **~/outfile** con intervalos de un segundo. El conjunto del comando completo debe estar entre paréntesis para que el control de trabajo interprete al conjunto como un trabajo individual.

```
[student@serverX ~]$ (while true; do echo -n "rock " >> ~/outfile; sleep 1; done)
```

3. En la ventana derecha, use **tail** para confirmar que el proceso nuevo se escriba en el archivo.

```
[student@serverX ~]$ tail -f ~/outfile
```

4. En la ventana izquierda, suspenda el proceso que está en ejecución. La shell devuelve la ID de trabajo entre corchetes. En la ventana derecha, confirme que se haya detenido la salida del proceso.

```
[student@serverX ~]$ Ctrl+z
```

5. En la ventana izquierda, visualice la lista de **jobs**. El + indica el *trabajo vigente*. Reinicie el trabajo en segundo plano. En la ventana derecha, confirme que la salida del proceso esté de nuevo activa.

```
[student@serverX ~]$ jobs
[1]+  Stopped                  ( while true; do
      echo -n "rock " >> ~/outfile; sleep 1;
done )
[student@serverX ~]$ bg
[student@serverX ~]$ jobs
```

6. En la ventana izquierda, inicie dos o más procesos para adjuntar el mismo archivo de salida. Reemplace "rock" por "paper" y, a continuación, por "scissors". Para que el proceso esté en segundo plano en forma correcta, el conjunto de comando completo debe estar entre paréntesis y debe finalizar con el signo "&".

```
[student@serverX ~]$ (while true; do echo -n "paper " >> ~/outfile; sleep 1; done) &
[student@serverX ~]$ (while true; do echo -n "scissors " >> ~/outfile; sleep 1;
done) &
```

7. En la ventana izquierda, visualice **jobs** para ver los tres procesos que están en "ejecución". En la ventana derecha, confirme que los tres procesos se estén adjuntando al archivo.

```
[student@serverX ~]$ jobs
```

8. Use solo los comandos que aprendió anteriormente y suspenda el proceso "rock". En la ventana izquierda, coloque en primer plano el trabajo, usando la ID de trabajo determinada de la lista **jobs** y, luego, utilice **Ctrl+z** para suspenderlo. Confirme que se haya detenido el proceso de "rock". En la ventana derecha, confirme que la salida de "rock" ya no esté activa.

```
[student@serverX ~]$ jobs
[student@serverX ~]$ fg %number
[student@serverX ~]$ Ctrl+z
```

9. Finalice el proceso de "paper". En la ventana izquierda, coloque en primer plano el trabajo y, luego, utilice **Ctrl+c** para finalizarlo. Confirme que el proceso de "paper" haya desaparecido. En la ventana derecha, confirme que la salida de "output" ya no esté activa.

```
[student@serverX ~]$ jobs
[student@serverX ~]$ fg %number
[student@serverX ~]$ Ctrl+c
```

10. En la ventana izquierda, visualice el resto de los trabajos que usan **ps**. El trabajo suspendido tiene el estado **T**. El otro trabajo que está en segundo plano está inactivo (**S**), ya que **ps** está "en cpu" (**R**) mientras se muestra.

```
[student@serverX ~]$ ps j
  PPID  PID  PGID   SID TTY      TPGID STAT   UID    TIME COMMAND
 4489  6223  6223   6223 pts/1     12918 Ss   1000   0:00 bash
 4489  6237  6237   6237 pts/2     9782 Ss   1000   0:00 bash
 6237  9782  9782   6237 pts/2     9782 S+   1000   0:00 tail -f /home/student/o
 7360  9856  7360   6223 pts/1     12918 T    1000   0:00 sleep 1
 7395 12916  7395   6223 pts/1     12918 S    1000   0:00 sleep 1
 6223 12918 12918   6223 pts/1     12918 R+   1000   0:00 ps j
```

11. Detenga los dos trabajos restantes. En la ventana de la izquierda, coloque en primer plano cualquier trabajo. Utilice **Ctrl+c** para finalizarlo. Repita con el trabajo restante. El trabajo "detenido" provisoriamente se reinicia cuando pasa a primer plano. Confirme que no queden trabajos y que se haya detenido la salida.

```
[student@serverX ~]$ fg %number
[student@serverX ~]$ Ctrl+c
[student@serverX ~]$ fg %number
[student@serverX ~]$ Ctrl+c
```

Capítulo 7. Administración y control de procesos Linux

```
[student@serverX ~]$ jobs
```

12. En la ventana derecha, detenga el comando **tail**. Cierre las ventanas de terminal extra.

```
[student@serverX ~]$ Ctrl+c
```

Finalización de procesos

Objetivos

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

- Use comandos para finalizar procesos y comunicarse con ellos.
- Defina las características de un proceso demonio.
- Termine sesiones y procesos de usuario.

Control de procesos con señales

Una señal es la interrupción de software que se envía a un proceso. Indica eventos de informe a un programa que está en ejecución. Los eventos que generan una señal pueden ser un *error*, *evento externo* (por ejemplo, una solicitud de entrada o salida, o un temporizador vencido), o una *solicitud explícita* (por ejemplo, el uso de un comando emisor de señal o secuencia de teclado).

La siguiente tabla enumera las señales fundamentales usadas por los administradores del sistema para la administración de procesos de rutina. Puede referirse a las señales ya sea por su nombre abreviado (**HUP**) o nombre propio (**SIGHUP**).

Señales fundamentales de administración de procesos

Número de señal	Nombre abreviado	Definición	Propósito
1	HUP	Colgar	Se usa para informar la finalización del proceso de control de un terminal. Además, se utiliza para solicitar que se reinicie el proceso (volver a cargar la configuración) sin finalización.
2	INT	Interrupción del teclado	Provoca la finalización del programa. Puede bloquearse o manipularse. Enviado al presionar una combinación de teclas INTR (Ctrl+c).
3	QUIT	Salida del teclado	Es similar a SIGINT , pero también provoca el volcado de un proceso en la finalización. Enviado al presionar una combinación de teclas QUIT (Ctrl+\).
9	KILL	Finalización, no se puede bloquear.	Provoca la finalización abrupta del programa. No se puede bloquear, ignorar ni manipular; siempre es grave.
15 <i>Predeterminado</i>	TÉRMINO	Termina	Provoca la finalización del programa. A diferencia de SIGKILL , puede bloquearse, ignorarse o manipularse. Es la manera correcta de solicitar la finalización de un programa; hace posible la autolimpieza.
18	CONT	Continuar	Se envía a un proceso para que se reinicie, en caso de que esté detenido. No puede

Número de señal	Nombre abreviado	Definición	Propósito
			bloquearse. Aún si se manipula, siempre reinicia el proceso
19	STOP	Detener, no se puede bloquear.	Suspende el proceso. No puede bloquearse ni manipularse.
20	TSTP	Detención del teclado	A diferencia de SIGSTOP , puede bloquearse, ignorarse o manipularse. Enviado al presionar una combinación de teclas SUSP (Ctrl+z) .



nota

Los números de señal varían en las distintas plataformas de hardware de Linux, pero los nombres y los significados de las señales están estandarizados. Para el uso del comando, se aconseja usar los nombres de señal en lugar de los números. Los números analizados en esta sección son para los sistemas Intel x86.

Cada señal tiene una *acción predeterminada* que, por lo general, es una de las siguientes:

Term: provoca que un programa finalice (se cierre) de inmediato.

Core: provoca que un programa guarde una imagen de la memoria (volcado central) y que, a continuación, finalice.

Stop: provoca que un programa deje de ejecutarse (se suspenda) y espere para continuar (se reinicie).

Los programas pueden estar preparados para señales de eventos esperadas mediante la implementación de rutinas de controlador que ignoren, reemplacen o amplíen la acción predeterminada de una señal.

Comandos para el envío de señales mediante una solicitud explícita

Los usuarios indican el proceso en primer plano actual mediante la escritura de una secuencia de control de teclado para suspender (**Ctrl+z**), finalizar (**Ctrl+c**), o realizar un volcado central (**Ctrl+**, del proceso. Para indicar un proceso o procesos en primer plano en una sesión diferente, se requiere de un comando emisor de señal.

Las señales pueden especificarse ya sea por nombre (e.g., **-HUP** o **-SIGHUP**) o número (e.g., **-1**). Los usuarios pueden finalizar sus propios procesos, pero se necesitan privilegios de root para finalizar procesos que son propiedad de otros usuarios.

- El comando **kill** envía una señal a un proceso mediante una ID. A pesar de su nombre, el comando **kill** puede usarse para enviar cualquier señal y no solo aquellas para finalizar programas.

```
[student@serverX ~]$ kill PID
[student@serverX ~]$ kill -signal PID
[student@serverX ~]$ kill -1
 1) SIGHUP      2) SIGINT      3) SIGQUIT      4) SIGILL      5) SIGTRAP
 6) SIGABRT     7) SIGBUS      8) SIGFPE       9) SIGKILL     10) SIGUSR1
11) SIGSEGV     12) SIGUSR2     13) SIGPIPE     14) SIGALRM     15) SIGTERM
16) SIGSTKFLT   17) SIGCHLD     18) SIGCONT     19) SIGSTOP     20) SIGTSTP
-- output truncated --
```

- Use la opción **killall** para enviar una señal a uno o más procesos que coincidan con los criterios de selección, como un nombre de comando, procesos que sean propiedad de un usuario específico o procesos de todo el sistema.

```
[student@serverX ~]$ killall command_pattern
[student@serverX ~]$ killall -signal command_pattern
[root@serverX ~]# killall -signal -u username command_pattern
```

- El comando **pkill**, al igual que **killall**, puede emitir una señal de varios procesos. **pkill** usa criterios de selección avanzados, que pueden incluir la combinación de:
 - Command*: procesos con un nombre de comando que coincide con un patrón.
 - UID*: procesos que son propiedad de una cuenta de usuario de Linux, efectiva o real.
 - GID*: procesos que son propiedad de una cuenta de grupo de Linux, efectiva o real.
 - Parent*: procesos secundarios de un proceso principal específico.
 - Terminal*: procesos que se ejecutan en un terminal de control específico.

```
[student@serverX ~]$ pkill command_pattern
[student@serverX ~]$ pkill -signal command_pattern
[root@serverX ~]# pkill -G GID command_pattern
[root@serverX ~]# pkill -P PPID command_pattern
[root@serverX ~]# pkill -t terminal_name -U UID command_pattern
```

Cierre de sesión de usuarios en forma administrativa

El comando **w** visualiza los usuarios que actualmente tienen una sesión iniciada en el sistema y sus actividades acumuladas. Use las columnas **TTY** y **FROM** para determinar la ubicación del usuario.

Todos los usuarios cuentan con un terminal de control, designado como **pts/N** mientras trabajan en una ventana de entorno gráfico (*Pseudo-terminal*) o **ttyN** en una consola del sistema, una consola alternativa u otro dispositivo terminal conectado directamente. Los usuarios remotos muestran su nombre de sistema de conexión en la columna **FROM** cuando usan la opción **-f**.

```
[student@serverX ~]$ w -f
12:43:06 up 27 min, 5 users, load average: 0.03, 0.17, 0.66
USER   TTY     FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
student :0      :0          12:20    ?xdm?   1:10   0.16s gdm-session-wor
student pts/0    :0          12:20    2.00s  0.08s  0.01s w -f
root    tty2          12:26    14:58   0.04s  0.04s -bash
bob     tty3          12:28    14:42   0.02s  0.02s -bash
student pts/1    desktop2.example.12:41  1:07   0.03s  0.03s -bash
[student@serverX ~]$
```

Averigüe cuánto tiempo un usuario estuvo en el sistema con la hora de inicio de sesión. Para cada sesión, los recursos de CPU consumidos por los trabajos actuales, incluidas las tareas en segundo plano y los procesos secundarios, se encuentran en la columna **JCPU**. El consumo de CPU del proceso de primer plano actual está en la columna **PCPU**.

Los usuarios pueden ser obligados a salir del sistema debido a infracciones contra la seguridad, asignación excesiva de recursos o necesidades administrativas. Se espera que

Capítulo 7. Administración y control de procesos Linux

los usuarios salgan de las aplicaciones innecesarias, cierren los intérpretes de comandos no usados y salgan de las sesiones de inicio de sesión cuando se les solicite.

En caso de que se produzcan situaciones en que no es posible comunicarse con los usuarios o tienen sesiones sin respuesta, consumo de recursos descontrolado o acceso al sistema inadecuado, es probable que sus sesiones deban finalizarse en forma administrativa con las señalizaciones.



Importante

A pesar de que **SIGTERM** es la señal predeterminada, **SIGKILL** es el administrador preferido más usado en forma errónea. Ya que la señal **SIGKILL** no puede manipularse ni ignorarse, siempre es grave. Sin embargo, obliga a la finalización sin permitir que el proceso terminado ejecute rutinas de autolimpieza. Se recomienda enviar primero **SIGTERM** y, a continuación, recuperar con **SIGKILL** solo si falla un proceso en la respuesta.

Los procesos y las sesiones pueden señalizarse en forma individual o colectiva. Para finalizar todos los procesos de un usuario, use el comando **pgrep**. Debido a que el proceso inicial en una sesión de inicio de sesión (*líder de sesión*) está diseñado para manipular las solicitudes de finalización de sesión e ignorar las señales de teclado involuntarias, la finalización de todos los procesos y shells de inicio de sesión de un usuario requiere del uso de la señal **SIGKILL**.

```
[root@serverX ~]# pgrep -l -u bob
6964 bash
6998 sleep
6999 sleep
7000 sleep
[root@serverX ~]# pkill -SIGKILL -u bob
[root@serverX ~]# pgrep -l -u bob
[root@serverX ~]#
```

Cuando los procesos que requieren atención están en la misma sesión de inicio de sesión, es probable que no sea necesario finalizar todos los procesos de un usuario. Determine el terminal de control para la sesión con el comando **w** y, a continuación, finalice solo los procesos que hagan referencia a la misma ID de terminal. A menos que se especifique **SIGKILL**, el líder de sesión (en este caso, la shell de inicio de sesión **bash**) manipula y supera en forma correcta la solicitud de finalización, pero finalizan todos los demás procesos de sesión.

```
[root@serverX ~]# pgrep -l -u bob
7391 bash
7426 sleep
7427 sleep
7428 sleep
[root@serverX ~]# w -h -u bob
bob      tty3      18:37      5:04   0.03s  0.03s -bash
[root@serverX ~]# pkill -t tty3
[root@serverX ~]# pgrep -l -u bob
7391 bash
[root@serverX ~]# pkill -SIGKILL -t tty3
[root@serverX ~]# pgrep -l -u bob
[root@serverX ~]#
```

Puede aplicarse el mismo proceso selectivo de finalización con las relaciones de proceso principal y secundario. Use el comando **pstree** para visualizar un árbol de proceso para el sistema o un solo usuario. Use la PID del proceso principal para finalizar todos los procesos secundarios que haya creado. Esta vez, la shell de inicio de sesión **bash** principal sobrevive porque la señal se dirige solo a sus procesos secundarios.

```
[root@serverX ~]# pstree -p bob
bash(8391)─sleep(8425)
              ├sleep(8426)
              └sleep(8427)
[root@serverX ~]# pkill -P 8391
[root@serverX ~]# pgrep -l -u bob
bash(8391)
[root@serverX ~]# pkill -SIGKILL -P 8391
[root@serverX ~]# pgrep -l -u bob
bash(8391)
[root@serverX ~]#
```



Referencias

info libc signal (*Manual de referencia de la biblioteca GNU C*)

- Sección 24: Manejo de señales

info libc processes (*Manual de referencia de la biblioteca GNU C*)

- Sección 26: Procesos

Páginas del manual: **kill(1)**, **killall(1)**, **pgrep(1)**, **pkill(1)**, **pstree(1)**, **signal(7)** y **w(1)**

Práctica: Finalización de procesos

En este ejercicio de laboratorio, los estudiantes usarán secuencias del teclado y señales para administrar y detener procesos.

Resultados:

Experiencia con la observación de resultados de iniciar y detener varios procesos de shell.

Antes de comenzar

Inicie sesión como student en serverX. Comience en su directorio de inicio.

1. Abra las dos ventanas de terminal, una al lado de la otra, para que puedan identificarse como *izquierda* y *derecha*.
2. En la ventana izquierda, inicie tres procesos que adjunten texto de un archivo de salida en intervalos de un segundo. Para que cada proceso esté en segundo plano en forma correcta, el conjunto completo del comando debe estar entre paréntesis y finalizar con un "&".

```
[student@serverX ~]$ (while true; do echo -n "game " >> ~/outfile; sleep 1; done) &
[student@serverX ~]$ (while true; do echo -n "set " >> ~/outfile; sleep 1; done) &
[student@serverX ~]$ (while true; do echo -n "match " >> ~/outfile; sleep 1; done)
&
```

3. En la ventana derecha, use **tail** para confirmar que los tres procesos se adjunten al archivo. En la ventana izquierda, visualice **jobs** para ver los tres procesos que están en "ejecución".

```
[student@serverX ~]$ tail -f ~/outfile
[student@serverX ~]$ jobs
[1]  Running                 ( while true; do
    echo -n "game " >> ~/outfile; sleep 1;
done ) &
[2]- Running                 ( while true; do
    echo -n "set " >> ~/outfile; sleep 1;
done ) &
[3]+ Running                 ( while true; do
    echo -n "match " >> ~/outfile; sleep 1;
done ) &
```

4. Use las señales para suspender el proceso de "games". Confirme que se haya detenido el proceso de "games". En la ventana derecha, confirme que la salida de "games" ya no esté activa.

```
[student@serverX ~]$ kill -SIGSTOP %number
[student@serverX ~]$ jobs
```

5. Use las señales para finalizar el proceso de "set". Confirme que el proceso de "set" haya desaparecido. En la ventana derecha, confirme que la salida de "set" ya no esté activa.

```
[student@serverX ~]$ kill -SIGTERM %number
```

```
[student@serverX ~]$ jobs
```

6. Use las señales para reanudar el proceso de "games". Confirme que el proceso de "games" esté en ejecución. En la ventana derecha, confirme que la salida de "games" esté de nuevo activa.

```
[student@serverX ~]$ kill -SIGCONT %number
[student@serverX ~]$ jobs
```

7. Finalice los dos trabajos restantes. Confirme que no queden trabajos y que se haya detenido la salida. En la ventana izquierda, finalice el comando **tail** en la ventana derecha.

Cierre las ventanas de terminal extra.

```
[student@serverX ~]$ kill -SIGTERM %number
[student@serverX ~]$ kill -SIGTERM %number
[student@serverX ~]$ jobs
[student@serverX ~]$ pkill -SIGTERM tail
[student@serverX ~]$
```

Monitoreo de la actividad de procesos

Objetivos

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

- Interpretar promedio de tiempo activo y de carga.
- Monitorear los procesos en tiempo real.

Promedio de carga

El kernel de Linux calcula una métrica de *promedio de carga* como un *promedio en movimiento exponencial* del *número de carga*, un conteo acumulativo de la CPU de solicitudes activas de recursos del sistema.

- Las *solicitudes activas* se cuentan desde las filas por CPU para subprocessos en ejecución y subprocessos en espera de E/S, ya que el kernel realiza el seguimiento de la actividad de los recursos del proceso y los cambios de estado del proceso correspondiente.
- El *número de carga* es un cálculo de rutina que se ejecuta cada cinco segundos de manera predeterminada, el cual almacena y promedia las solicitudes activas en un número único para todas las CPU.
- El *promedio en movimiento exponencial* es una fórmula matemática para emparejar los extremos de los datos de tendencia, aumentar la importancia de la actividad actual y disminuir la calidad de los datos antiguos.
- El *promedio de carga* es el resultado de la rutina de cálculo del número de carga. En conjunto, se refiere a los tres valores que se muestran de los datos de actividad del sistema, promediados de los últimos 1, 5 y 15 minutos.

Comprensión del cálculo del promedio de carga Linux

El promedio de carga representa la carga del sistema percibida durante un período. Linux implementa el cálculo del promedio de carga como una representación de los tiempos de espera de servicio esperados, no solo de la CPU, sino también de E/S del disco y de la red.

- Linux cuenta los procesos, y también los subprocessos individualmente, como tareas separadas. Las filas de solicitudes de la CPU para subprocessos en ejecución (*nr_running*) y subprocessos en espera de recursos de E/S (*nr_iowait*) lógicamente corresponden a estados de procesos **R** (Ejecución) y **D** (Suspensión ininterrumpida). La espera de E/S incluye la suspensión de tareas para las respuestas esperadas del disco y de la red.
- El número de carga es un cálculo de conteo global, que totaliza la suma para todas las CPU. Dado que las tareas que se retoman después de una suspensión se pueden reprogramar para distintas CPU, los conteos precisos por CPU son difíciles, pero se puede garantizar un conteo acumulativo preciso. Los promedios de carga que se muestran representan a todas las CPU.
- Linux cuenta cada hiperproceso del núcleo físico de una CPU y microprocesador como unidades de ejecución separadas, representadas lógicamente y tratadas como CPU individuales. Cada CPU tiene filas de solicitudes independientes. Vista de **/proc/cpuinfo** para la representación del kernel de las CPU del sistema.

```
[student@serverX ~]$ grep "model name" /proc/cpuinfo
model name : Intel(R) Core(TM) i5 CPU          M 520 @ 2.40GHz
model name : Intel(R) Core(TM) i5 CPU          M 520 @ 2.40GHz
model name : Intel(R) Core(TM) i5 CPU          M 520 @ 2.40GHz
model name : Intel(R) Core(TM) i5 CPU          M 520 @ 2.40GHz
[student@serverX ~]$ grep "model name" /proc/cpuinfo | wc -l
4
```

- Algunos sistemas UNIX solo tenían en cuenta la utilización de la CPU o la longitud de la fila de ejecución para indicar la carga del sistema. Dado que un sistema con CPU inactivas puede experimentar esperas excesivas debido a que los recursos del disco o de la red están ocupados, en el promedio de carga de Linux se tiene en consideración la E/S. Cuando haya promedios altos de carga con actividad mínima de CPU, se debe examinar la actividad del disco y de la red.

Interpretación de los valores que se muestran del promedio de carga

Los tres valores representan los valores calculados durante los últimos 1, 5 y 15 minutos. Una rápida mirada puede indicar si la carga del sistema parece estar subiendo o bajando. Calcule el valor de carga aproximado *por CPU* para determinar si el sistema está experimentando una espera significativa.

- **top, uptime, w y gnome-system-monitor** muestran valores promedio de carga.

```
[student@serverX ~]$ uptime
15:29:03 up 14 min,  2 users,  load average: 2.92, 4.48, 5.20
```

- Dividir los valores promedio de carga que se muestran por el número de CPU lógicas en el sistema. Un valor por debajo de 1 indica utilización de recursos satisfactoria y tiempos de espera mínimos. Un valor por encima de 1 indica saturación de recursos y algo de tiempo de espera del servicio.

```
# From /proc/cpuinfo, system has four logical CPUs, so divide by 4:
#                           load average: 2.92, 4.48, 5.20
#       divide by number of logical CPUs:   4   4   4
#                                         -----
#                           per-CPU load average: 0.73 1.12 1.30
#
# This system's load average appears to be decreasing.
# With a load average of 2.92 on four CPUs, all CPUs were in use ~73% of the time.
# During the last 5 minutes, the system was overloaded by ~12%.
# During the last 15 minutes, the system was overloaded by ~30%.
```

- Una fila de una CPU inactiva tiene número de carga 0. Cada subproceso listo y en espera incrementa el contador en 1. Con un contador de fila total de 1, el recurso (CPU, disco o red) está en uso, pero sin solicitudes en espera. Las solicitudes adicionales incrementan el contador; sin embargo, como muchas solicitudes se pueden procesar dentro del período, aumenta la *utilización* del recurso, pero no los *tiempos de espera*.
- Los procesos en suspensión para E/S debido a un disco o recurso de red ocupados se incluyen en el contador y aumentan el promedio de carga. Mientras no haya una indicación de utilización de la CPU, el contador de la fila continúa indicando que los usuarios y programas están esperando los servicios del recurso.

Capítulo 7. Administración y control de procesos Linux

- Hasta que no se produce una saturación del recurso, un promedio de carga se mantendrá por debajo de 1, dado que las tareas rara vez son encontradas en las filas de espera. El promedio de carga solo aumenta cuando la saturación del recurso provoca que las solicitudes se mantengan en fila y sean contadas por la rutina del cálculo de carga. Cuando la utilización del recurso se aproxima al 100 %, cada solicitud adicional comienza a experimentar un tiempo de espera del servicio.

Monitoreo del proceso en tiempo real

El programa **top** es una vista dinámica de los procesos del sistema, que muestra un encabezado del resumen seguido de un proceso o lista de subprocessos similares a la información de **ps**. A diferencia del resultado estático de **ps**, **top** continuamente se actualiza a un intervalo configurable y ofrece capacidades de reorganización, ordenado y resaltado de columnas. Las configuraciones del usuario se pueden guardar y hacer persistentes.

Las columnas de resultados predeterminadas se diferencian de otras herramientas de recursos en:

- La ID del proceso (**PID**).
- El nombre de usuario (**USER**) es el propietario del proceso.
- La memoria virtual (**VIRT**) es toda la memoria que está utilizando el proceso, incluido el conjunto residente, las bibliotecas compartidas y cualquier página de memoria asignada o intercambiada. (Con la etiqueta **VSZ** en el comando **ps**).
- La memoria residente (**RES**) es la memoria física que utiliza el proceso, incluido cualquier objeto residente compartido. (Con la etiqueta **RSS** en el comando **ps**).
- El estado del proceso **S** se muestra como:
 - **D** = Suspensión ininterrumpida
 - **R** = En ejecución o ejecutable
 - **S** = En suspensión
 - **T** = Detenido o en seguimiento
 - **Z** = Inerte
- El tiempo de CPU (**TIME**) es el tiempo total de procesamiento desde que comenzó el proceso. Se puede alternar para incluir el tiempo acumulativo de todos los procesos secundarios.
- El nombre del comando de proceso (**COMMAND**).

Pulsaciones de tecla fundamentales en top

Clave	Propósito
? o h	Ayudar en pulsaciones de tecla interactiva.
l, t, m	Alternar entre carga, subprocessos y líneas de encabezado de la memoria.
1	Alternar mostrando CPU individuales o un resumen de todas las CPU en el encabezado.

Clave	Propósito
s ⁽¹⁾	Cambiar la tasa de actualización (pantalla), en segundos decimales (p. ej., 0.5, 1, 5).
b	Alternar resaltado reverso para procesos en <i>ejecución</i> ; solo negrita de manera predeterminada.
B	Permite el uso de negrita en la visualización, en el encabezado y en los procesos en <i>ejecución</i> .
H	Alternar subprocessos; mostrar resumen del proceso o subprocessos individuales.
u, U	Filtrar por cualquier nombre de usuario (eficaz, real).
M	Ordenar procesos enumerados por uso de memoria, en orden decreciente.
P	Ordenar procesos enumerados por utilización del procesador, en orden decreciente.
k ⁽¹⁾	Eliminar un proceso. Cuando recibe un aviso, ingresar PID , luego signal .
r ⁽¹⁾	Cambie el valor de niceness de un proceso. Cuando recibe un aviso, ingrese PID , luego nice_value .
w	Escriba (guarde) la configuración actual de la visualización para usar en el próximo reinicio de top .
q	Salir.
Nota:	⁽¹⁾ No está disponible si top se inicia en modo seguro. Ver top(1) .



Referencias

Monitor del Sistema GNOME

- **yelp help:gnome-system-monitor**

Páginas del manual: **ps(1)**, **top(1)**, **uptime(1)** y **w(1)**

Práctica: Control de la actividad de proceso

En este ejercicio de laboratorio, los estudiantes usarán el comando **top** para visualizar, clasificar y detener procesos en forma dinámica.

Resultados

Practicar la administración de procesos en tiempo real.

Antes de comenzar

Realice las siguientes tareas como **student** en la máquina serverX. Ejecute **lab process101 setup** en serverX a fin de prepararse para este ejercicio.

```
[student@serverX ~]$ lab process101 setup
```

1. Abra las dos ventanas de terminal, una al lado de la otra, para que puedan identificarse como *izquierda* y *derecha*. En el terminal derecho, ejecute la utilidad **top**. Modifique el tamaño de la ventana para que sea lo más alta posible.

```
[student@serverX ~]$ top
```

2. En el terminal izquierdo, determine la cantidad de CPU lógicas de esta máquina virtual.

```
[student@serverX ~]$ grep "model name" /proc/cpuinfo | wc -l  
1
```

3. En el terminal izquierdo, ejecute una sola instancia del **process101** ejecutable.

```
[student@serverX ~]$ process101
```

4. En el terminal derecho, observe la pantalla de **top**. Presione las teclas **1**, **t** y **m** en forma individual para alternar la carga, los subprocessos y las líneas del encabezado de memoria. Después de observar este comportamiento, asegúrese de que se muestren todos los encabezados.
5. Anote la ID de proceso (PID) para **process101**. Observe el porcentaje de CPU para el proceso, que se espera que sea alrededor del 25 % o el 30 %.

Observe los promedios de carga. Por ejemplo, en una máquina virtual de una sola CPU, el promedio de carga de un minuto actualmente es inferior al valor de 1. El valor observado puede estar afectado por la contención del recurso desde otra máquina virtual o el host virtual.

6. En el terminal izquierdo, ejecute una segunda instancia de **process101**.

```
[student@serverX ~]$ process101
```

7. En **top**, anote la ID de proceso (PID) para el segundo **process101**. Observe el porcentaje de CPU para el proceso, que también se espera que sea alrededor del 25 % o el 30 %.

Observe de nuevo el promedio de carga de un minuto, que todavía debería ser inferior a 1. Espere un máximo de un minuto para permitir que el cálculo se adapte a la carga de trabajo nueva.

8. En el terminal izquierdo, ejecute una tercera instancia de **process101**.

```
[student@serverX ~]$ process101
```

9. En **top**, anote la ID de proceso (PID) para el tercer **process101**. Observe el porcentaje de CPU para el proceso; una vez más, se espera que sea alrededor del 25 % o el 30 %.

Observe de nuevo el promedio de carga de un minuto, que ahora se espera que sea superior a 1. Espere un máximo de un minuto para permitir que el cálculo se adapte a la carga de trabajo nueva.

10. *Opcional:* si esta máquina virtual tiene más de una CPU lógica, comience lentamente otras instancias de **process101** hasta que el promedio de carga de un minuto iguale o supere la cantidad de CPU lógicas. Divida el valor del promedio de carga por la cantidad de CPU para determinar el promedio de carga calculado por CPU.
11. Una vez que haya finalizado de observar los valores promedio de carga, finalice cada uno de los procesos **process101** desde **top**.
 - 11.1 Presione **k**. Observe el aviso que está debajo de los encabezados y arriba de las columnas.
 - 11.2 Escriba la PID para una de las instancias de **process101**. Presione **Enter**.
 - 11.3 Presione **Enter** de nuevo para usar la señal **SIGTERM** predeterminada de **15**. Confirme que el proceso seleccionado ya no se observe en **top**. Si la PID no se modifica, repita estos pasos de finalización, sustituya la señal **SIGKILL 9** cuando se le solicite.
12. Repita el paso anterior para cada instancia de **process101** restante. Confirme que no quede ninguna instancia de **process101** en **top**.
13. En la ventana derecha, presione **q** para salir de **top**. Cierre las ventanas de terminal extra.

Ejercicio de laboratorio: Monitoreo y administración de procesos de Linux

En este ejercicio de laboratorio, los estudiantes localizarán y administrarán los procesos que utilizan la mayoría de los recursos en un sistema.

Resultados

Experiencia con el uso de **top** como herramienta de administración de procesos.

Andes de comenzar

Ejecute **lab processes setup** como usuario **root** en serverX a fin de prepararse para este ejercicio.

```
[root@serverX ~]# lab processes setup
```

Realice las siguientes tareas como **student** en la máquina serverX.

1. En una ventana de terminal, ejecute la utilidad **top**. Modifique el tamaño de la ventana para que sea lo más alta posible.
2. Observe la pantalla **top**. La pantalla predeterminada ordena los resultados por utilización de la CPU (de mayor a menor). ¿Qué procesos están utilizando la mayoría del tiempo de la CPU?
3. Cambie la pantalla para ordenar el contenido por cantidad de memoria que utiliza cada proceso.
4. ¿Qué procesos tienen las asignaciones de memoria más grandes?
5. Desactive el uso de negrita en la pantalla. Guarde esta configuración para volver a utilizarla cuando se reinicie **top**.
6. Finalice **top** y vuelva a iniciarla. Confirme que la nueva pantalla utilice la configuración guardada; es decir, que la pantalla comience con el contenido ordenado por utilización de memoria y con el uso de negrita desactivado.
7. Modifique la pantalla para que el contenido se ordene por utilización de la CPU una vez más. Active el uso de negrita. Observe que solo las entradas de proceso *Running* o *Runnable* (estado **R**) están en negrita. Guarde esta configuración.
8. Abra otra ventana de terminal si es necesario. Como usuario **root**, suspenda el proceso **hippo**. En **top**, observe que el estado del proceso ahora es **T**.
9. El proceso **hippo** desaparece rápidamente de la pantalla porque ha dejado de usar recursos de la CPU de manera activa. Incluya en una lista la información del proceso de la línea de comandos para confirmar el estado del proceso.
10. Reanude la ejecución de los procesos **hippo**.
11. Cuando termine de observar la pantalla, utilice la línea de comandos para finalizar los procesos extra *elephant* e *hippo*. Confirme que los procesos ya no se vean en **top**.

-
12. Verifique que la limpieza se realice correctamente; para ello, ejecute la secuencia de comandos para calificar. De ser necesario, busque y termine los procesos incluidos en una lista por la secuencia de comandos para calificar y repita dicha secuencia.
 13. Salga de la pantalla de **top**. Cierre las ventanas de terminal extra.

Solución

En este ejercicio de laboratorio, los estudiantes localizarán y administrarán los procesos que utilizan la mayoría de los recursos en un sistema.

Resultados

Experiencia con el uso de **top** como herramienta de administración de procesos.

Antes de comenzar

Ejecute **lab processes setup** como usuario **root** en serverX a fin de prepararse para este ejercicio.

```
[root@serverX ~]# lab processes setup
```

Realice las siguientes tareas como **student** en la máquina serverX.

1. En una ventana de terminal, ejecute la utilidad **top**. Modifique el tamaño de la ventana para que sea lo más alta posible.

```
[student@serverX ~]$ top
top - 12:47:46 up 2:02, 3 users, load average: 1.67, 1.25, 0.73
Tasks: 361 total, 6 running, 355 sleeping, 0 stopped, 0 zombie
%Cpu(s): 98.5 us, 1.4 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 0.1 si, 0.0 st
KiB Mem: 2043424 total, 897112 used, 1146312 free, 1740 buffers
KiB Swap: 4079612 total, 0 used, 4079612 free. 296276 cached Me

      PID USER      PR  NI      VIRT      RES      SHR S %CPU %MEM     TIME+ COMMAND
  4019 root      20   0    4156      76      0 R 57.5  0.0  2:54.15 hippo
 2492 student   20   0 1359500 168420  37492 S 16.8  8.2  3:55.58 gnome-shell
 1938 root      20   0 189648  35972    7568 R  1.9  1.8  0:29.66 Xorg
 2761 student   20   0  620192 19688 12296 S  0.4  1.0  0:04.48 gnome-termi+
output truncated
```

2. Observe la pantalla **top**. La pantalla predeterminada ordena los resultados por utilización de la CPU (de mayor a menor). ¿Qué procesos están utilizando la mayoría del tiempo de la CPU?

A parte de la shell GNOME predeterminada, busque el proceso con el nombre **hippo**.

3. Cambie la pantalla para ordenar el contenido por cantidad de memoria que utiliza cada proceso.

Presione **M**.

```
top - 12:57:38 up 2:11, 3 users, load average: 2.09, 1.70, 1.19
Tasks: 360 total, 5 running, 355 sleeping, 0 stopped, 0 zombie
%Cpu(s): 99.8 us, 0.2 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 2043424 total, 896952 used, 1146472 free, 1740 buffers
KiB Swap: 4079612 total, 0 used, 4079612 free. 296280 cached Mem

      PID USER      PR  NI      VIRT      RES      SHR S %CPU %MEM     TIME+ COMMAND
  2492 student   20   0 1359500 168420  37492 S  0.5  8.2  4:01.04 gnome-shell
  4013 root      20   0  55360  51208   152 S  0.0  2.5  0:00.43 elephant
  1938 root      20   0 189648  35972    7568 R  0.2  1.8  0:30.49 Xorg
  2576 student   20   0  533752  33684 27784 S  0.1  1.6  0:09.29 vmtoolsd
  2420 student   20   0  916268  25616 14404 S  0.0  1.3  0:00.61 gnome-setti+
  2550 student   20   0 1048204 23136 16060 S  0.0  1.1  0:00.46 nautilus
```

```
output truncated
```

- ¿Qué procesos tienen las asignaciones de memoria más grandes?

A parte de la shell GNOME predeterminada y de **Xorg**, busque un proceso con el nombre **elephant**.

- Desactive el uso de negrita en la pantalla. Guarde esta configuración para volver a utilizarla cuando se reinicie **top**.

Presione la tecla **B** mayúscula para desactivar el uso de negrita.

Presione la tecla **W** mayúscula para guardar esta configuración. El archivo de configuración predeterminado es **.toprc** en el directorio principal del usuario actual.

- Finalice **top** y vuelva a iniciararlo. Confirme que la nueva pantalla utilice la configuración guardada; es decir, que la pantalla comience con el contenido ordenado por utilización de memoria y con el uso de negrita desactivado.

Presione **q** para salir de la pantalla actual y, luego, vuelva a ejecutar **top**.

```
[student@serverX ~]$ top
```

- Modifique la pantalla para que el contenido se ordene por utilización de la CPU una vez más. Active el uso de negrita. Observe que solo las entradas de proceso *Running* o *Runnable* (estado **R**) están en negrita. Guarde esta configuración.

Presione la tecla **P** mayúscula para ordenar el contenido por utilización de la CPU.

Presione la tecla **B** mayúscula para activar el uso de negrita.

Presione la tecla **W** mayúscula para guardar esta configuración.

- Abra otra ventana de terminal si es necesario. Como usuario **root**, suspenda el proceso **hippo**. En **top**, observe que el estado del proceso ahora es **T**.

```
[student@serverX ~]$ su -
Password: redhat
[root@serverX ~]# pkill -SIGSTOP hippo
```

- El proceso **hippo** desaparece rápidamente de la pantalla porque ha dejado de usar recursos de la CPU de manera activa. Incluya en una lista la información del proceso de la línea de comandos para confirmar el estado del proceso.

```
[root@serverX ~]# ps -f $(pgrep hippo)
```

- Reanude la ejecución de los procesos **hippo**.

```
[root@serverX ~]# pkill -SIGCONT hippo
```

- Cuando termine de observar la pantalla, utilice la línea de comandos para finalizar los procesos extra **elephant** e **hippo**. Confirme que los procesos ya no se vean en **top**.

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

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

12. Verifique que la limpieza se realice correctamente; para ello, ejecute la secuencia de comandos para calificar. De ser necesario, busque y termine los procesos incluidos en una lista por la secuencia de comandos para calificar y repita dicha secuencia.

```
[root@serverX ~]# lab processes grade
```

13. Salga de la pantalla de **top**. Cierre las ventanas de terminal extra.

Presione **q** para salir.

Resumen

Procesos

Definir los componentes de un proceso e interpretar comandos para la visualización de un proceso.

Control de trabajos

Práctica de amplias técnicas de administración de procesos, que incluyen el inicio, la suspensión y la conexión con múltiples tareas simultáneas.

Finalización de procesos

Use señales para detener, iniciar y recargar procesos y configuraciones de procesos.

Monitoreo de la actividad de procesos

Administrar la carga de trabajo del sistema mediante el uso de promedios de cargas y estadísticas de procesos.



CAPÍTULO 8

CONTROL DE SERVICIOS Y DEMONIOS

Descripción general	
Meta	Controlar y monitorear servicios de red y demonios del sistema con <code>systemd</code> .
Objetivos	<ul style="list-style-type: none">• Enumerar los demonios del sistema y los servicios de red iniciados por el servicio <code>systemd</code> y las unidades socket.• Controlar los demonios del sistema y los servicios de red con <code>systemctl</code>.
Secciones	<ul style="list-style-type: none">• Identificación de procesos del sistema comenzados en forma automática (y práctica)• Control de servicios del sistema (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">• Control de servicios y demonios

Identificación de procesos del sistema comenzados en forma automática

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder enumerar los demonios del sistema y los servicios de red iniciados por el servicio **systemd** y las unidades socket.

Introducción a **systemd**

El arranque del sistema y los procesos del servidor son administrados por *el sistema systemd y el administrador del servicio*. Este programa proporciona un método para activar los recursos del sistema, los demonios del servidor y otros procesos, tanto en el momento del arranque como en un sistema que está en funcionamiento.

Los demonios son procesos que esperan o se ejecutan en segundo plano y realizan varias tareas. Generalmente, los demonios se inician automáticamente en el momento del arranque y continúan ejecutándose hasta que se apaga el sistema o son detenidos manualmente. Por convención, los nombres de muchos programas demonios finalizan con la letra "d".

Para estar atento a las conexiones, un demonio usa un *socket*. Este es el canal de comunicación principal con los clientes locales o remotos. Los sockets pueden ser creados por los demonios o pueden ser separados del demonio y ser creados por otro proceso, como `systemd`. El socket pasa al demonio cuando el cliente establece una conexión.

A menudo, un *servicio* hace referencia a uno o más demonios, pero iniciar o detener un servicio puede, en cambio, hacer una modificación única en el estado del sistema, que no implica dejar un proceso demonio en ejecución después de esto (que se denomina **oneshot**).

Un poco de historia

Durante muchos años, la ID 1 de proceso de los sistemas Linux y UNIX ha sido el proceso **init**. Este proceso era responsable de activar otros servicios en el sistema y es el origen del término "init system". Los demonios usados con más frecuencia se iniciaban en los sistemas en el momento del arranque con las secuencias de comandos *System V* y *LSB*. Estas son secuencias de comandos de la shell y pueden variar de una distribución a otra. Los demonios usados con menos frecuencia se iniciaban a pedido por otro servicio, como **initd** o **xinetd**, que escucha las conexiones del cliente. Estos sistemas tienen muchas limitaciones, que son resueltas con `systemd`.

En Red Hat Enterprise Linux 7, la ID 1 de proceso es **systemd**, que es el sistema init nuevo. Algunas de las funciones nuevas que proporciona `systemd` son:

- Capacidades de paralelización, que aumentan la velocidad de arranque de un sistema.
- Inicio a pedido de los demonios sin necesidad de otro servicio.
- Administración de dependencia del servicio automática, que puede prevenir los tiempos de inactividad prolongados, como evitar que se inicie un servicio de red cuando la red no está disponible.
- Método para realizar el seguimiento de los procesos relacionados en forma conjunta con el uso de los grupos de control de Linux.



nota

Con systemd, se usan las secuencias de comandos del servicio basado en la shell solo para algunos servicios heredados. Por lo tanto, se reemplazan los archivos de configuración con las variables de la shell, como aquellos que se encuentran en **/etc/sysconfig**. Aquellos que todavía están en uso están incluidos como archivos del entorno systemd y se leen como pares NOMBRE=VALOR. Ya no se proporcionan como una secuencia de comandos de la shell.

Unidades **systemctl** y **systemd**

El comando **systemctl** se usa para administrar diferentes tipos de objetos de systemd denominados *unidades*. Con **systemctl -t help** puede mostrarse una lista de los tipos de unidades disponibles.



Importante

El **systemctl** puede abreviar u "omitar" los nombres de unidad, las entradas de árbol de proceso y las descripciones de unidad, a menos que se ejecute con la opción **-l**.

A continuación, se enumeran algunos de los tipos de unidades más usados:

- Las unidades de servicio tienen la extensión **.service** y representan servicios del sistema. Este tipo de unidad se usa para iniciar los demonios usados con más frecuencia, como un servidor web.
- Las unidades socket tienen la extensión **.socket** y representan sockets de comunicación entre procesos (IPC). El control del socket pasará a un demonio o servicio iniciado recientemente cuando se realice una conexión de cliente. Las unidades de socket se usan para demorar el inicio de un servicio en el momento del arranque y para iniciar servicios usados con menos frecuencia a pedido. En principio, son similares a los servicios que usan el superservidor **xinetd** para iniciar a pedido.
- Las unidades de ruta tienen la extensión **.path** y se usan para demorar la activación de un servicio hasta que ocurra un cambio en el sistema de archivos específico. Esto se usa con más frecuencia en servicios que utilizan directorios de cola, como los sistemas de impresión.

Estados de servicio

El estado de un servicio puede visualizarse con **systemctl status name.type**. Si no se proporciona el tipo de unidad, **systemctl** mostrará el estado de la unidad de servicio, en caso de que exista una.

```
[root@serverX ~]# systemctl status sshd.service
sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled)
   Active: active (running) since Thu 2014-02-27 11:51:39 EST; 7h ago
     Main PID: 1073 (sshd)
        CGroup: /system.slice/sshd.service
                  └─1073 /usr/sbin/sshd -D
```

Capítulo 8. Control de servicios y demonios

```
Feb 27 11:51:39 server0.example.com systemd[1]: Started OpenSSH server daemon.
Feb 27 11:51:39 server0.example.com sshd[1073]: Could not load host key: /et.....
Feb 27 11:51:39 server0.example.com sshd[1073]: Server listening on 0.0.0.0 ....
Feb 27 11:51:39 server0.example.com sshd[1073]: Server listening on :: port 22.
Feb 27 11:53:21 server0.example.com sshd[1270]: error: Could not load host k...y
Feb 27 11:53:22 server0.example.com sshd[1270]: Accepted password for root f...2
Hint: Some lines were ellipsized, use -l to show in full.
```

En el resultado del estado, se pueden encontrar varias palabras clave que indican el estado del servicio:

Palabra clave:	Descripción:
loaded (cargado)	Se procesó el archivo de configuración de la unidad.
active (activo); en ejecución	En ejecución con uno o más procesos en curso.
active (activo); cerrado	Se completó correctamente la configuración de una sola vez.
active (activo); en espera	En ejecución, pero a la espera de un evento.
inactive (inactivo)	Detenido.
habilitado	Se iniciará en el momento del arranque.
deshabilitado	No se iniciará en el momento del arranque.
estático	No puede habilitarse, pero puede iniciarse por una unidad habilitada en forma automática.



nota

El comando **systemctl status NAME** reemplaza al comando **service NAME status** usado en versiones anteriores de Red Hat Enterprise Linux.

Enumeración de los archivos de unidad con systemctl

En este ejemplo, continúe con los próximos pasos mientras el instructor realiza una demostración sobre cómo obtener la información de estado de los servicios.



nota

Observe que el comando **systemctl** paginará automáticamente el resultado con **less**.

1. Consulte el estado de todas las unidades para verificar el arranque del sistema.

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

2. Consulte el estado solo de las unidades de servicio.

```
[root@serverX ~]# systemctl --type=service
```

3. Investigue alguna unidad que tenga el estado de falla o mantenimiento. Otra alternativa es agregar la opción **-l** para mostrar el resultado completo.

```
[root@serverX ~]# systemctl status rngd.service -l
```

4. El argumento **status** también puede usarse para determinar si una unidad en particular está activa y mostrar si la unidad está habilitada para iniciarse en el momento del arranque. Los comandos alternativos también pueden mostrar con facilidad los estados activo y habilitado:

```
[root@serverX ~]# systemctl is-active sshd  
[root@serverX ~]# systemctl is-enabled sshd
```

5. Enumere el estado activo de todas las unidades cargadas. Otra opción es limitar el tipo de unidad. La opción **--all** agregará unidades inactivas.

```
[root@serverX ~]# systemctl list-units --type=service  
[root@serverX ~]# systemctl list-units --type=service --all
```

6. Visualice los parámetros de configuración de habilitado e inhabilitado para todas las unidades. Otra opción es limitar el tipo de unidad.

```
[root@serverX ~]# systemctl list-unit-files --type=service
```

7. Visualice solo los servicios con fallas.

```
[root@serverX ~]# systemctl --failed --type=service
```



Referencias

Páginas del manual **systemd(1)**, **systemd.unit(5)**, **systemd.service(5)**, **systemd.socket(5)** y **systemctl(1)**

Es posible encontrar información adicional en el capítulo sobre la administración de servicios con **systemd** en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Práctica: Identificar el estado de unidades systemd

En este ejercicio de laboratorio, identificará los servicios que estén instalados y funcionando en el sistema.

Resultados:

Una lista de servicios activos y habilitados en el sistema.

Antes de comenzar

Restablezca su sistema serverX.

1. Enumere todas las unidades de servicio en el sistema.

```
[student@serverX ~]$ systemctl list-units --type=service
```

2. Enumere todas las unidades de socket, activas e inactivas, en el sistema.

```
[student@serverX ~]$ systemctl list-units --type=socket --all
```

3. Explore el estado del servicio **chrony**. Este servicio se utiliza para la sincronización del tiempo en red (NTP).

- 3.1. Muestre el estado del servicio **chrony**. Observe la ID del proceso de todos los demonios activos.

```
[student@serverX ~]$ systemctl status chronyd
```

- 3.2. Confirme que los demonios enumerados estén funcionando.

```
[student@serverX ~]$ ps -p PID
```

4. Explore el estado del servicio **sshd**. Este servicio se utiliza para una comunicación cifrada segura entre sistemas.

- 4.1. Determine si el servicio **sshd** está habilitado para comenzar en el arranque del sistema.

```
[student@serverX ~]$ systemctl is-enabled sshd
```

- 4.2. Determine si el servicio **sshd** está activo sin mostrar toda la información de estado.

```
[student@serverX ~]$ systemctl is-active sshd
```

- 4.3. Muestre el estado del servicio **sshd**.

```
[student@serverX ~]$ systemctl status sshd
```

5. Enumere los estados habilitados y deshabilitados de todas las unidades de servicio.

```
[student@serverX ~]$ systemctl list-unit-files --type=service
```

Control de servicios del sistema

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder controlar los demonios del sistema y los servicios de red con **systemctl**.

Iniciar y detener demonios del sistema en un sistema en funcionamiento.

Los cambios realizados en un archivo de configuración u otros tipos de actualizaciones de servicio posiblemente requieran el reinicio del servicio. Un servicio que ya no se utiliza puede detenerse antes de quitar el software. Un servicio que no se utilice frecuentemente puede ser iniciado manualmente por un administrador solo cuando sea necesario.

En este ejemplo, realice los siguientes pasos mientras el instructor realiza una demostración de cómo administrar servicios en un sistema en funcionamiento.

1. Vea el estado de un servicio.

```
[root@serverX ~]# systemctl status sshd.service
```

2. Verifique que el proceso esté en funcionamiento.

```
[root@serverX ~]# ps -up PID
```

3. Detenga el servicio y verifique el estado.

```
[root@serverX ~]# systemctl stop sshd.service  
[root@serverX ~]# systemctl status sshd.service
```

4. Inicie el servicio y vea el estado. La ID del proceso ha cambiado.

```
[root@serverX ~]# systemctl start sshd.service  
[root@serverX ~]# systemctl status sshd.service
```

5. Detenga y, luego, inicie el servicio con un solo comando.

```
[root@serverX ~]# systemctl restart sshd.service  
[root@serverX ~]# systemctl status sshd.service
```

6. Emite instrucciones para que un servicio lea y vuelva a cargar su archivo de configuración sin que se detenga completamente y se inicie. La ID del proceso no cambiará.

```
[root@serverX ~]# systemctl reload sshd.service  
[root@serverX ~]# systemctl status sshd.service
```

Dependencias de unidades

Los servicios pueden iniciarse como dependencias de otros servicios. Si una unidad de socket está habilitada y la unidad de servicio con el mismo nombre no lo está, el servicio se iniciará automáticamente cuando se realice una solicitud en el socket de red. Los servicios también pueden ser activados por unidades de ruta cuando se cumple una condición del sistema de archivos. Por ejemplo, un archivo colocado en el directorio de colas de impresión hará que el servicio de impresión **cups** se inicie si no está funcionando.

```
[root@serverX ~]# systemctl stop cups.service
Warning: Stopping cups, but it can still be activated by:
  cups.path
  cups.socket
```

Para detener completamente los servicios de impresión en un sistema, detenga las tres unidades. Al deshabilitar el servicio, se deshabilitarán las dependencias.

El comando **systemctl list-dependencies UNIT** puede utilizarse para imprimir un árbol de las otras unidades que deben iniciarse si se inicia la unidad especificada. Según la dependencia exacta, la otra unidad posiblemente deba estar funcionando antes o después de que se inicia la unidad especificada. La opción **--reverse** de este comando mostrará las unidades que deben tener la unidad especificada iniciada para ejecutarse.

Enmascaramiento de servicios

En ocasiones, es posible que en un sistema haya servicios en conflicto instalados. Por ejemplo, hay múltiples métodos para administrar redes (red y NetworkManager) y firewalls (iptables y firewalld). A fin de evitar que un administrador inicie un servicio por error, existe la opción de *enmascararese* servicio. El enmascaramiento creará un enlace en los directorios de configuración de modo que nada ocurra en caso de que se inicie el servicio.

```
[root@serverX ~]# systemctl mask network
ln -s '/dev/null' '/etc/systemd/system/network.service'
[root@serverX ~]# systemctl unmask network
rm '/etc/systemd/system/network.service'
```



Importante

Un servicio deshabilitado no se iniciará automáticamente en el arranque ni a través de otros archivos de unidad, pero puede iniciarse manualmente. Un servicio enmarcado no puede iniciarse de manera manual ni automática.

Habilitación de demonios del sistema para que se inicien o detengan durante el arranque

El inicio de un servicio en un sistema en funcionamiento no garantiza el inicio del servicio cuando se vuelva a arrancar el sistema. De manera similar, el detenimiento de un servicio en un sistema en funcionamiento no evitará que se reinicie cuando se vuelva a arrancar el sistema. Los servicios se inician durante el proceso de arranque cuando se crean enlaces en los directorios de configuración **systemd** correspondientes. Dichos vínculos se crean y quitan con comandos **systemctl**.

Capítulo 8. Control de servicios y demonios

En este ejemplo, realice los siguientes pasos mientras el instructor realiza una demostración sobre cómo habilitar y deshabilitar los servicios.

1. Vea el estado de un servicio.

```
[root@serverX ~]# systemctl status sshd.service
```

2. Deshabilite el servicio y verifique el estado. Tenga en cuenta que la deshabilitación de un servicio no detiene el servicio.

```
[root@serverX ~]# systemctl disable sshd.service
[root@serverX ~]# systemctl status sshd.service
```

3. Habilite el servicio y verifique el estado.

```
[root@serverX ~]# systemctl enable sshd.service
[root@serverX ~]# systemctl is-enabled sshd.service
```

Resumen de los comandos `systemctl`

Los servicios pueden iniciarse y detenerse en un sistema en funcionamiento, y habilitarse o deshabilitarse para que se inicien automáticamente durante el proceso de arranque.

Tarea:	Comando:
Ver información detallada sobre el estado de una unidad.	<code>systemctl status UNIT</code>
Detener un servicio en un sistema en funcionamiento.	<code>systemctl stop UNIT</code>
Iniciar un servicio en un sistema en funcionamiento.	<code>systemctl start UNIT</code>
Reiniciar un servicio en un sistema en funcionamiento.	<code>systemctl restart UNIT</code>
Volver a cargar el archivo de configuración de un servicio en ejecución.	<code>systemctl reload UNIT</code>
Deshabilitar completamente el inicio (tanto manual como durante el proceso de arranque) de un servicio.	<code>systemctl mask UNIT</code>
Poner un servicio enmascarado a disposición.	<code>systemctl unmask UNIT</code>
Configurar un servicio para que se inicie durante el proceso de arranque.	<code>systemctl enable UNIT</code>
Deshabilitar el inicio de un servicio durante el proceso de arranque.	<code>systemctl disable UNIT</code>
Enumerar unidades necesarias y deseadas por la unidad especificada.	<code>systemctl list-dependencies UNIT</code>



Referencias

Páginas del manual **systemd(1)**, **systemd.unit(5)**, **systemd.service(5)**, **systemd.socket(5)** y **systemctl(1)**

Es posible encontrar información adicional en el capítulo sobre la administración de servicios con **systemd** en la *Guía del administrador del sistema Red Hat Enterprise Linux para Red Hat Enterprise Linux 7*, que se puede encontrar en

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

Práctica: Uso de systemctl para administrar servicios

En este ejercicio de laboratorio, administrará una unidad de servicio que ya está instalada en el sistema.

Resultados:

Se inhabilita el servicio **chronyd** y ya no se ejecuta en el sistema.

Antes de comenzar

Restablezca su sistema serverX.

- Observe los resultados de **systemctl restart** y los comandos **systemctl reload**.

- Muestre el estado del servicio **sshd**. Tenga en cuenta la ID de proceso de demonio.

```
[student@serverX ~]$ systemctl status sshd
```

- Reinic peace el servicio **sshd** y visualice el estado. Cambió la ID de proceso del demonio.

```
[student@serverX ~]$ sudo systemctl restart sshd
[student@serverX ~]$ systemctl status sshd
```

- Vuelva a cargar el servicio **sshd** y visualice el estado. La ID de proceso del demonio no cambió y no se interrumpieron las conexiones.

```
[student@serverX ~]$ sudo systemctl reload sshd
[student@serverX ~]$ systemctl status sshd
```

- Verifique que el servicio **chronyd** se esté ejecutando.

```
[student@serverX ~]$ systemctl status chronyd
```

- Detenga el servicio **sshd** y visualice el estado.

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

- Determine si el servicio **chronyd** está habilitado para comenzar en el arranque del sistema.

```
[student@serverX ~]$ systemctl is-enabled chronyd
```

- Reinic peace el sistema y, a continuación, visualice el estado del servicio **chronyd**.

```
[student@serverX ~]$ systemctl status chronyd
```

-
6. Inhabilite el servicio **chronyd** para que no se inicie en el arranque del sistema y, luego, visualice el estado del servicio.

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

7. Reinicie el sistema y, a continuación, visualice el estado del servicio **chronyd**.

```
[student@serverX ~]$ systemctl status chronyd
```

Ejercicio de laboratorio: Control de servicios y demonios

En este ejercicio de laboratorio, administrará una unidad de servicio que ya está instalada en el sistema.

Resultados:

El servicio **psacct** está habilitado y en funcionamiento en el sistema, y el servicio **rsyslog** está deshabilitado y ya no está en ejecución en el sistema.

Antes de comenzar

Restablezca su sistema serverX.

1. Inicie el servicio **psacct**.
2. Configure el servicio **psacct** para que comience en el arranque del sistema.
3. Detenga el servicio **rsyslog**.
4. Configure el servicio **rsyslog** para que no se inicie en el momento de arranque del sistema.
5. Reinicie el sistema; a continuación, ejecute **lab services grade** para verificar la configuración.

Solución

En este ejercicio de laboratorio, administrará una unidad de servicio que ya está instalada en el sistema.

Resultados:

El servicio **psacct** está habilitado y en funcionamiento en el sistema, y el servicio **rsyslog** está deshabilitado y ya no está en ejecución en el sistema.

Andes de comenzar

Restablezca su sistema serverX.

1. Inicie el servicio **psacct**.

```
[student@serverX ~]$ sudo systemctl start psacct  
[student@serverX ~]$ sudo systemctl status psacct
```

2. Configure el servicio **psacct** para que comience en el arranque del sistema.

```
[student@serverX ~]$ sudo systemctl enable psacct  
[student@serverX ~]$ sudo systemctl status psacct
```

3. Detenga el servicio **rsyslog**.

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

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

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

5. Reinicie el sistema; a continuación, ejecute **lab services grade** para verificar la configuración.

```
[student@serverX ~]$ lab services grade
```

Resumen

Identificación de procesos del sistema comenzados en forma automática

Determinar el estado de los demonios del sistema y los servicios de red iniciados por **systemd**.

Control de servicios del sistema

Iniciar, detener y habilitar servicios usando **systemctl**.



CAPÍTULO 9

CONFIGURACIÓN Y PROTECCIÓN DEL SERVICIO OPENSSH

Descripción general	
Meta	Configurar acceso seguro a la línea de comandos en sistemas remotos con OpenSSH
Objetivos	<ul style="list-style-type: none">Inicie sesión en un sistema remoto usando ssh para ejecutar comandos desde el aviso de shell.Configure ssh para permitir inicios de sesión seguros sin contraseña mediante el uso de un archivo de clave de autenticación privada.Personalice la configuración de sshd para limitar los inicios de sesión directos como root o para deshabilitar la autenticación con contraseña.
Secciones	<ul style="list-style-type: none">Acceso a la línea de comandos remota con SSH (y práctica)Configuración de autenticación con clave de SSH (y práctica)Personalización de la configuración del servicio SSH (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">Configuración y protección del servicio OpenSSH

Acceso a la línea de comandos remota con SSH

Objetivo

Tras finalizar esta sección, los estudiantes deberían poder iniciar sesión en un sistema remoto usando ssh para ejecutar comandos desde su aviso de shell.

¿Qué es OpenSSH secure shell (SSH)?

El término OpenSSH hace referencia a la implementación del software **Secure Shell** que se utiliza en el sistema. OpenSSH **Secure Shell**, **ssh**, se utiliza para ejecutar una shell en un sistema remoto de manera segura. Si tiene una cuenta de usuario en un sistema Linux remoto que proporciona los servicios SSH, **ssh** es el comando normalmente usado para iniciar sesión de manera remota en ese sistema. El comando **ssh** también se puede usar para ejecutar un comando individual en un sistema remoto.

Ejemplos de Secure Shell

Aquí le mostramos algunos ejemplos de la sintaxis del comando **ssh** para el inicio de sesión remoto y la ejecución remota:

- Cree una shell interactiva remota como el usuario actual y, luego, vuelva a su shell anterior cuando termine con el comando **exit**.

```
[student@host ~]$ ssh remotehost  
student@remotehost's password:  
[student@remotehost ~]$ exit  
Connection to remotehost closed.  
[student@host ~]$
```

- Conéctese a una shell remota como un usuario diferente (**remoteuser**) en un host seleccionado (**remotehost**):

```
[student@host ~]$ ssh remoteuser@remotehost  
remoteuser@remotehost's password:  
[remoteuser@remotehost ~]$
```

- Ejecute un único comando (**hostname**) en un host remoto (**remotehost**) y como usuario remoto (**remoteuser**) de manera que regrese la salida a la pantalla local:

```
[student@host ~]$ ssh remoteuser@remotehost hostname  
remoteuser@remotehost's password:  
remotehost.example.com  
[student@host ~]$
```

El comando **w** muestra una lista de usuarios actualmente con sesión activa en el equipo. Esto es especialmente útil para mostrar qué usuarios están con sesión activa con **ssh**, desde qué ubicaciones remotas y qué están haciendo.

```
[student@host ~]$ w -f
```

USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
student	tty1	:0	Wed08	2days	1:52m	0.07s	pam: gdm-passwo
root	tty6	-		12:33	4:14m	16.27s	15.74s -bash
student	pts/0	:0.0	Wed08		5:11	1.63s	/usr/bin/gnome-
student	pts/1	:0.0	Wed08		43:44	14.48s	13.81s vim hello.c
student	pts/3	:0.0	Wed14		0.00s	0.06s	0.06s w
visitor	pts/6	server2.example. 09:22		3:14	0.02s	0.02s	-bash

En este ejemplo, el usuario *student* inició sesión en la consola virtual 1 (**tty1**) mediante el inicio de sesión gráfico (**:0**) aproximadamente a las 8:00 del miércoles. El usuario *student* actualmente tiene tres pseudoterminales abiertos (**pts/0**, **pts/1**, and **pts/3**) iniciados mediante el entorno gráfico; estos son, casi con certeza, ventanas de terminales. En una ventana, *student* está editando **hello.c**. El usuario *root* inició sesión en la consola virtual 6, hoy a las 12:33. El usuario *visitor* inició sesión en el pseudoterminal 6 hoy a las 09:22 desde el host server2.example.com (observe que el nombre ha sido truncado), probablemente con **ssh**, y ha estado inactivo en su aviso de shell durante 3 minutos y 14 segundos.

Llaves SSH del host

SSH asegura la comunicación a través del cifrado con llave pública. Cuando un cliente **ssh** se conecta a un servidor SSH, antes de que el cliente inicie sesión, el servidor le envía una copia de su *llave pública*. Esto se utiliza con el fin de establecer el cifrado seguro para el canal de comunicación y autenticar el servidor para el cliente.

La primera vez que un usuario utiliza **ssh** para conectarse a un servidor en particular, el comando **ssh** almacena la llave pública del servidor en el archivo **~/.ssh/known_hosts** del usuario. Cada vez que el usuario se conecte nuevamente, el cliente se asegura de obtener la misma clave pública desde el servidor comparando la entrada del servidor en el archivo **~/.ssh/known_hosts** con la clave pública que envió el servidor. Si las claves *no* coinciden, el cliente supone que el tráfico de red sufre un secuestro o que el servidor está en riesgo, e interrumpe la conexión.

Esto significa que, si se cambia una clave pública del servidor (porque la clave se perdió debido a una falla en el disco duro o porque fue reemplazada por alguna razón legítima), los usuarios deberán actualizar los archivos **~/.ssh/known_hosts** para eliminar la entrada anterior y, así, poder entrar.

- Las identificaciones del host se almacenan en **~/.ssh/known_hosts** en su sistema cliente local:

```
$ cat ~/.ssh/known_hosts
remotehost,192.168.0.101 ssh-rsa AAAAB3Nzac...
```

- Las claves de host se almacenan en **/etc/ssh/ssh_host_key*** en el servidor SSH.

```
$ ls /etc/ssh/*key*
ssh_host_dsa_key      ssh_host_key          ssh_host_rsa_key
ssh_host_dsa_key.pub  ssh_host_key.pub      ssh_host_rsa_key.pub
```



nota

Un enfoque aún mejor consiste en añadir entradas haciendo coincidir los archivos **ssh_host_*****key.pub** de un servidor con los del usuario **~/.ssh/known_hosts** o los de todo el sistema **/etc/ssh/ssh_known_hosts** anticipadamente cuando cambian las claves públicas. Consulte **ssh-copy-id(1)** para conocer una manera avanzada de administrar las claves ssh.



Referencias

Es posible encontrar información adicional en el capítulo sobre el uso de la utilidad ssh en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Páginas del manual: **ssh(1)**, **w(1)**, **hostname(1)**

Práctica: Acceso remoto a la línea de comandos

En este ejercicio de laboratorio, los estudiantes iniciarán sesión en un sistema remoto como usuarios diferentes y ejecutarán los comandos.

Resultados:

Los estudiantes iniciarán sesión en un sistema remoto y ejecutarán los comandos con la shell segura OpenSSH.

1. Inicie sesión como student en su máquina desktopX.
2. Ejecute **ssh** en su equipo serverX. Acepte la clave de host (si se le solicita). La clave de host se registra en nuestra máquina local para identificar la máquina remota. El comando **ssh** no se podrá ejecutar en forma correcta si el host ssh remoto tiene otra clave que no es la que está registrada como clave de host. Los registros de la clave de host se guardan en el archivo **known_hosts** en el directorio **.ssh**, en el directorio principal del usuario en el sistema local.

```
[student@desktopX ~]$ ssh student@serverX
The authenticity of host 'serverX (172.25.X.11)' can't be established.
ECDSA key fingerprint is 47:bf:82:cd:fa:68:06:ee:d8:83:03:1a:bb:29:14:a3.
Are you sure you want to continue connecting (yes/no)? yes
student@serverX's password: student
```

3. Ejecute el comando **w**. El resultado de **w** indica claramente que iniciamos sesión como usuario student desde desktopX.

```
[student@serverX ~]$ w -f
11:01:23 up 1 day, 19:10, 1 user, load average: 0,0,0
USER   TTY   FROM      LOGIN@ IDLE   JCPU   PCPU   WHAT
student pts/1 desktopX 11:01  0.00s  0.12s  0.09s w
```

4. Ejecute el comando **exit** para finalizar la conexión de shell segura.

```
[student@serverX ~]$ exit
[student@desktopX ~]$
```

5. Esta vez, ejecute **ssh** para su máquina de serverX como usuario **root**.

```
[student@desktopX ~]$ ssh root@serverX
root@serverX's password: redhat
[root@serverX ~]#
```

6. Ejecute el comando **w** nuevamente. En esta oportunidad, el resultado de **w** muestra la conexión activa a la cuenta del usuario root desde desktopX.

```
[root@serverX ~]# w -f
11:01:23 up 1 day, 19:10, 1 user, load average: 0,0,0
```

Capítulo 9. Configuración y protección del servicio OpenSSH

```
USER      TTY      FROM      LOGIN@ IDLE    JCPU   PCPU
root      pts/2    desktopX  11:09   0.00s  0.13s  0.08s w
```

- Ejecute el comando **exit** para finalizar la conexión de shell segura.

```
[root@serverX ~]# exit
[student@desktopX ~]$
```

- Existen diferentes motivos acerca de por qué el host remoto podría haber cambiado en forma legítima su clave de host. Una razón habitual es cuando la máquina remota se reemplaza debido a una falla de hardware o se reinstala. Por lo general, es aconsejable solo eliminar la entrada de clave para el host en el archivo **known_hosts**. En este caso, hay solo una entrada de host en **known_hosts**; por lo tanto, puede eliminarse en forma completa. Elimine el archivo **known_hosts** para el usuario student.

```
[student@desktopX ~]$ rm ~/.ssh/known_hosts
```

- Vuelva a ejecutar **ssh** en serverX como **root**. Acepte la clave, inicie sesión y, luego, salga de la sesión.

```
[student@desktopX ~]$ ssh root@serverX
The authenticity of host 'serverX (::1)' can't be established.
ECDSA key fingerprint is 47:bf:82:cd:fa:68:06:ee:d8:83:03:1a:bb:29:14:a3.
Are you sure you want to continue connecting (yes/no)? yes
root@serverX's password: redhat
[root@serverX ~]# exit
[student@desktopX ~]$
```

- Use **ssh** de forma no interactiva para ejecutar el comando **hostname** en serverX como **root**.

```
[student@desktopX ~]$ ssh root@serverX hostname
root@serverX's password: redhat
serverX.example.com
```

Configuración de autenticación basada en llaves SSH

Objetivo

Tras finalizar esta sección, los estudiantes deberían poder configurar SSH para permitir inicios de sesión seguros sin contraseñas mediante el uso de un archivo de llave de autenticación privada.

Autenticación mediante llave SSH

Los usuarios pueden autenticar los inicios de sesión **ssh** sin una contraseña si utilizan *autenticación mediante llave pública*. **ssh** permite que los usuarios realicen la autenticación usando un esquema de llave privada y pública. Esto significa que se generan dos llaves: una privada y una pública. El archivo de llave privada se utiliza como credencial de autenticación y, al igual que una contraseña, debe ser secreta y segura. La llave pública se copia en los sistemas en los que el usuario desea iniciar sesión y se utiliza para verificar la llave privada. No es necesario que la llave pública sea secreta. Un servidor SSH que tiene llave pública puede emitir una pregunta que solo un sistema que guarde su llave privada podrá responder. En consecuencia, usted puede realizar la autenticación con la presencia de su llave. Esto le permite acceder a los sistemas sin que sea necesario escribir siempre una contraseña y, aun así, la acción sigue siendo segura.

La generación de claves se realiza con el comando **ssh-keygen**. Este comando genera la clave privada `~/.ssh/id_rsa` y la clave pública `~/.ssh/id_rsa.pub`.



nota

Durante la generación de claves, tiene la opción de especificar una frase de contraseña, la cual será necesaria para acceder a su clave privada. En caso de robo de la clave privada, resultará muy difícil para cualquiera que no sea el emisor usarla si está protegida con una frase de contraseña. Esto le da tiempo para crear un nuevo par de claves y quitar todas las referencias relacionadas con las anteriores, antes de que un intruso que haya decodificado la clave privada pueda utilizarla.

Siempre es recomendable proteger la clave privada con una frase contraseña, ya que la clave le permite acceder a otras máquinas. Sin embargo, esto significa que deberá escribir su frase de contraseña cada vez que utilice la clave, de manera que el proceso de autenticación deja de ser sin contraseña. Esto puede evitarse utilizando **ssh-agent**, al que se le puede dar la frase de contraseña una vez al comienzo de la sesión (mediante **ssh-add**), de modo que la pueda proporcionar cuando sea necesario mientras mantenga la sesión iniciada.

Para obtener información adicional sobre el comando **ssh-agent**, consulte la Guía de administración de Red Hat System, capítulo 8.2.4.2.: Configuración de ssh-agent.

Una vez que se hayan generado las claves SSH, se guardarán de modo predeterminado en el directorio `.ssh/` de su directorio principal. Los permisos deben ser 600 en la clave privada y 644 en la clave pública.

Capítulo 9. Configuración y protección del servicio OpenSSH

Para poder usar la autenticación mediante claves, la clave pública debe copiarse en el sistema de destino. Esto puede realizarse con **ssh-copy-id**.

```
[student@desktopX ~]$ ssh-copy-id root@desktopY
```

Al copiar la clave en otro sistema mediante **ssh-copy-id**, este copiará el archivo `~/.ssh/id_rsa.pub` de forma predeterminada.

Demostración de claves SSH

- Utilice **ssh-keygen** para crear un par de claves públicas y privadas.

```
[student@desktopX ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa): Enter
Created directory '/home/student/.ssh'.
Enter passphrase (empty for no passphrase): redhat
Enter same passphrase again: redhat
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
The key fingerprint is:
a4:49:cf:fb:ac:ab:c8:ce:45:33:f2:ad:69:7b:d2:5a student@desktopX.example.com
The key's randomart image is:
+--[ RSA 2048]----+
| |
| |
| . .
| . *
| . * S
| + + .
| o.E
| o oo+oo
| .=**ooo
+-----+
```

- Utilice **ssh-copy-id** para copiar la clave pública en la ubicación correcta en un sistema remoto. Por ejemplo:

```
[student@desktopX ~]$ ssh-copy-id -i ~/.ssh/id_rsa.pub root@serverX.example.com
```

Referencias

Es posible encontrar información adicional en el capítulo sobre el uso de autenticación mediante claves en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en <https://access.redhat.com/documentation/>

Páginas del manual: **ssh-keygen(1)**, **ssh-copy-id(1)**, **ssh-agent(1)**, **ssh-add(1)**

Práctica: Uso de la autenticación mediante claves SSH

En este ejercicio de laboratorio, configurará la autenticación mediante claves SSH.

Resultados:

Los estudiantes configurarán la autenticación mediante claves del usuario SSH a fin de iniciar conexiones SSH.

1. Cree un par de claves SSH como **student** en desktopX sin utilizar una frase de contraseña.

```
[student@desktopX ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa): Enter
Created directory '/home/student/.ssh'.
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
...
```

2. Envíe la clave pública de SSH a la cuenta **student** de serverX.

```
[student@desktopX ~]$ ssh-copy-id serverX
The authenticity of host 'serverX (172.25.X.11)' can't be established.
ECDSA key fingerprint is 33:fa:a1:3c:98:30:ff:f6:d4:99:00:4e:7f:84:3e:c3.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out
any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted
now it is to install the new keys
student@serverX's password: student

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'student@serverX'"
and check to make sure that only the key(s) you wanted were added.
```

3. Ejecute el comando **hostname** con **ssh** para visualizar el nombre del host de la máquina serverX.example.com sin necesidad de ingresar una contraseña.

```
[student@desktopX ~]$ ssh serverX 'hostname'
serverX.example.com
```

Personalización de la configuración del servicio SSH

Objetivo

Tras finalizar esta sección, los estudiantes deberían poder personalizar la configuración de sshd para restringir los inicios de sesión directos como root o para inhabilitar la autenticación con contraseña.

Archivo de configuración del servidor OpenSSH

Si bien la configuración del servidor OpenSSH no suele requerir modificación, hay medidas adicionales de seguridad disponibles.

Pueden modificarse varios aspectos del servidor OpenSSH en el archivo de configuración `/etc/ssh/sshd_config`.

Prohibir al usuario root el inicio de sesión con SSH

Desde el punto de vista de la seguridad, es aconsejable prohibir al usuario root que inicie sesión en el sistema en forma directa con `ssh`.

- El nombre de usuario root existe en cada sistema Linux de manera predeterminada; por lo tanto, un posible atacante solo tiene que adivinar la contraseña en lugar de la combinación de nombre de usuario y contraseña válidos.
- El usuario root tiene privilegios sin restricciones.

El servidor OpenSSH tiene un parámetro de archivo de configuración interno para prohibir el inicio de sesión en el sistema como usuario root, que es comentado de manera predeterminada en el archivo `/etc/ssh/sshd_config`:

```
#PermitRootLogin yes
```

Si se habilita la opción anterior en el archivo de configuración `/etc/ssh/sshd_config` de la siguiente manera, el usuario root no podrá iniciar sesión en el sistema con el comando `ssh` después de que se haya reiniciado el servicio sshd:

```
PermitRootLogin no
```

El servicio sshd tiene que reiniciarse para que puedan implementarse los cambios:

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

Otra opción es solo permitir el inicio de sesión en ssh con clave como root con:

```
PermitRootLogin without-password
```

Prohibir la autenticación de contraseña con SSH

El solo hecho de permitir el inicio de sesión mediante clave a la línea de comando remota tiene varias ventajas:

- Las claves SSH son más extensas que una contraseña estándar y este detalle aporta seguridad.
- El inicio del acceso a la shell remota implica menos esfuerzo después de la configuración inicial.

Existe una opción en el archivo de configuración **/etc/ssh/sshd_config** que activa una autenticación por contraseña de manera predeterminada:

```
PasswordAuthentication yes
```

Para evitar la autenticación de contraseña, la opción **PasswordAuthentication** tiene que configurarse en **no** y es necesario reiniciar el servicio sshd:

```
PasswordAuthentication no
```

Recuerde que cada vez que cambie el archivo **/etc/ssh/sshd_config**, debe reiniciarse el servicio sshd:

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



Referencias

Páginas del manual: **ssh(1)**, **sshd_config(5)**

Práctica: Restricción de inicios de sesión en SSH

En este ejercicio de laboratorio, habilitará características de seguridad adicionales en OpenSSH.

Resultados:

Prohibe el inicio de sesión directo por medio de SSH como usuario root en serverX. Prohibe que los usuarios empleen contraseñas para iniciar sesión en serverX a través de SSH. Los usuarios regulares deben seguir teniendo permiso para realizar la autenticación mediante clave pública.

Andes de comenzar

Restablezca los sistemas desktopX y serverX.

Ejecute **lab ssh setup** tanto en desktopX como en serverX. Esta acción creará una cuenta de usuario denominada **visitor** con la contraseña **password**.

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

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

1. Genere claves SSH en desktopX, copie la clave pública en la cuenta **student** en serverX y compruebe que las claves funcionen.
 - 1.1. Genere las claves SSH en desktopX.

```
[student@desktopX ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa): Enter
Created directory '/home/student/.ssh'.
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
...
```

- 1.2. Copie la clave pública SSH en la cuenta **student** en serverX.

```
[student@desktopX ~]$ ssh-copy-id serverX
The authenticity of host 'serverX (172.25.X.11)' can't be established.
ECDSA key fingerprint is 33:fa:a1:3c:98:30:ff:f6:d4:99:00:4e:7f:84:3e:c3.
Are you sure you want to continue connecting (yes/no)? yes

/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys
student@serverX's password: student

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'student@serverX'"
```

```
and check to make sure that only the key(s) you wanted were added.
```

- 1.3. Verifique que la autenticación mediante claves SSH funcione para el usuario student en serverX.

```
[student@desktopX ~]$ ssh student@serverX  
[student@serverX ~]$
```

2. Inicie sesión en la máquina serverX y obtenga privilegios de superusuario.

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

3. Configure SSH en serverX para impedir que el usuario root inicie sesión.

- 3.1. Como usuario root, edite **/etc/ssh/sshd_config** en serverX, de modo que la entrada "PermitRootLogin" no tenga comentarios y esté definida en "no".

```
PermitRootLogin no
```

- 3.2. Reinicie el servicio SSH en la máquina serverX.

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

- 3.3. Confirme que **root** no pueda iniciar sesión con SSH, pero que se permita que **student** inicie sesión.

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

4. Configure SSH en serverX para impedir la autenticación de contraseñas.

- 4.1. Edite el archivo de configuración **/etc/ssh/sshd_config** como usuario root para que la entrada "PasswordAuthentication" esté definida en "no":

```
PasswordAuthentication no
```

- 4.2. Reinicie el servicio SSH.

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

- 4.3. Confirme que **visitor** no pueda iniciar sesión utilizando una contraseña, pero que se permita que **student** inicie sesión utilizando las claves SSH que se crearon antes.

```
[student@desktopX ~]$ ssh visitor@serverX  
Permission denied (publickey, gssapi-keyex, gssapi-with-mic).  
[student@desktopX ~]$ ssh student@serverX  
[student@serverX ~]$
```

Ejercicio de laboratorio: Configuración y protección del servicio OpenSSH

En este ejercicio de laboratorio, agregará medidas de seguridad al servicio ssh.

Resultados:

Los estudiantes configurarán las claves de SSH, configurarán y permitirán en forma exclusiva la autenticación con clave del usuario, y bloquearán el servicio OpenSSH para evitar que el usuario root inicie sesión en el sistema con SSH.

Andes de comenzar

Restablezca los sistemas desktopX y serverX.

Ejecute **lab ssh setup** como el usuario **student** tanto en desktopX como en serverX. Esta acción creará una cuenta de usuario denominada **visitor** con la contraseña **password**.

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

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

A menos que se especifique, todos los pasos deben completarse como usuario **visitor**.

1. Genere las claves de SSH en desktopX para el usuario visitor y copie la clave pública en la cuenta **visitor** en serverX.
2. Inhabilite el inicio de sesión de ssh para el usuario root y la autenticación de SSH con contraseña en serverX.
3. Verifique que el usuario root no tenga permitido el inicio de sesión en serverX mediante el uso de ssh, mientras el usuario visitor está con la clave privada.

Solución

En este ejercicio de laboratorio, agregará medidas de seguridad al servicio ssh.

Resultados:

Los estudiantes configurarán las claves de SSH, configurarán y permitirán en forma exclusiva la autenticación con clave del usuario, y bloquearán el servicio OpenSSH para evitar que el usuario root inicie sesión en el sistema con SSH.

Andes de comenzar

Restablezca los sistemas desktopX y serverX.

Ejecute **lab ssh setup** como el usuario **student** tanto en desktopX como en serverX. Esta acción creará una cuenta de usuario denominada **visitor** con la contraseña **password**.

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

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

A menos que se especifique, todos los pasos deben completarse como usuario **visitor**.

1. Genere las claves de SSH en desktopX para el usuario visitor y copie la clave pública en la cuenta **visitor** en serverX.

- 1.1. Genere una clave pública de SSH en desktopX como usuario visitor.

```
[visitor@desktopX ~]$ ssh-keygen
```

- 1.2. Instale la clave pública de SSH (generada previamente en desktopX) en la cuenta **visitor** de serverX.

```
[visitor@desktopX ~]$ ssh-copy-id serverX
The authenticity of host 'serverX (172.25.X.11)' can't be established.
ECDSA 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
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys
visitor@serverX's password: password

Number of key(s) added: 1

Now try logging into the machine, with:    "ssh 'visitor@serverX'"
and check to make sure that only the key(s) you wanted were added.
```

2. Inhabilite el inicio de sesión de ssh para el usuario root y la autenticación de SSH con contraseña en serverX.

- 2.1. Inicie sesión en la máquina virtual serverX como usuario root.

```
[visitor@desktopX ~]$ ssh root@serverX
```

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

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

```
PermitRootLogin no  
PasswordAuthentication no
```

2.3. Reinicie el servicio sshd en serverX.

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

3. Verifique que el usuario root no tenga permitido el inicio de sesión en serverX mediante el uso de ssh, mientras el usuario visitor está con la clave privada.

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

```
[visitor@desktopX ~]$ ssh root@serverX  
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

3.2. Intente iniciar sesión como usuario student para serverX desde desktopX mediante ssh. Debería fallar porque no agregamos la clave pública desde ese usuario a la cuenta student en la máquina serverX.

```
[visitor@desktopX ~]$ ssh student@serverX  
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

3.3. Verifique que el servicio ssh todavía acepte la autenticación con clave mediante la conexión correcta a serverX como usuario visitor con el comando **ssh**.

```
[visitor@desktopX ~]$ ssh visitor@serverX  
[visitor@serverX ~]$
```

Resumen

Acceso a la línea de comandos remota con SSH

El servicio OpenSSH es el software estándar que permite acceder a la línea de comandos remota de manera segura.

Configuración de autenticación basada en llaves SSH

Con el uso de la autenticación mediante llaves SSH, la administración remota de sistemas obtiene seguridad adicional.

Personalización de la configuración del servicio SSH

La configuración del servicio OpenSSH, sshd, puede cambiarse mediante la edición del archivo /etc/ssh/sshd_config y el reinicio del servicio con systemctl.



CAPÍTULO 10

ANÁLISIS Y ALMACENAMIENTO DE REGISTROS

Visión general:	
Meta	Ubicar e interpretar correctamente archivos de registro del sistema relevantes para la solución de problemas.
Objetivos	<ul style="list-style-type: none">Describir la arquitectura básica syslog en Red Hat Enterprise Linux 7.Interpretar entradas en archivos syslog relevantes para la solución de problemas o revisar el estado del sistema.Buscar e interpretar entradas en el journal de systemd para solucionar problemas o revisar el estado del sistema.Configurar systemd-journald para almacenar el diario en disco en lugar de almacenarlo en memoria.Mantener una sincronización de tiempos y configuración de zona horaria precisas para garantizar sellos de tiempo correctos en los registros del sistema.
Secciones	<ul style="list-style-type: none">Arquitectura de registro de sistema (y práctica)Revisión de archivos Syslog (y práctica)Revisión de entradas del Journal de systemd (y práctica)Conservación del Journal de systemd (y práctica)Mantenimiento de tiempo exacto (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">Análisis y almacenamiento de registros

Arquitectura de registro del sistema

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder describir la arquitectura básica de syslog en Red Hat Enterprise Linux 7.

Inicio de sesión del sistema

Los procesos y el kernel del sistema operativo deben poder llevar un registro de los eventos que suceden. Estos registros pueden ser útiles para realizar una auditoría del sistema y solucionar problemas. Por convención, se almacenan de forma persistente en el directorio **/var/log**.

Red Hat Enterprise Linux incluye un sistema de registro estándar que se basa en el protocolo Syslog. Muchos programas utilizan este sistema para registrar eventos y organizarlos en archivos de registro. En Red Hat Enterprise Linux 7, hay dos servicios que se encargan de los mensajes de syslog: **systemd-journald** y **rsyslog**.

El demonio **systemd-journald** proporciona un servicio de administración de registros mejorado que recopila mensajes del kernel, las primeras etapas del proceso de arranque, la salida estándar y los errores de demonios a medida que se inician y ejecutan, y syslog. Escribe estos mensajes en un diario estructurado de eventos que, de manera predeterminada, no se conserva entre un reinicio y otro. Esto permite recopilar en una base de datos central los mensajes de syslog y los eventos que syslog omite. Los mensajes de syslog son reenviados de **systemd-journald** a **rsyslog** para su posterior procesamiento.

El servicio **rsyslog** luego ordena los mensajes de syslog por tipo (o utilidad) y prioridad, y los escribe en archivos persistentes en el directorio **/var/log**.

El directorio **/var/log** contiene diversos archivos específicos de sistemas y de servicios que mantiene **rsyslog**:

Generalidades de los archivos de registro del sistema

Archivo de registro	Propósito
/var/log/messages	La mayoría de los mensajes de syslog se registran aquí. Las excepciones son mensajes relacionados con tareas de autenticación y procesamiento de correos electrónicos, que realizan periódicamente trabajos, y aquellos relacionados exclusivamente con tareas de depuración.
/var/log/secure	El archivo de registro para errores y mensajes relacionados con seguridad y autenticación.
/var/log/maillog	El archivo de registro con mensajes relacionados con el servidor de correo.
/var/log/cron	El archivo de registro relacionado con tareas ejecutadas en forma periódica.
/var/log/boot.log	Los mensajes relacionados con el arranque del sistema se registran aquí.



Referencias

Páginas del manual: **systemd-journald.service(8)**, **rsyslogd(8)**,
rsyslog.conf(5)

Es posible encontrar información adicional en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en
| <https://access.redhat.com/documentation/>

Práctica: Componentes de registro de sistema

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

/var/log	/var/log/boot.log	/var/log/cron	/var/log/maillog
/var/log/messages	/var/log/secure		

Propósito	Archivo de registro
La mayoría de los mensajes de syslog se registran aquí. Las excepciones son mensajes relacionados con tareas de autenticación, procesamiento de correos electrónicos, trabajos realizados periódicamente o aquellos relacionados exclusivamente con tareas de depuración.	
El archivo de registro para errores y mensajes relacionados con seguridad y autenticación.	
El directorio en que rsyslog escribe todos los archivos de registro.	
El archivo de registro con mensajes relacionados con el servidor de correo.	
El archivo de registro relacionado con tareas ejecutadas en forma periódica.	

Propósito	Archivo de registro
Los mensajes relacionados con el arranque del sistema se registran aquí.	

Solución

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

Propósito	Archivo de registro
La mayoría de los mensajes de syslog se registran aquí. Las excepciones son mensajes relacionados con tareas de autenticación, procesamiento de correos electrónicos, trabajos realizados periódicamente o aquellos relacionados exclusivamente con tareas de depuración.	/var/log/messages
El archivo de registro para errores y mensajes relacionados con seguridad y autenticación.	/var/log/secure
El directorio en que rsyslog escribe todos los archivos de registro.	/var/log
El archivo de registro con mensajes relacionados con el servidor de correo.	/var/log/maillog
El archivo de registro relacionado con tareas ejecutadas en forma periódica.	/var/log/cron
Los mensajes relacionados con el arranque del sistema se registran aquí.	/var/log/boot.log

Revisión de archivos Syslog

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder interpretar las entradas en los archivos syslog correspondientes para solucionar problemas o revisar el estado del sistema.

Archivos syslog

Muchos programas usan el protocolo *syslog* para registrar eventos en el sistema. Cada mensaje se clasifica por instalación (tipo de mensaje) y prioridad (gravedad del mensaje). Las instalaciones disponibles se documentan en la página del manual **rsyslog.conf(5)**.

Las ocho prioridades también se estandarizan y clasifican de la siguiente manera:

Descripción general de las prioridades de syslog

Código	Prioridad	Gravedad
0	emerg	El sistema no se puede usar.
1	alert	Se debe implementar una acción de inmediato.
2	crit	Condición crítica.
3	err	Condición de error no crítica.
4	warning	Condición de advertencia.
5	notice	Evento normal pero importante.
6	info	Evento informativo.
7	debug	Mensaje de nivel de depuración.

El servicio rsyslogd usa la instalación y la prioridad de los mensajes de registro para determinar cómo resolverlos. Esto se configura mediante el archivo **/etc/rsyslog.conf** y los archivos ***.conf** en **/etc/rsyslog.d**. Los programas y los administradores pueden cambiar la configuración de **rsyslogd**, de tal manera que no pueda sobrescribirse con las actualizaciones de **rsyslog** mediante la inclusión de archivos personalizados que tienen el sufijo **.conf** en el directorio **/etc/rsyslog.d**.

En la sección **##### RULES #####** de **/etc/rsyslog.conf**, se incluyen directivas que definen dónde se almacenan los mensajes de registro. En el lado izquierdo de cada línea, se indican la instalación y la gravedad del mensaje de registro que se corresponde con la directiva. El archivo rsyslog.conf puede contener el carácter ***** como comodín en los campos de instalación y gravedad, donde es válido para todas las instalaciones o todas las gravedades. En el lado derecho de cada línea, se indica en qué archivo se debe guardar el mensaje de registro. Generalmente, los mensajes de registro se guardan en archivos ubicados en el directorio **/var/log**.



nota

Los archivos de registro se conservan mediante el servicio **rsyslog**, y el directorio **/var/log** contiene una variedad de archivos de registro específicos para determinados servicios. Por ejemplo, el servidor web Apache o Samba generan sus propios archivos de registro en el subdirectorio correspondiente del directorio **/var/log**.

Un mensaje manejado por **rsyslog** puede aparecer en varios archivos de registro diferentes. Para evitar eso, el campo de gravedad puede configurarse como **none**, lo que significa que ninguno de los mensajes dirigidos hacia esta instalación se agregan al archivo de registro especificado.

En lugar de registrar mensajes de syslog en un archivo, pueden imprimirse en las terminales de todos los usuarios que hayan iniciado sesión. En el archivo **rsyslog.conf** predeterminado, esto se hace para todos los mensajes que tienen la prioridad "emerg".

Sección de reglas de muestra de **rsyslog.conf**

```
##### RULES #####
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                     /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none      /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                    /var/log/secure

# Log all the mail messages in one place.
mail.*                                         -/var/log/maillog

# Log cron stuff
cron.*                                         /var/log/cron

# Everybody gets emergency messages
*.emerg                                         :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                  /var/log/spooler

# Save boot messages also to boot.log
local7.*                                         /var/log/boot.log
```



nota

El archivo **rsyslog.conf** está documentado en la página del manual **rsyslog.conf(5)** y en la amplia documentación HTML de **/usr/share/doc/rsyslog-*/manual.html** que está en el *rsyslog-doc*, que está disponible en el canal de software de Red Hat Enterprise Linux 7, pero no está incluido en el medio de instalación.

Rotación del archivo de registro

Los registros se "rotan" mediante la utilidad **logrotate** para evitar que llenen el sistema de archivos que contiene **/var/log/**. Cuando se rota un archivo de registro, se le cambia el nombre con una extensión que indica la fecha en que se rotó: el archivo **/var/log/messages** anterior puede pasar a ser **/var/log/messages-20141030** si se rota el 30 de octubre de 2014. Una vez que se rotó el archivo de registro anterior, se crea un nuevo archivo de registro y se notifica al servicio que escribe en este.

Después de una determinada cantidad de rotaciones, habitualmente después de cuatro semanas, el archivo de registro anterior se descarta para liberar espacio en disco. Una tarea de cron ejecuta el programa de rotación de archivos de registros a diario para verificar si es necesario rotar algún registro. La mayoría de los archivos de registro se rotan semanalmente, pero el programa de rotación de archivos de registros rota algunos más rápido o más lento, o cuando alcanzan un tamaño determinado.

La configuración de logrotate no se aborda en este curso. Si desea obtener más información, consulte la página del manual **logrotate(8)**.

Análisis de una entrada de syslog

Los registros del sistema escritos por **rsyslog** comienzan con el mensaje más antiguo en la parte superior y el mensaje más nuevo al final del archivo de registro. Todas las entradas en los archivos de registro administrados por **rsyslog** se graban en formato estándar. El siguiente ejemplo explicará la anatomía de un mensaje de archivo de registro en el archivo de registro **/var/log/secure**:

```
①Feb 11 20:11:48 ②localhost ③sshd[1433]: ④Failed password for student from
172.25.0.10 port 59344 ssh2
```

- ① La marca de tiempo cuando se grabó la entrada de registro.
- ② El host desde donde se envió el mensaje de registro.
- ③ El programa o el proceso que envió el mensaje de registro.
- ④ El mensaje real enviado.

Monitoreo de un archivo de registro con tail

Para reproducir problemas e inconvenientes, puede ser especialmente útil controlar uno o más archivos de registro para eventos. El comando **tail -f /path/to/file** proporciona las últimas 10 líneas del archivo especificado y continúa ofreciendo líneas nuevas a medida que se escriben en el archivo monitoreado.

Capítulo 10. Análisis y almacenamiento de registros

Para monitorear los intentos de inicio de sesión fallidos en un terminal, ejecute **ssh** como usuario root mientras otro usuario intenta iniciar sesión en la máquina serverX:

```
[root@serverX ~]$ tail -f /var/log/secure
...
Feb 10 09:01:13 localhost sshd[2712]: Accepted password for root from 172.25.254.254
port 56801 ssh2
Feb 10 09:01:13 localhost sshd[2712]: pam_unix(sshd:session): session opened for user
root by (uid=0)
```

Envío de un mensaje de syslog con logger

El comando **logger** puede enviar mensajes al servicio **rsyslog**. De manera predeterminada, envía el mensaje al usuario de la instalación con el aviso de gravedad (**user.notice**), a menos que se especifique lo contrario con la opción **-p**. Es especialmente útil, probar los cambios en la configuración de **rsyslog**.

Para enviar un mensaje a **rsyslogd** que se graba en el archivo de registro **/var/log/boot.log**, ejecute lo siguiente:

```
[root:@serverX ~]$ logger -p local7.notice "Log entry created on serverx"
```

Referencias

Páginas del manual: **logger(1)**, **tail(1)**, **rsyslog.conf(5)** y **logrotate(8)**

rsyslog Manual

- **/usr/share/doc/rsyslog-*/*manual.html** provisto por el paquete *rsyslog-doc*

Es posible encontrar información adicional en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Práctica: Encontrar entradas de registro

En este ejercicio de laboratorio, volverá a configurar **rsyslog** para escribir mensajes específicos en un archivo de registro nuevo.

Resultados:

El servicio **rsyslog** escribe todos los mensajes con depuración de prioridad en el archivo de registro **/var/log/messages-debug** con fines de solución de problemas temporales.

1. Configure **rsyslog** en serverX para registrar todos los mensajes con depuración de gravedad, o superiores, para cualquier servicio en un archivo de registro **/var/log/messages-debug** creado recientemente mediante el agregado del archivo de configuración **rsyslog /etc/rsyslog.d/debug.conf**. Verifique que el mensaje de registro de depuración generado con el comando **logger** llegue en el archivo de registro **/var/log/messages-debug**.
 - 1.1. Cambie la configuración de **rsyslog** para registrar todos los mensajes con la depuración de gravedad para **/var/log/messages-debug** en serverX mediante el agregado del archivo **/etc/rsyslog.d/debug.conf**.

```
[root@serverX ~]# echo "*.*.debug /var/log/messages-debug" >/etc/rsyslog.d/debug.conf
```

- 1.2. Reinicie el servicio rsyslog en serverX.

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

2. Genere un mensaje de registro de depuración con el comando **logger** y verifique que el mensaje se registre en el archivo de registro **/var/log/messages-debug** con el comando **tail** en serverX.

- 2.1. Monitoree el archivo **/var/log/messages-debug** con el comando **tail** en serverX.

```
[root@serverX ~]# tail -f /var/log/messages-debug
```

- 2.2. En otra ventana de terminal, use el comando **logger** para generar un mensaje de depuración en serverX.

```
[root@serverX ~]# logger -p user.debug "Debug Message Test"
```

- 2.3. Regrese al terminal que todavía está ejecutando el comando **tail -f /var/log/messages-debug** y verifique el mensaje enviado cuando aparezca el comando **logger**.

```
[root@serverX ~]# tail -f /var/log/messages-debug  
...
```

Capítulo 10. Análisis y almacenamiento de registros

```
Feb 13 10:37:44 localhost root: Debug Message Test
```

Revisión de las entradas del journal de systemd

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder encontrar e interpretar las entradas de registro en el journal de systemd para solucionar problemas o revisar el estado del sistema.

Cómo encontrar eventos con `journalctl`

El journal de systemd almacena datos de registro en un archivo binario estructurado e indicado. Estos datos incluyen información adicional sobre el evento de registro. En el caso de los eventos de syslog, esto puede incluir, por ejemplo, el recurso y la prioridad del mensaje original.



Importante

En Red Hat Enterprise Linux 7, el diario de systemd se almacena en `/run/log` de manera predeterminada, y sus contenidos se borran después del reinicio. Esta configuración puede ser modificada por el administrador del sistema y se analiza en otra parte de este curso.

El comando `journalctl` muestra el journal del sistema completo que comienza con la entrada de registro más antigua, cuando se ejecuta como usuario root:

```
[root@serverX ~]# journalctl
Feb 13 10:01:01 server1 run-parts(/etc/cron.hourly)[8678]: starting 0yum-hourly.cron
Feb 13 10:01:01 server1 run-parts(/etc/cron.hourly)[8682]: finished 0yum-hourly.cron
Feb 13 10:10:01 server1 systemd[1]: Starting Session 725 of user root.
Feb 13 10:10:01 server1 systemd[1]: Started Session 725 of user root.
Feb 13 10:10:01 server1 CROND[8687]: (root) CMD (/usr/lib64/sa/sa1 1 1)
```

El comando `journalctl` resalta en negrita los mensajes de texto con aviso o advertencia de prioridad, y los mensajes con error de prioridad y superiores se resaltan en rojo.

La clave para usar en forma correcta el journal para la solución de problemas y auditorías es limitar las búsquedas en el journal para mostrar solo el resultado relevante. En los siguientes párrafos, se presentarán varias estrategias diferentes para restringir el resultado de consultas del journal.

De manera predeterminada, `journalctl -n` muestra las 10 últimas entradas de registro. Se necesita un parámetro opcional para la cantidad de las últimas entradas de registro que se deben mostrar. Para mostrar las últimas 5 entradas de registro, ejecute:

```
[root@serverX ~]# journalctl -n 5
```

Al solucionar problemas, puede ser práctico filtrar el resultado del journal por prioridad de las entradas del diario. El comando `journalctl -p` usa el nombre o el número de los niveles de prioridad conocidos y muestra los niveles indicados y todas las entradas de nivel

Capítulo 10. Análisis y almacenamiento de registros

más alto. Los niveles de prioridad conocidos para **journalctl** son depuración, información, aviso, advertencia, error, gravedad, alerta y emergencia.

Para filtrar el resultado del comando **journalctl** a fin de que solo enumere cualquier entrada de registro de error de prioridad o superior, ejecute:

```
[root@serverX ~]# journalctl -p err
```

Al igual que el comando **tail -f, journalctl -f** ofrece las últimas 10 líneas del journal y continúa proporcionando las entradas del journal nuevas a medida que se escriben en el journal.

```
[root@serverX ~]# journalctl -f
```

Cuando se buscan eventos específicos, puede ser útil limitar el resultado a un lapso de tiempo específico. El comando **journalctl** tiene dos opciones para limitar el resultado a un intervalo de tiempo determinado, las opciones **--since** y **--until**. Ambas opciones toman un parámetro de tiempo con el formato **YYYY-MM-DD hh:mm:ss**. Si se omite la fecha, el comando asume que la fecha es hoy y si no se indica la parte de la hora, se asume que el día completo comienza a las 00:00:00. Ambas opciones consideran **yesterday, today** y **tomorrow** como parámetros válidos, además del campo de fecha y hora.

Proporciona todas las entradas del journal que se registraron hoy:

```
[root@serverX ~]# journalctl --since today
```

Proporciona las entradas del journal desde el 10 de febrero de 2014 a las 20:30:00 hasta el 13 de febrero de 2014 a las 12:00:00:

```
[root@serverX ~]# journalctl --since "2014-02-10 20:30:00" --until "2014-02-13 12:00:00"
```

Además del contenido visible del journal, existen campos adjuntos a las entradas del registro que solo pueden verse cuando se activa el resultado de explicación extensa. Para filtrar el resultado de una consulta del journal, pueden usarse todos los campos adicionales que se muestran. Esto es útil para restringir el resultado de búsquedas complejas para determinados eventos del journal.

```
[root@serverX ~]# journalctl -o verbose
Thu 2014-02-13 02:06:00.409345 EST [s=0b47abbff995149c191a8e539e18c3f9c;
i=d28;b=1ea26e84667848af9a4a2904a76ff9a5;m=4d6878ff5a;t=4f244525daa67;
x=880bc65783036719]
_PRIOORITY=6
_UID=0
_GID=0
_BOOT_ID=1ea26e84667848af9a4a2904a76ff9a5
_MACHINE_ID=4513ad59a3b442ffa4b7ea88343fa55f
_CAP_EFFECTIVE=0000001fffffffff
_TRANSPORT=syslog
_SYSLOG_FACILITY=10
_SYSLOG_IDENTIFIER=sshd
_COMM=sshd
_EXE=/usr/sbin/sshd
_SYSTEMD_CGROUP=/system.slice/sshd.service
_SYSTEMD_UNIT=sshd.service
```

```
_SELINUX_CONTEXT=system_u:system_r:sshd_t:s0-s0:c0.c1023
_HOSTNAME=serverX
_CMDLINE=sshd: root [priv]
SYSLOG_PID=6833
_PID=6833
MESSAGE=Failed password for root from 172.25.X.10 port 59371 ssh2
_SOURCE_REALTIME_TIMESTAMP=1392275160409345
```

Entre las opciones más prácticas para buscar líneas que sean relevantes para un proceso o evento especial están:

- `_COMM`, el nombre del comando
- `_EXE`, la ruta hacia el ejecutable para el proceso
- `_PID`, la PID del proceso
- `_UID`, la UID del usuario que ejecuta el proceso
- `_SYSTEMD_UNIT`, la unidad systemd que inició el proceso

Puede combinarse más de una de estas opciones. Por ejemplo, la siguiente consulta muestra las entradas del journal relacionadas con los procesos que fueron iniciados por el archivo de unidad de systemd, `sshd.service`, que también tiene el PID 1182:

```
[root@serverX ~]# journalctl _SYSTEMD_UNIT=sshd.service _PID=1182
```



nota

Para obtener una lista de los campos más usados del journal, consulte la página del manual `systemd.journal-fields(7)`.



Referencias

Páginas del manual: (1) y `systemd.journal-fields (7)`**journalctl**

Es posible encontrar información adicional en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en
<https://access.redhat.com/documentation/>

Práctica: búsqueda de eventos con journalctl

En este ejercicio de laboratorio, filtrará el journal de systemd según criterios específicos.

Resultados:

Los estudiantes practicarán visualizar la salida del journal de **systemd** de manera que coincida con diferentes criterios.

1. Obtener la salida de solo los mensajes del journal **systemd** que se originan en el proceso **systemd** que se ejecuta siempre con la identificación de proceso 1 en serverX.

```
[root@serverX ~]# journalctl _PID=1
```

2. Visualice todos los mensajes del journal **systemd** que se originan en un servicio del sistema iniciado con una identificación de usuario 81 en serverX.

```
[root@serverX ~]# journalctl _UID=81
```

3. Obtener los mensajes del journal con prioridad **warning** y de nivel superior en serverX.

```
[root@serverX ~]# journalctl -p warning
```

4. Cree una consulta **journalctl** para mostrar todos los eventos de registro registrados en los 10 minutos anteriores en serverX. El comando asume una hora actual de 9:15:00.

```
[root@serverX ~]# journalctl --since 9:05:00 --until 9:15:00
```

5. Visualice solo los eventos que se originan en el servicio **sshd** con el archivo de unidad del sistema **sshd.service** registrado desde las 9:00:00 de esta mañana en serverX.

```
[root@serverX ~]# journalctl --since 9:00:00 _SYSTEMD_UNIT="sshd.service"
```

Preservando el journal de systemd

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder configurar **systemd-journald** para que almacene el diario en el disco y no en la memoria.

Almacenar el journal del sistema de manera permanente.

De manera predeterminada, el journal de systemd se conserva en **/run/log/journal**, lo que significa que se borra cuando se reinicia el sistema. El journal es un mecanismo nuevo en Red Hat Enterprise Linux 7, y para la mayoría de las instalaciones, basta con un journal detallado que comienza con el último inicio.

Si el directorio **/var/log/journal** existe, el journal se registrará, en cambio, en ese directorio. La ventaja es que los datos históricos estarán disponibles de inmediato en el inicio. Sin embargo, incluso cuando el journal sea persistente, no todos los datos se conservarán para siempre. El journal tiene un mecanismo de rotación de registro incorporado que se activará mensualmente. Además, de manera predeterminada, el journal no podrá tener más del 10 % del sistema de archivos en el que está ubicado ni dejar menos del 15 % del sistema de archivos libre. Estos valores pueden ajustarse en **/etc/systemd/journald.conf**, y los límites actuales del tamaño del journal se registran cuando comienza el proceso **systemd-journald**, como puede verse con el siguiente comando, que muestra las dos primeras líneas de la salida de **journalctl**:

```
[root@serverX ~]# journalctl | head -2
-- Logs begin at Wed 2014-03-05 15:13:37 CST, end at Thu 2014-03-06 21:57:54 CST. --
Mar 05 15:13:37 serverX.example.com systemd-journal[94]: Runtime journal is using 8.0M
(max 277.8M, leaving 416.7M of free 2.7G, current limit 277.8M).
```

El journal de systemd puede hacerse persistente si se crea el directorio **/var/log/journal** como usuario raíz:

```
[root@serverX ~]# mkdir /var/log/journal
```

Asegúrese de que el directorio **/var/log/journal** sea propiedad del usuario raíz y del grupo **systemd-journal**, y que tenga los permisos 2755.

```
[root@serverX ~]# chown root:systemd-journal /var/log/journal
[root@serverX ~]# chmod 2755 /var/log/journal
```

Es necesario que se reinicie el sistema o que se envíe la señal especial **USR1** como usuario root al proceso **systemd-journald**.

```
[root@serverX ~]# killall -USR1 systemd-journald
```

Puesto que el journal de systemd ahora es persistente en todos los reinicios, **journalctl -b** puede reducir la salida si solo muestra los mensajes de registros desde el último inicio del sistema.

```
[root@serverX ~]# journalctl -b
```



nota

Cuando se depura el bloqueo de un sistema con un journal constante, generalmente es necesario limitar la cola del journal al reinicio anterior al bloqueo. La opción **-b** puede estar acompañada por un número negativo que indica la cantidad de arranques anteriores del sistema a la que debe limitarse la salida. Por ejemplo, **journalctl -b -1** limita la salida al inicio anterior.



Referencias

Páginas del manual: **mkdir(1)**, **systemd-journald(1)**, **killall(1)**

Es posible encontrar información adicional en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en
<https://access.redhat.com/documentation/>

Práctica: Configuración del journal de systemd constante

En este ejercicio de laboratorio, los estudiantes usarán el journal de systemd constante.

Resultados:

El journal de **systemd** se escribe en el disco.

- Configure el journal de systemd para que sea constante en todos los reinicios.

- Configure el directorio **/var/log/journal** en serverX.

```
[root@serverX ~]# mkdir /var/log/journal  
[root@serverX ~]# chown root:systemd-journal /var/log/journal  
[root@serverX ~]# chmod 2755 /var/log/journal
```

- Envíe la señal **USR1** al **systemd-journald** o reinicie serverX.

```
[root@serverX ~]# killall -USR1 systemd-journald
```

- Para verificar que el journal de systemd sea constante, busque un directorio nuevo con los archivos de registro del journal de systemd que se escribieron en **/var/log/journal**. (Los archivos exactos que aparecen pueden variar en el sistema, pero el directorio debe tener contenidos similares al siguiente ejemplo).

```
[root@serverX ~]# ls /var/log/journal/4513ad59a3b442ffa4b7ea88343fa55f  
system.journal      user-1000.journal
```

Mantenimiento de la hora correcta

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder conservar la sincronización precisa de la hora y la configuración de la zona horaria para garantizar que las marcas de tiempo sean correctas en los registros del sistema.

Configure los relojes y la zona horaria local.

La hora correcta del sistema sincronizado es muy importante para el análisis del archivo de registro en varios sistemas. El *Protocolo de tiempo en red (NTP)* es una manera estándar para que las máquinas proporcionen y obtengan la información de la hora correcta de Internet. Una máquina puede obtener información de la hora correcta de los servicios NTP públicos en Internet, como el NTP Pool Project. Otra opción es un reloj de hardware de alta calidad para proporcionar la hora precisa a los clientes locales.

El comando **timedatectl** muestra una descripción general de los parámetros de configuración relacionados con la hora, que incluyen la hora actual, la zona horaria y los parámetros de configuración de sincronización de NTP del sistema.

```
[student@serverX ~]$ timedatectl
  Local time: Thu 2014-02-13 02:16:15 EST
  Universal time: Thu 2014-02-13 07:16:15 UTC
    RTC time: Thu 2014-02-13 07:16:15
   Timezone: America/New_York (EST, -0500)
     NTP enabled: yes
    NTP synchronized: no
      RTC in local TZ: no
        DST active: no
    Last DST change: DST ended at
                      Sun 2013-11-03 01:59:59 EDT
                      Sun 2013-11-03 01:00:00 EST
  Next DST change: DST begins (the clock jumps one hour forward) at
                      Sun 2014-03-09 01:59:59 EST
                      Sun 2014-03-09 03:00:00 EDT
```

Está disponible una base de datos con las zonas horarias conocidas y puede enumerarse con:

```
[student@serverX ~]$ timedatectl list-timezones
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Bamako
...
```

Los nombres de las zonas horarias se basan en la base de datos de zonas horarias "tz" (o "zoneinfo") públicas que están a cargo de la Autoridad para la Asignación de Números de Internet (IANA). Las zonas horarias se nombran según el continente u océano; luego, por lo general, pero no siempre, la ciudad más grande dentro de la región de la zona horaria. Por ejemplo, la mayoría de la zona horaria de montaña de los EE. UU. se denomina "América/Denver".

La elección del nombre correcto puede ser no intuitiva en casos donde las localidades dentro de una zona horaria tienen normas horarias de aprovechamiento de la luz solar. Por ejemplo, en los EE. UU., gran parte del estado de Arizona (hora de la zona montañosa de los EE. UU.) no modifica la hora para aprovechar la luz solar y su huso horario es el de "América/Phoenix".

El comando **tzselect** es práctico para identificar los nombres de la zona horaria zoneinfo correcta. De manera interactiva, se le formulan preguntas al usuario sobre la ubicación del sistema y se proporciona el nombre de la zona horaria correcta. No implementa cambios en la configuración de la zona horaria del sistema.

La configuración del sistema para la zona horaria actual puede modificarse como usuario root:

```
[root@serverX ~]# timedatectl set-timezone America/Phoenix
[root@serverX ~]# timedatectl
    Local time: Thu 2014-02-13 00:23:54 MST
    Universal time: Thu 2014-02-13 07:23:54 UTC
        RTC time: Thu 2014-02-13 07:23:53
       Timezone: America/Phoenix (MST, -0700)
      NTP enabled: yes
    NTP synchronized: no
      RTC in local TZ: no
        DST active: n/a
```

Para cambiar los parámetros de configuración de fecha y hora actuales con el comando **timedatectl**, está disponible la opción **set-time**. La hora se especifica con el formato "DD-MM-AAA hh:mm:ss", donde se puede omitir la fecha o la hora. Para cambiar la hora a 09:00:00, ejecute:

```
[root@serverX ~]$ timedatectl set-time 9:00:00
[root@serverX ~]$ timedatectl
    Local time: Thu 2014-02-13 09:00:27 MST
    Universal time: Thu 2014-02-13 16:00:27 UTC
        RTC time: Thu 2014-02-13 16:00:28
       Timezone: America/Phoenix (MST, -0700)
      NTP enabled: yes
    NTP synchronized: no
      RTC in local TZ: no
        DST active: n/a
```

La opción **set-ntp** habilita o inhabilita la sincronización de NTP para el ajuste de hora automático. La opción requiere de un argumento **true** o **false** para activarla o desactivarla. Para activar la sincronización de NTP, ejecute:

```
[student@desktopX ~]$ timedatectl set-ntp true
```

Configuración y control de chronyd

El servicio **chronyd** se encarga de que el reloj de hardware local (RTC), que por lo general es impreciso, esté dentro de los parámetros establecidos mediante la sincronización con los servidores NTP configurados o, en caso de que no haya conectividad de red disponible, con la desviación del reloj de RTC calculada que se registra en el **driftfile** especificado en el archivo de configuración **/etc/chrony.conf**.

Capítulo 10. Análisis y almacenamiento de registros

De manera predeterminada, **chrony** usa servidores del NTP Pool Project para la sincronización del tiempo y no necesita otra configuración. Puede ser útil cambiar los servidores NTP cuando la máquina en cuestión esté en una red aislada.

La calidad de la fuente de la hora NTP está determinada por el valor del **estrato** informado por la fuente de la hora. El **estrato** determina la cantidad de saltos con que la máquina se aleja del reloj de referencia de alto rendimiento. El reloj de referencia es una fuente de hora de **estrato 0**. Un servidor NTP conectado en forma directa a dicho reloj es un **estrato 1**, mientras que una máquina que sincroniza la hora a partir de un servidor NTP es una fuente de hora **estrato 2**.

Existen dos categorías de fuentes de hora que pueden configurarse en el archivo de configuración **/etc/chrony.conf**, **server** y **peer**. El **server** se encuentra un estrato más arriba que el servidor NTP local y **peer** está en el mismo estrato. Puede especificarse más de un **server** y más de un **peer**, uno por línea.

El primer argumento de la línea **server** es la dirección IP o el nombre de DNS del servidor NTP. A continuación del nombre o de la dirección IP del servidor, puede especificarse una serie de opciones para el servidor. Se recomienda usar la opción **iburst** porque, una vez que se inicie el servicio, se realizarán cuatro mediciones en un período breve a fin de lograr una sincronización del reloj inicial más precisa.

Para volver a configurar el servidor **chrony** para sincronizarlo con `classroom.example.com`, en lugar de hacerlo con los servidores predeterminados configurados en **/etc/chrony.conf**, elimine las otras entradas de servidor y reemplácelas con la siguiente entrada del archivo de configuración:

```
# Use public servers from the pool.ntp.org project.
server classroom.example.com iburst
```

Después de orientar **chrony** hacia la fuente de hora local, `classroom.example.com`, es necesario reiniciar el servicio:

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

El comando **chronyc** actúa como cliente para el servicio **chrony**. Después de configurar la sincronización NTP, puede ser práctico verificar si el servidor NTP se usó para sincronizar el reloj del sistema. Esto puede lograrse con el comando **chronyc sources** o, para un resultado más extenso con explicaciones adicionales sobre el resultado, con el comando **chronyc sources -v**:

```
[root@serverX ~]$ chronyc sources -v
210 Number of sources = 1

-- Source mode '^' = server, '=' = peer, '#' = local clock.
/ -- Source state '*' = current synced, '+' = combined , '-' = not combined,
| / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.
||                               .- xxxx [ yyyy ] +/- zzzz
||                               / xxxx = adjusted offset,
||           Log2(Polling interval) -.          | yyyy = measured offset,
||                               \          | zzzz = estimated error.
||                               |
MS Name/IP address      Stratum Poll Reach LastRx Last sample
=====
```

```
^* classroom.example.com      8   6   17   23   -497ns[-7000ns] +/-  956us
```

El carácter * en el campo **S** (estado Source) indica que el servidor classroom.example.com se usó como fuente de hora y el servidor NTP es la máquina que se toma actualmente como referencia para la sincronización.



nota

Red Hat Enterprise Linux 6 y las versiones anteriores usan **ntpd** y **ntpq** para administrar la configuración de NTP. Puede encontrar más información en la documentación de Red Hat Enterprise Linux 6.



Referencias

Páginas del manual **timedatectl(1)**, **tzselect(8)**, **chronyd(8)**, **chrony.conf(5)** y **chronyc(1)**

Es posible encontrar información adicional en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en
<https://access.redhat.com/documentation/>

NTP Pool Project

<http://www.pool.ntp.org/>

Base de datos de zona horaria

<http://www.iana.org/time-zones>

Práctica: Ajuste de la hora del sistema

En este ejercicio de laboratorio, los estudiantes ajustarán la zona horaria en un sistema y sincronizarán el reloj de hardware con una fuente de hora de **NTP**.

Resultados

Los estudiantes configurarán el sistema serverX para usar la zona horaria correspondiente a Haití y configurarán **chrony** en serverX para usar el servidor **NTP** que se está ejecutando en classroom.example.com como fuente de hora.

1. Su máquina serverX ha sido reubicada en Haití. Cambie la zona horaria en la máquina serverX para que coincida con Haití y verifique que la zona horaria se haya modificado de forma adecuada.

1.1. Identifique la zona horaria correcta para Haití en serverX.

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

Therefore TZ='America/Port-au-Prince' will be used.
Local time is now: Thu Nov 20 11:07:46 EST 2014.
Universal Time is now: Thu Nov 20 16:07:46 UTC 2014.
Is the above information OK?
 1) Yes
 2) No
#? 1

You can make this change permanent for yourself by appending the line
TZ='America/Port-au-Prince'; export TZ
to the file '.profile' in your home directory; then log out and log in again.
```

```
Here is that TZ value again, this time on standard output so that you  
can use the /usr/bin/tzselect command in shell scripts:  
America/Port-au-Prince
```

1.2. Cambie la zona horaria a Estados Unidos/Port-au-Prince en serverX.

```
[root@serverX ~]# timedatectl set-timezone America/Port-au-Prince
```

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

```
[root@serverX ~]# timedatectl  
    Local time: Wed 2014-11-20 11:09:00 EST  
    Universal time: Wed 2014-11-20 16:09:00 UTC  
        RTC time: Wed 2014-11-20 16:09:00  
      Timezone: America/Port-au-Prince (EST, -0500)  
    NTP enabled: yes  
NTP synchronized: no  
   RTC in local TZ: no  
     DST active: no  
Last DST change: DST ended at  
                  Sun 2014-11-02 01:59:59 EDT  
                  Sun 2014-11-02 01:00:00 EST  
Next DST change: DST begins (the clock jumps one hour forward) at  
                  Sun 2015-03-08 01:59:59 EST  
                  Sun 2015-03-08 03:00:00 EDT
```

2. Habilite la sincronización de **NTP** en el sistema serverX y use classroom.example.com como fuente de hora.

2.1. Configure **chronyd** para sincronizar la hora en serverX con classroom.example.com. Edite **/etc/chrony.conf** para que se asemeje al siguiente extracto del archivo de configuración:

```
# Use public servers from the pool.ntp.org project.  
# Please consider joining the pool (http://www.pool.ntp.org/join.html).  
# server 0.rhel.pool.ntp.org iburst  
# server 1.rhel.pool.ntp.org iburst  
# server 2.rhel.pool.ntp.org iburst  
# server 3.rhel.pool.ntp.org iburst  
server classroom.example.com iburst  
...
```

2.2. Reinicie el servicio **chronyd** en serverX.

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

2.3. Active la sincronización de **NTP** en serverX si no está activada.

```
[root@serverX ~]# timedatectl set-ntp true
```

3. Verifique que el sistema serverX tenga su reloj sincronizado con classroom.example.com mediante el uso de **NTP**.

3.1. Verifique que el reloj de hardware en serverX se haya sincronizado con **NTP**.

```
[root@serverX ~]# timedatectl  
...  
NTP synchronized: yes  
...
```

- 3.2. Verifique que se utilice el sistema classroom.example.com como fuente de hora para sincronizar el reloj en serverX.

```
[root@serverX ~]# chronyc sources -v  
210 Number of sources = 1  
  
.-- Source mode '^' = server, '=' = peer, '#' = local clock.  
/- .- Source state '*' = current synced, '+' = combined , '-' = not combined,  
| / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  
|| | .- xxxx [ yyyy ] +/- zzzz  
|| | / xxxx = adjusted offset,  
|| | Log2(Polling interval) -- | yyyy = measured offset,  
|| | \ | zzzz = estimated error.  
||  
MS Name/IP address Stratum Poll Reach LastRx Last sample  
=====  
^* classroom.example.com 8 6 37 51 -25ns[-703us] +/- 128us
```

Ejercicio de laboratorio: Análisis y almacenamiento de registros

En este ejercicio de laboratorio, los estudiantes cambiarán la zona horaria y registrarán todos los registros de fallas de autenticación en un archivo aparte.

Resultados:

En serverX, se establece correctamente la zona horaria para Jamaica, se ejecuta un comando para mostrar todas las entradas del journal registradas en los últimos 30 minutos y se configura **rsyslog** para enviar todos los mensajes de instalación **authpriv** con **alert** o una prioridad superior a un nuevo archivo de registro, **/var/log/auth-errors**.

Antes de comenzar

Restablezca su sistema serverX.

1. Su máquina serverX ha sido reubicada en Jamaica. Cambie la zona horaria de la máquina serverX al horario de Jamaica y compruebe que el cambio se haya realizado correctamente.
2. Muestre todas las entradas del journal **systemd** registradas en los últimos 30 minutos en serverX.
3. Configure **rsyslogd** para que registre mensajes de syslog relacionados con problemas de autenticación y de seguridad que tengan prioridad alerta o superior para el archivo **/var/log/auth-errors**. Use el archivo **/etc/rsyslog.d/auth-errors.conf** para hacer esto; créelo si es necesario. Pruebe estos cambios mediante el comando **logger**.

Solución

En este ejercicio de laboratorio, los estudiantes cambiarán la zona horaria y registrarán todos los registros de fallas de autenticación en un archivo aparte.

Resultados:

En serverX, se establece correctamente la zona horaria para Jamaica, se ejecuta un comando para mostrar todas las entradas del journal registradas en los últimos 30 minutos y se configura **rsyslog** para enviar todos los mensajes de instalación **authpriv** con **alert** o una prioridad superior a un nuevo archivo de registro, **/var/log/auth-errors**.

Andes de comenzar

Restablezca su sistema serverX.

1. Su máquina serverX ha sido reubicada en Jamaica. Cambie la zona horaria de la máquina serverX al horario de Jamaica y compruebe que el cambio se haya realizado correctamente.

- 1.1. Identifique la zona horaria correcta de Jamaica en serverX.

```
[root@serverX ~]# timedatectl list-timezones
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
...
America/Jamaica
...
```

- 1.2. Cambie la zona horaria a Jamaica en serverX.

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

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

```
[root@serverX ~]# timedatectl
    Local time: Thu 2014-02-13 11:16:59 EST
    Universal time: Thu 2014-02-13 16:16:59 UTC
        RTC time: Thu 2014-02-13 16:17:00
       Timezone: America/Jamaica (EST, -0500)
      NTP enabled: yes
     NTP synchronized: no
      RTC in local TZ: no
        DST active: n/a
```

2. Muestre todas las entradas del journal **systemd** registradas en los últimos 30 minutos en serverX.

Suponiendo que la hora actual sea 9:30:00, se usará el siguiente comando

```
[root@serverX ~]# journalctl --since 9:00:00 --until 9:30:00
```

3. Configure **rsyslogd** para que registre mensajes de syslog relacionados con problemas de autenticación y de seguridad que tengan prioridad alerta o superior para el archivo **/var/log/auth-errors**. Use el archivo **/etc/rsyslog.d/auth-errors.conf** para hacer esto; créelo si es necesario. Pruebe estos cambios mediante el comando **logger**.

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

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

- 3.2. Reinicie el servicio **rsyslog** en serverX.

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

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

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

- 3.4. Compruebe que el mensaje enviado a syslog con el comando **logger** aparezca en el archivo **/var/log/auth-errors** de serverX en el terminal con **tail /var/log/auth-errors**.

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

Resumen

Arquitectura de registro del sistema

La arquitectura de registro consiste en **systemd-journald**, que recolecta mensajes de registro, y en **rsyslog**, que ordena y escribe mensajes de registro en archivos de registro.

Revisión de archivos Syslog

Los archivos de registro del sistema son mantenidos por **rsyslog**.

Revisión de las entradas del journal de systemd

El journal de systemd ofrece capacidades avanzadas para consultar eventos.

Preservando el journal de systemd

Configuración de **systemd-journald** para el almacenamiento permanente del diario en el disco.

Mantenimiento de la hora correcta

La sincronización de la hora es un aspecto importante para el análisis de archivos de registro.



CAPÍTULO 11

ADMINISTRACIÓN DE LA RED DE RED HAT ENTERPRISE LINUX

Descripción general	
Meta	Configurar la red IPv4 básica en los sistemas Red Hat Enterprise Linux.
Objetivos	<ul style="list-style-type: none">Explicar los conceptos fundamentales de la red de computadora.Realizar una prueba y revisar la configuración de red actual con las utilidades básicas.Administrar la configuración de la red y los dispositivos con <code>nmcli</code> y NetworkManager.Modificar la configuración de la red mediante la edición de los archivos de configuración.Configurar y probar el nombre del host del sistema y la resolución de nombre.
Secciones	<ul style="list-style-type: none">Conceptos de red (y práctica)Validación de la configuración de red (y práctica)Configuración de red con <code>nmcli</code> (y práctica)Edición de archivos de configuración de red (y práctica)Configuración de nombres de host y resolución de nombre (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">Administración de la red de Red Hat Enterprise Linux

Conceptos de red

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder explicar conceptos fundamentales de redes de computadoras.

Redes IPv4

Los estándares de TCP/IP siguen un modelo de red de cuatro capas que se especifica en RFC1122.

- **Aplicación**

Cada aplicación tiene especificaciones para que los clientes y los servidores puedan comunicarse en las plataformas. Entre los protocolos comunes se incluyen SSH (inicio de sesión remoto), HTTPS (web segura), NFS o CIFS (uso compartido de archivo) y SMTP (envío de correo electrónico).

- **Transporte**

Los protocolos de transporte son TCP y UDP. TCP es una comunicación confiable orientada a la conexión, mientras que UDP es un protocolo de *datagramas* sin conexión. Los protocolos de aplicaciones utilizan puertos TCP o UDP. En el archivo **/etc/services**, encontrará una lista de puertos conocidos y registrados.

Cuando un paquete se envía por la red, la combinación del puerto de servicio y la dirección IP forma un socket. Cada paquete tiene un socket de origen y un socket de destino. Esta información puede utilizarse al realizar tareas de monitoreo y filtrado.

- **Internet**

Internet, o capa de red, transporta datos desde el host de origen hasta el host de destino. Cada host tiene una dirección IP y un prefijo que se utiliza para determinar direcciones de red. Los enruteadores se utilizan para conectar redes.

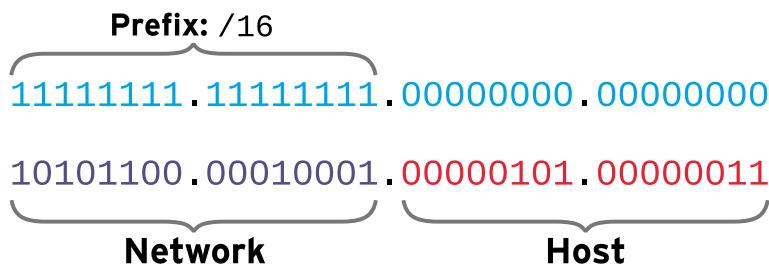
ICMP es un protocolo de control en esta capa. En lugar de puertos, tiene tipos. La utilidad **ping** es un ejemplo de paquetes ICMP para probar la conectividad. **ping** envía un paquete ICMP ECHO_REQUEST. Un **ping** exitoso recibe una confirmación ICMP ECHO_REPLY. Un **ping** no exitoso puede recibir mensajes de error ICMP, como "no se puede alcanzar el destino", o directamente puede no recibir ninguna respuesta.

- **Enlace**

La capa de enlace, o acceso a medios, proporciona la conexión a medios físicos. Los tipos de redes más comunes son Ethernet (802.3) cableada y WLAN (802.11) inalámbrica. Cada dispositivo físico tiene una dirección de hardware (MAC) que se utiliza para identificar el destino de paquetes en el segmento de red local.

IP Address:

$$172.17.5.3 = \textcolor{red}{10101100}.\textcolor{red}{00010001}.\textcolor{red}{00000101}.\textcolor{red}{00000011}$$
Netmask:

$$255.255.0.0 = \textcolor{blue}{11111111}.\textcolor{blue}{11111111}.\textcolor{blue}{00000000}.\textcolor{blue}{00000000}$$
**IP Address:**

$$192.168.5.3 = \textcolor{red}{11000000}.\textcolor{blue}{10101000}.\textcolor{red}{00000101}.\textcolor{red}{00000011}$$
Netmask:

$$255.255.255.0 = \textcolor{blue}{11111111}.\textcolor{blue}{11111111}.\textcolor{blue}{11111111}.\textcolor{blue}{00000000}$$


Figura 11.1: Máscaras de red y direcciones IPv4

Direcciones IPv4

Una dirección IPv4 es un numero de 32 bits, el cual generalmente se expresa en decimales en cuatro *octetos*, cuyo valor oscila entre 0 y 255, separados por puntos. La dirección se divide en dos partes: la *parte de la red* y la *parte del host*. Todos los hosts en la misma subred, que pueden comunicarse entre sí directamente sin un enrutador, cuentan con la misma parte de red; la parte de red identifica la subred. Dos hosts en la misma subred no pueden tener la misma parte de host; la parte del host identifica un host en particular en una subred.

En la Internet moderna, el tamaño de una subred IPv4 es variable. Para saber qué parte de una dirección IPv4 es la parte de red y cuál es la parte de host, un administrador debe conocer la *máscara de red* que se asignó a la subred. La máscara de red indica cuántos bits de la dirección IPv4 pertenecen a la subred. Cuantos más bits haya disponibles para la parte del host, más hosts habrá en la subred.

La dirección más baja posible en una subred (la parte de host son todos ceros en binario), algunas veces, se denomina *dirección de red*. La dirección más alta posible en una subred (la parte de host son todos los unos en binario) se utiliza para los mensajes de broadcast en IPv4 y se denomina *dirección de broadcast*.

Las máscaras de red se expresan de dos formas. La sintaxis más antigua de la máscara de red que utiliza 24 bits para la parte de red indicaría 255.255.255.0. Una sintaxis más nueva denominada notación CIDR, especificaría un *prefijo de red* de /24. Ambas formas transmiten la misma información; a saber, cuántos bits principales en la dirección IP contribuyen a la dirección de red.

Los siguientes ejemplos ilustran cómo se relacionan la dirección IP, el prefijo (máscara de red), la parte de red y la parte del host.

Cálculo de la dirección de red para 192.168.1.107/24

Dirección de host	192.168.1.107	11000000.10101000.00000001.01101011
Prefijo de red	/24 (255.255.255.0)	11111111.11111111.11111111.00000000
Dirección de red	192.168.1.0	11000000.10101000.00000001.00000000
Dirección de broadcast	192.168.1.255	11000000.10101000.00000001.11111111

Cálculo de la dirección de red para 10.1.1.18/8

Dirección de host	10.1.1.18	00001010.00000001.00000001.00010010
Prefijo de red	/8 (255.0.0.0)	11111111.00000000.00000000.00000000
Dirección de red	10.0.0.0	00001010.00000000.00000000.00000000
Dirección de broadcast	10.255.255.255	00001010.11111111.11111111.11111111

Cálculo de la dirección de red para 172.16.181.23/19

Dirección de host	172.168.181.23	10101100.10101000.10110101.00010111
Prefijo de red	/19 (255.255.224.0)	11111111.11111111.11100000.00000000
Dirección de red	172.168.160.0	10101100.10101000.10100000.00000000
Dirección de broadcast	172.168.191.255	10101100.10101000.10111111.11111111

La dirección especial 127.0.0.1 siempre apunta al sistema local ("localhost") y la red 127.0.0.0/8 pertenece al sistema local, para que pueda comunicarse con ella misma usando protocolos de red.

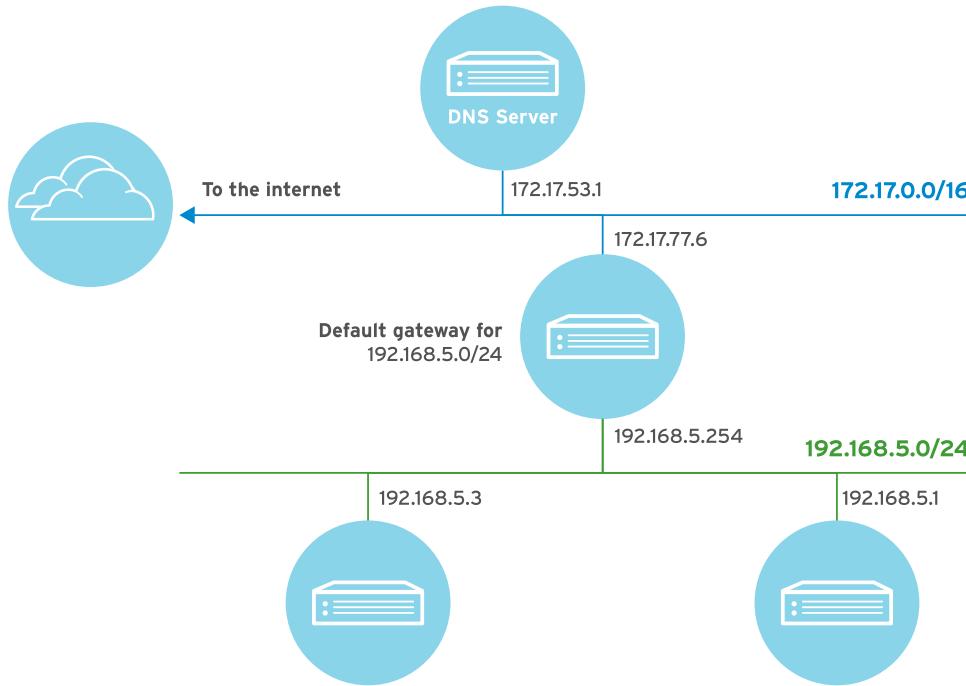


Figura 11.2: Conceptos de DNS y enrutamiento de red

Enrutamiento IPv4

Ya sea que se utilice IPv4 o IPv6, el tráfico de red debe desplazarse desde un host a otro y de una red a otra. Cada host tiene una *tabla de enrutamiento*, que le indica cómo enrutar el tráfico para redes particulares. Las entradas de la tabla de enrutamiento incluirán una red de destino, que se conecta para dirigir el tráfico, y la dirección IP de cualquier enrutador intermedio necesario para transmitir el mensaje a su destino final. La entrada de la tabla de enrutamiento que coincide con el destino del tráfico de red se utiliza para enrutarla. Si dos entradas coinciden, se utiliza la que tiene el prefijo más extenso.

Si el tráfico de red no coincide con una ruta más específica, la tabla de enrutamiento normalmente tiene una entrada para una *ruta predeterminada* a toda la Internet IPv4, 0.0.0.0/0. Esta ruta predeterminada apunta a un *enrutador* en una subred a la que se puede acceder, es decir, en una subred que tiene una ruta más específica en la tabla de enrutamiento del host.

Si un enrutador recibe tráfico que no está dirigido a este, en lugar de ignorarlo como un host normal, *reenvía* el tráfico sobre la base de su propia tabla de enrutamiento. Esto puede enviar el tráfico directamente al host de destino (si el enrutador se encuentra en la subred de destino) o se lo puede reenviar a otro enrutador. Este proceso de reenvío continúa hasta que el tráfico alcanza su destino final.

Ejemplo de tabla de enrutamiento

Destino	Interfaz	Enrutador (si es necesario)
192.0.2.0/24	wlo1	
192.168.5.0/24	enp3s0	

Destino	Interfaz	Enrutador (si es necesario)
0.0.0.0/0 (predeterminado)	enp3s0	192.168.5.254

En este ejemplo, el tráfico que se mueve para la dirección IP 192.0.2.102 desde este host se transmitirá directamente a ese destino a través de la interfaz inalámbrica **wlo1** porque su coincidencia más cercana es con la ruta 192.0.2.0/24. El tráfico de la dirección IP 192.168.5.3 se transmitirá directamente a ese destino a través de la interfaz Ethernet **enp3s0** porque su coincidencia más cercana es con la ruta 192.168.5.0/24.

El tráfico de la dirección IP 10.2.24.1 se transmitirá de una interfaz Ethernet **enp3s0** a un enrutador a través de 192.168.5.254, que reenviará el tráfico al destino final. La coincidencia más cercana de ese tráfico es con la ruta 0.0.0.0/0, ya que no hay una ruta más específica en la tabla de enrutamiento de este host. El enrutador usará su propia tabla de enrutamiento para determinar adónde reenviar el tráfico.

Nombres y direcciones IP

El protocolo IP utiliza direcciones para comunicarse, pero los seres humanos preferirían trabajar con nombres en lugar de cadenas de números largos y difíciles de recordar. DNS, el sistema de nombres de dominio, es una red distribuida de servidores que asignan nombres de host a direcciones IP. Para que el servicio de nombres funcione, el host debe estar apuntado a un *servidor de nombres*. Este servidor de nombres no debe estar en la misma subred, simplemente necesita que el host tenga acceso a ella.

Configuración de red estática o DHCP

Muchos sistemas están configurados para obtener valores de red automáticamente durante el proceso de arranque. De acuerdo con los archivos de configuración local, debe usarse DHCP y un servicio de cliente aparte consulta a la red por un servidor y obtiene un alquiler de valores de red.

Si no hay un servidor DHCP disponible, el sistema debe usar una configuración *estática* en la que los valores de red se lean desde un archivo de configuración local. El administrador de red o el equipo de arquitectura son los encargados de obtener los valores de red correctos para asegurarse de que no haya ningún conflicto con otros sistemas.

Como DHCP usa la dirección de hardware para hacer un seguimiento de las asignaciones, solo una dirección puede asignarse por interfaz con DHCP. Múltiples direcciones estáticas pueden asignarse a una sola interfaz. Esta práctica es común en sistemas que alojan servicios para varios clientes, como el alojamiento basado en la IP HTTP. Las interfaces Red Hat Enterprise Linux generalmente tienen una dirección IPv4 y una dirección de enlace local IPv6, aunque pueden tener asignadas más direcciones.

Nombres de interfaces de red

Tradicionalmente, las interfaces de red en Linux se enumeran de la siguiente manera: **eth0**, **eth1**, **eth2**, etc. Sin embargo, el mecanismo que define estos nombres puede efectuar cambios en cuanto a qué interfaz recibe un determinado nombre a medida que se añaden o eliminan dispositivos. El comportamiento de asignación de nombre predeterminado en Red Hat Enterprise Linux 7 consiste en asignar nombres fijos según firmware, topología de dispositivo y tipo de dispositivo. Los nombres de interfaces tienen los siguientes caracteres:

- Las interfaces Ethernet comienzan con *en*, las interfaces WLAN comienzan con *wl* y las interfaces WWAN comienzan con *ww*.

- El o los siguientes caracteres representan el tipo de adaptador: *o* significa incorporado, *s* significa ranura de conexión en caliente y *p* significa ubicación geográfica de PCI. Aunque no esté disponible de manera predeterminada, los administradores también utilizan una *x* para incorporar una dirección MAC.
- Por último, un número *N* se utiliza para representar un índice, una identificación o un puerto.
- Si el nombre fijo no puede determinarse, se usarán los nombres tradicionales, como *ethN*.

Por ejemplo, la primera interfaz de red integrada puede tener el nombre **eno1** y una interfaz de tarjeta PCI puede llamarse **enp2s0**. Los nombres nuevos facilitan la distinción de la relación entre un puerto y su nombre si el usuario conoce los dos, pero la desventaja es que el usuario no puede suponer que un sistema con una interfaz llame **eth0** a esa interfaz.



nota

Los nombres de las interfaces de red pueden anularse. Si el administrador instaló y habilitó el paquete **biosdevname**, o si definió reglas de asignación de nombres a dispositivos **udev** personalizadas, los valores anularán el esquema de asignación de nombres predeterminado. Dependiendo del soporte para **biosdevname** en el BIOS del sistema, podrán utilizarse nombres como **em1**, **em2**, etc. para tarjetas de red incorporadas (correspondientes a sus nombres en el chasis). Las tarjetas PCI(e) se representan con **pYpX** (por ejemplo: **p4p1**), en el que **Y** es el número de ranura PCI y **X** es el número para el puerto de esa tarjeta específica.



Referencias

Páginas del manual: **services(5)**, **ping(8)**, **biosdevname(1)** y **udev(7)**

Es posible encontrar información adicional en los capítulos sobre la configuración de redes y la asignación de nombres de dispositivos de red consistente en la *Guía de administración de la red de Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Práctica: Conceptos de red

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

Dirección IPv4 no válida	Esta configuración es viable.
La dirección IP no puede ser una dirección de red.	
La puerta de enlace no se encuentra en la misma subred.	
No está configurada la resolución de nombre.	

Parámetros de configuración de red	Corrección
IP address: 172.17.0.351/16 Gateway: 172.17.0.1 DNS server: 172.17.0.254	
IP address: 10.1.2.3/24 Gateway: 10.1.2.1 DNS server: 172.17.4.53	
IP address: 192.168.7.0/24 Gateway: 192.168.7.1 DNS server: 192.168.0.254	
IP address: 10.4.5.6/24 Gateway: 10.4.6.1	

Parámetros de configuración de red	Corrección
DNS server: 192.168.0.254	
IP address: 172.17.23.5/16 Gateway: 172.17.0.1	

Solución

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

Parámetros de configuración de red	Corrección
IP address: 172.17.0.351/16 Gateway: 172.17.0.1 DNS server: 172.17.0.254	Dirección IPv4 no válida
IP address: 10.1.2.3/24 Gateway: 10.1.2.1 DNS server: 172.17.4.53	Esta configuración es viable.
IP address: 192.168.7.0/24 Gateway: 192.168.7.1 DNS server: 192.168.0.254	La dirección IP no puede ser una dirección de red.
IP address: 10.4.5.6/24 Gateway: 10.4.6.1 DNS server: 192.168.0.254	La puerta de enlace no se encuentra en la misma subred.
IP address: 172.17.23.5/16 Gateway: 172.17.0.1	No está configurada la resolución de nombre.

Validación de la configuración de red

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder probar y revisar la configuración de red actual con las utilidades básicas.

Visualización de las direcciones IP

El comando `/sbin/ip` se usa para mostrar la información del dispositivo y la dirección.

```
[student@desktopX ~]$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 52:54:00:00:00:0a brd ff:ff:ff:ff:ff:ff
    ③inet 172.25.0.10/24 brd ④172.25.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    ⑤inet6 fe80::5054:ff:fe00:b/64 scope link
        valid_lft forever preferred_lft forever
```

- ① Una interfaz activa tiene el estado de **UP**.
- ② La línea del enlace especifica la dirección de hardware (MAC) del dispositivo.
- ③ La línea `inet` muestra la dirección IPv4 y el prefijo.
- ④ La dirección, el alcance y el nombre del dispositivo de transmisión también están en esta línea.
- ⑤ La línea `inet6` muestra la información de IPv6.

El comando `ip` también puede usarse para mostrar las estadísticas sobre el rendimiento de la red. Los paquetes recibidos (RX) y transmitidos (TX), los errores y los contadores dados de baja pueden usarse para identificar problemas de red provocados por congestión, poca memoria y saturación de ejecuciones.

```
[student@desktopX ~]$ ip -s link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
link/ether 52:54:00:00:00:0a brd ff:ff:ff:ff:ff:ff
    RX: bytes packets errors dropped overrun mcast
      269850     2931       0       0       0       0
    TX: bytes packets errors dropped carrier collsns
      300556     3250       0       0       0       0
```

Solución de problemas de ruta

El comando `/sbin/ip` también se usa para mostrar la información de ruta.

```
[student@desktopX ~]$ ip route
default via 172.25.0.254 dev eth0 proto static metric 1024
172.25.X.0/24 dev eth0 proto kernel scope link src 172.25.X.10
10.0.0.0/8 dev eth1 proto kernel scope link src 10.0.0.11
```

Todos los paquetes que estén destinados para la red 10.0.0.0/8 se enviarán directamente al destino mediante la `eth1` del dispositivo. Todos los paquetes que estén destinados para la

Capítulo 11. Administración de la red de Red Hat Enterprise Linux

red 172.25. La red X.0/24 se enviará directamente al destino mediante la eth0 del dispositivo. Todos los demás paquetes se enviarán al enrutador predeterminado que está ubicado en 172.25.X.254, y también mediante la eth0 del dispositivo.

El comando **ping** se usa para comprobar la conectividad. El comando continuará ejecutándose hasta que se presione **Ctrl+C**, a menos que se indiquen otras opciones para limitar la cantidad de paquetes enviados.

```
[student@desktopX ~]$ ping -c3 172.25.X.254
```

Para realizar el seguimiento de la ruta hacia un host remoto, use **traceroute** o **tracepath**. Ambos comandos pueden usarse para realizar el seguimiento de una ruta con paquetes de UDP; sin embargo, muchas redes bloquean el tráfico de UDP e ICMP. El comando **traceroute** tiene opciones para realizar el seguimiento de la ruta con paquetes UDP (predeterminado), ICMP (-I) o TCP (-T), pero es probable que no se instalen de manera predeterminada.

```
[student@desktopX ~]$ tracepath access.redhat.com
...
4: 71-32-28-145.rcmt.qwest.net          48.853ms asymm 5
5: dcp-brdr-04.inet.qwest.net           100.732ms asymm 7
6: 206.111.0.153.ptr.us.xo.net         96.245ms asymm 7
7: 207.88.14.162.ptr.us.xo.net         85.270ms asymm 8
8: ae1d0.cir1.atlanta6-ga.us.xo.net    64.160ms asymm 7
9: 216.156.108.98.ptr.us.xo.net       108.652ms
10: bu-ether13.at1ngamq46w-bcr00.tbone.rr.com 107.286ms asymm 12
...
```

Cada línea del resultado de **tracepath** representa un enrutador o *hop* por donde pasa el paquete entre el origen y el destino final. Se proporciona información adicional como disponible, que incluye la sincronización en ambos sentidos (RTT) y cualquier cambio en el tamaño de la unidad de transmisión máxima (MTU).

Solución de problemas en puertos y servicios

Los servicios TCP usan sockets como terminales para la comunicación y se componen de una dirección IP, protocolo y número de puerto. En general, los servicios están atentos a los puertos estándar mientras que los clientes usan un puerto disponible en forma aleatoria. Los nombres más conocidos de puertos estándares están enumerados en el archivo **/etc/services**.

El comando **ss** se usa para mostrar las estadísticas del socket. El comando **ss** tiene por objeto reemplazar la herramienta anterior **netstat**, incluida en el paquete *net-tools*, que algunos administradores de sistemas pueden conocer más, pero que es probable que no siempre esté instalada.

```
[student@desktopX ~]$ ss -ta
State      Recv-Q Send-Q      Local Address:Port          Peer Address:Port
LISTEN      0      128          *:sunrpc                  *:*
LISTEN      0      128          ①*:ssh                   *:*
LISTEN      0      100          ②127.0.0.1:smtp        *:*
LISTEN      0      128          *:36889                  *:*
ESTAB       0      0            ③172.25.X.10:ssh      172.25.254.254:59392
LISTEN      0      128          :::sunrpc                *:*:
```

LISTEN	0	128	④ ::::ssh	:::*
LISTEN	0	100	⑤ ::1:smtp	:::*
LISTEN	0	128	:::34946	:::*

- ① El puerto usado para SSH escucha todas las direcciones IPv4. El "*" se usa para indicar "todos" cuando se hace referencia a los puertos o las direcciones IPv4.
- ② El puerto usado para SMTP presta atención a la interfaz de circuito de retorno de la IPv4 127.0.0.1.
- ③ La conexión SSH establecida está en la interfaz 172.25.X.10 y se origina de un sistema con una dirección de 172.25.254.254.
- ④ El puerto usado para SSH está atento a todas las direcciones IPv6. Se usa la sintaxis "::" para representar todas las interfaces de IPv6.
- ⑤ El puerto usado para SMTP presta atención a la interfaz de circuito de retorno de la IPv6 ::1.

Opciones para ss y netstat.

Opción	Descripción
-n	Muestra números en lugar de nombres para las interfaces y los puertos.
-t	Muestra los sockets TCP.
-u	Muestra los sockets UDP.
-l	Muestra solo los sockets a los que está atento.
-a	Muestra todos los sockets (a los que presta atención y los establecidos).
-p	Muestra el proceso de usar los sockets.



Referencias

Páginas del manual: **ip-link(8)**, **ip-address(8)**, **ip-route(8)**, **ip(8)**, **ping(8)**, **tracepath(8)**, **traceroute(8)**, **ss(8)** y **netstat(8)**.

Es posible encontrar información adicional en el capítulo sobre configuración de la red en la *Guía de administración de la red de Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Práctica: Cómo examinar la configuración de red

En este ejercicio de laboratorio, examinará la configuración de red del sistema actual.

Resultados:

Identificar las interfaces de la red actual y las direcciones básicas de la red.

Antes de comenzar

Restablezca su sistema serverX.

1. Visualizar la dirección IP y la máscara de red actuales de todas las interfaces.

```
[student@serverX ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 52:54:00:00:00:0b brd ff:ff:ff:ff:ff:ff
    inet 172.25.X.11/24 brd 172.25.X.255 scope global dynamic eth0
        valid_lft 12704sec preferred_lft 12704sec
    inet6 fe80::5054:ff:fe00:b/64 scope link
        valid_lft forever preferred_lft forever
```

2. Visualizar las estadísticas correspondientes a la interfaz eth0.

```
[student@serverX ~]$ ip -s link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode
  DEFAULT qlen 1000
    link/ether 52:54:00:00:00:0b brd ff:ff:ff:ff:ff:ff
    RX: bytes packets errors dropped overrun mcast
      418398     4588      0      0      0
    TX: bytes packets errors dropped carrier collsns
      360733     1730      0      0      0
```

3. Visualizar la información de enrutamiento.

```
[student@serverX ~]$ ip route
default via 172.25.X.254 dev eth0 proto static metric 1024
172.25.X.0/24 dev eth0 proto kernel scope link src 172.25.X.11
```

4. Verificar que se pueda acceder al enrutador.

```
[student@serverX ~]$ ping -c3 172.25.X.254
PING 172.25.X.254 (172.25.X.254) 56(84) bytes of data.
64 bytes from 172.25.X.254: icmp_seq=1 ttl=64 time=0.489 ms
64 bytes from 172.25.X.254: icmp_seq=2 ttl=64 time=0.510 ms
64 bytes from 172.25.X.254: icmp_seq=3 ttl=64 time=0.458 ms
```

```
--- 172.25.X.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.458/0.485/0.510/0.033 ms
```

5. Mostrar todos los saltos entre el sistema local y classroom.example.com.

```
[student@serverX ~]$ tracepath classroom.example.com
 1: classroom.example.com                                0.522ms !H
                                         Resume: pmtu 65535
```

6. Visualizar los sockets TCP de escucha en el sistema local.

```
[student@serverX ~]$ ss -lt
State      Recv-Q Send-Q      Local Address:Port          Peer Address:Port
LISTEN      0      128          *:55630                  *:*
LISTEN      0      128          *:sunrpc                *:*
LISTEN      0      128          *:ssh                   *:*
LISTEN      0      100         127.0.0.1:smtp           *:*
LISTEN      0      128          :::sunrpc               :::*
LISTEN      0      128          :::ssh                  :::*
LISTEN      0      128          :::33079                :::*
LISTEN      0      100          :::1:smtp                :::*
```

Configuración de red con nmcli

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder administrar valores y dispositivos de red con **nmcli** y NetworkManager.

NetworkManager

NetworkManager es un demonio que monitorea y administra valores de red. Además del demonio, hay una miniaPLICACIÓN DEL ÁREA DE NOTIFICACIONES DE GNOME QUE PROPORCIONA INFORMACIÓN SOBRE EL ESTADO DE LA RED. LAS HERRAMIENTAS GRÁFICAS Y DE LA LÍNEA DE COMANDOS SE COMUNICAN CON NETWORKMANAGER Y GUARDAN ARCHIVOS DE CONFIGURACIÓN EN EL DIRECTORIO /etc/sysconfig/network-scripts.

Un *dispositivo* es una interfaz de red. Una *conexión* es una configuración utilizada para un dispositivo que está compuesto por un grupo de valores. Es posible que existan múltiples conexiones para un dispositivo, pero solo puede haber una activa por vez. Por ejemplo, un sistema normalmente está conectado con una red con valores proporcionados por DHCP. En ocasiones, el sistema debe estar conectado con una red de laboratorio o de centro de datos, que solo puede ser estática. En lugar de cambiar la configuración manualmente, cada configuración puede almacenarse como una conexión independiente.

Visualización de información de red con nmcli

Para visualizar una lista con todas las conexiones, use **nmcli con show**. Para enumerar solo las conexiones activas, añada la opción **--active**.

```
[root@desktopX ~]# nmcli con show
NAME           UUID                                  TYPE      DEVICE
static-eth0    f3e8dd32-3c9d-48f6-9066-551e5b6e612d 802-3-ethernet  eth0
System eth0    5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03 802-3-ethernet  --
guest         f601ca8a-6647-4188-a431-dab48cc63bf4   802-11-wireless wlp3s0
[root@desktopX ~]# nmcli con show --active
NAME           UUID                                  TYPE      DEVICE
static-eth0    f3e8dd32-3c9d-48f6-9066-551e5b6e612d 802-3-ethernet  eth0
guest         f601ca8a-6647-4188-a431-dab48cc63bf4   802-11-wireless wlp3s0
```

Especifique una identificación de conexión (nombre) para ver información detallada sobre esa conexión. Los valores en minúscula representan la configuración de la conexión. Los nombres de propiedad y configuración se definen en la página del manual **nm-settings(5)**. Los valores en mayúscula son datos activos.

```
[root@desktopX ~]# nmcli con show "static-eth0"
...
ipv4.method:          manual
ipv4.dns:             172.25.254.254, 8.8.8.8
ipv4.dns-search:
ipv4.addresses:       { ip = 172.25.X.10/24, gw = 172.25.X.254 }
ipv4.routes:
ipv4.ignore-auto-routes: no
ipv4.ignore-auto-dns:  no
ipv4.dhcp-client-id:  --
ipv4.dhcp-send-hostname: yes
ipv4.dhcp-hostname:   --
```

```
ipv4.never-default:          no
ipv4.may-fail:              yes
ipv6.method:                auto
...
```

El comando **nmcli** también puede usarse para visualizar el estado del dispositivo e información detallada sobre el mismo.

```
[root@desktopX ~]# nmcli dev status
DEVICE  TYPE      STATE   CONNECTION
eth0    ethernet  connected static-eth0
wlp3s0  wifi      connected guest
lo     loopback  unmanaged --
[root@desktopX ~]# nmcli dev show eth0
GENERAL.DEVICE:           eth0
GENERAL.TYPE:              ethernet
GENERAL.HWADDR:            52:54:00:00:00:0A
GENERAL.MTU:               1500
GENERAL.STATE:             100 (connected)
GENERAL.CONNECTION:        static-eth0
GENERAL.CON-PATH:          /org/freedesktop/NetworkManager/
ActiveConnection/1
WIRED-PROPERTIES.CARRIER:  on
IP4.ADDRESS[1]:            ip = 172.25.X.10/24, gw = 172.25.X.254
IP4.DNS[1]:                172.25.254.254
IP6.ADDRESS[1]:            ip = fe80::5054:fff:fe00:b/64, gw = ::
```

Creación de conexiones de red con **nmcli**

Cuando se crea una conexión de red nueva con **nmcli**, el orden de los argumentos importa. Los argumentos comunes aparecen primero y deben incluir el tipo y la interfaz. Luego, se deben determinar los argumentos específicos del tipo y, finalmente, definir la dirección IP, el prefijo y la información de la puerta de enlace. Múltiples direcciones IP pueden especificarse para un único dispositivo. Valores adicionales, como un servidor DNS, se definen como modificaciones una vez creada la conexión.

Ejemplos de creación de conexiones nuevas

Realice los siguientes pasos mientras el instructor habla sobre la sintaxis **nmcli**.

- Defina una conexión nueva con el nombre "default" que establezca su conexión automática como conexión Ethernet en el dispositivo eth0 usando DHCP.

```
[root@desktopX ~]# nmcli con add con-name "default" type ethernet ifname eth0
```

- Cree una conexión nueva con el nombre "static"; luego especifique la dirección IP y la puerta de enlace. No establezca la conexión automática.

```
[root@desktopX ~]# nmcli con add con-name "static" ifname eth0 autoconnect no type
                     ethernet ip4 172.25.X.10/24 gw4 172.25.X.254
```

- El sistema establecerá la conexión automática usando DHCP al inicio. Cambie a la conexión estática.

```
[root@desktopX ~]# nmcli con up "static"
```

Capítulo 11. Administración de la red de Red Hat Enterprise Linux

- Vuelva a la conexión DHCP.

```
[root@desktopX ~]# nmcli con up "default"
```



Importante

Si la conexión estática se pierde, la conexión predeterminada intentará establecer la conexión automática. Para deshabilitar una interfaz y evitar la conexión automática desde el punto de vista administrativo, utilice **nmcli dev disconnect DEVICE_NAME**.

Opciones de tipo

Las opciones de tipos de conexiones dependen del tipo empleado. Una conexión de tipo ethernet puede opcionalmente especificar una dirección MAC para la conexión. Una conexión de tipo Wi-Fi debe especificar la SSID y puede definir opciones adicionales. Hay muchos otros tipos disponibles, como conexión en puente, conexión de agregación, conexión en equipo, VPN y VLAN. Si desea conocer todas las opciones, utilice **nmcli con add help**.

```
[root@desktopX ~]# nmcli con add help
Usage: nmcli connection add { ARGUMENTS | help }

ARGUMENTS := COMMON_OPTIONS TYPE_SPECIFIC_OPTIONS IP_OPTIONS

COMMON_OPTIONS:
    type <type>
    ifname <interface name> | "*"
    [con-name <connection name>
     [autoconnect yes|no]
     [save yes|no]

TYPE_SPECIFIC_OPTIONS:
    ethernet:      [mac <MAC address>
                    [cloned-mac <cloned MAC address>
                     [mtu <MTU>
...
...
```

Modificación de interfaces de red con nmcli

Una conexión existente puede modificarse con argumentos **nmcli con mod**. Los argumentos son conjuntos de pares de claves/valores. La clave incluye un nombre de configuración y un nombre de propiedad. Utilice **nmcli con show "<ID>"** para ver una lista con los valores actuales para una conexión. En la página de manual **nm-settings(5)** se documentan los nombres de configuración y propiedad, además del uso.

```
[root@desktopX ~]# nmcli con show "static"
connection.id:                      static
connection.uuid:                     f3e8dd32-3c9d-48f6-9066-551e5b6e612d
connection.interface-name:           eth0
connection.type:                     802-3-ethernet
connection.autoconnect:              yes
connection.timestamp:                1394905322
connection.read-only:                no
...
```

Ejemplos de modificaciones en las conexiones

Realice los siguientes pasos mientras el instructor habla sobre la sintaxis **nmcli**.

- Apague la conexión automática.

```
[root@desktopX ~]# nmcli con mod "static" connection.autoconnect no
```

- Especifique un servidor DNS.

```
[root@desktopX ~]# nmcli con mod "static" ipv4.dns 172.25.X.254
```

- Se pueden añadir o eliminar valores de algunos argumentos de configuración. Añada un símbolo +/- delante del argumento. Añada un servidor DNS adicional.

```
[root@desktopX ~]# nmcli con mod "static" +ipv4.dns 8.8.8.8
```

- Reemplace la dirección IP estática y la puerta de enlace.

```
[root@desktopX ~]# nmcli con mod "static" ipv4.addresses "172.25.X.10/24  
172.25.X.254"
```

- Añada una dirección IP secundaria sin una puerta de enlace.

```
[root@desktopX ~]# nmcli con mod "static" +ipv4.addresses 10.10.10.10/16
```

**Importante**

El comando **nmcli con mod** guardará la configuración en los archivos de configuración. A fin de activar los cambios, la conexión debe activarse o reactivarse.

```
[root@desktopX ~]# nmcli con up "static"
```

Resumen de los comandos **nmcli**

Comandos básicos de conexiones y dispositivos de **nmcli**:

Comandos nmcli

Comando	Usar el
estado nmcli dev	Enumerar todos los dispositivos.
nmcli con show	Enumerar todas las conexiones.
nmcli con up "<ID>"	Activar una conexión.
nmcli con down "<ID>"	Desactivar una conexión. La conexión se reiniciará si la conexión automática está activada.
nmcli dev dis <DEV>	Desactivar una interfaz y deshabilitar temporalmente la conexión automática.

Comando	Usar el
nmcli net off	Deshabilitar todas las interfaces administradas.
nmcli con add ...	Añadir una conexión nueva.
nmcli con mod "<ID>" ...	Modificar una conexión.
nmcli con del "<ID>"	Eliminar una conexión.



nota

El comando **nmcli** también tiene un modo de edición interactiva. Para una interfaz gráfica, utilice **nm-connection-editor**.



Referencias

Páginas del manual: **nmcli(5)**, **nmcli-examples(5)** y **nm-settings(1)**

Es posible encontrar información adicional en la sección sobre el uso de la herramienta de línea de comandos NetworkManager nmcli en la *Guía de administración de la red de Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Práctica: Configuración de red con **nmcli**

En este ejercicio de laboratorio, configurará los parámetros de red con **nmcli**.

Resultados:

Conversión de un sistema de DHCP a configuración estática.

Antes de comenzar

Restablezca su sistema serverX.

- Visualice los parámetros de configuración de red con **nmcli**.

- 1.1. Muestre todas las conexiones.

```
[student@serverX ~]$ nmcli con show
NAME           UUID                                  TYPE      DEVICE
System eth0    5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0
```

- 1.2. Muestre todos los parámetros de configuración para la conexión activa.

```
[student@serverX ~]$ nmcli con show "System eth0"
connection.id:                         System eth0
connection.uuid:                        5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03
connection.interface-name:               eth0
connection.type:                        802-3-ethernet
connection.autoconnect:                 yes
connection.timestamp:                  1394813303
connection.read-only:                  no
connection.permissions:                ...
...
IP4.ADDRESS[1]:                         ip = 172.25.X.11/24, gw = 172.25.X.254
IP4.DNS[1]:                            172.25.254.254
IP4.DOMAIN[1]:                          example.com
...
```

- 1.3. Muestre el estado del dispositivo.

```
[student@serverX ~]$ nmcli dev status
DEVICE  TYPE      STATE      CONNECTION
eth0    ethernet  connected  System eth0
lo     loopback  unmanaged  --
```

- 1.4. Muestre los parámetros de configuración para el dispositivo eth0.

```
[student@serverX ~]$ nmcli dev show eth0
GENERAL.DEVICE:                     eth0
GENERAL.TYPE:                       ethernet
GENERAL.HWADDR:                     52:54:00:00:00:0B
GENERAL.MTU:                        1500
GENERAL.STATE:                      100 (connected)
GENERAL.CONNECTION:                 System eth0
GENERAL.CON-PATH:                   /org/freedesktop/NetworkManager/
ActiveConnection/1
WIRED-PROPERTIES.CARRIER:          on
IP4.ADDRESS[1]:                     ip = 172.25.X.11/24, gw = 172.25.X.254
```

Capítulo 11. Administración de la red de Red Hat Enterprise Linux

IP4.DNS[1]:	172.25.254.254
IP4.DOMAIN[1]:	example.com
IP6.ADDRESS[1]:	ip = fe80::5054:ff:fe00:b/64, gw = ::

2. Cree una conexión estática con la misma dirección IPv4, prefijo de red y puerta de enlace predeterminada. Nombre la conexión nueva como *static-eth0*.



Advertencia

Dado que el acceso al equipo se logra a través de la conexión de red principal, configurar los valores incorrectos durante la configuración de red puede hacer que su equipo no pueda encontrarse. Si esto sucede, use el botón **Reset** que está arriba de lo que antes era la pantalla gráfica del equipo e inténtelo de nuevo.

```
[student@serverX ~]$ sudo nmcli con add con-name "static-eth0" ifname eth0 type
ethernet ip4 172.25.X.11/24 gw4 172.25.X.254
Connection 'static-eth0' (f3e8dd32-3c9d-48f6-9066-551e5b6e612d) successfully added.
```

3. Modifique la conexión nueva para agregar el parámetro de configuración DNS.

```
[student@serverX ~]$ sudo nmcli con mod "static-eth0" ipv4.dns 172.25.254.254
```

4. Muestre y active la conexión nueva.

- 4.1. Visualice todas las conexiones.

```
[student@serverX ~]$ nmcli con show
NAME           UUID                                  TYPE      DEVICE
static-eth0    f3e8dd32-3c9d-48f6-9066-551e5b6e612d  802-3-ethernet --
System eth0    5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0
```

- 4.2. Visualice la conexión activa.

```
[student@serverX ~]$ nmcli con show --active
System eth0    5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0
```

- 4.3. Active la conexión nueva.

```
[student@serverX ~]$ sudo nmcli con up "static-eth0"
Connection successfully activated (D-Bus active path: /org/freedesktop/
NetworkManager/ActiveConnection/3)
```

- 4.4. Visualice la conexión activa.

```
[student@serverX ~]$ nmcli con show --active
NAME           UUID                                  TYPE      DEVICE
static-eth0    f3e8dd32-3c9d-48f6-9066-551e5b6e612d  802-3-ethernet  eth0
```

5. Pruebe la conectividad con las direcciones de red nuevas.

5.1. Verifique la dirección IP.

```
[student@serverX ~]$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    qlen 1000
        link/ether 52:54:00:00:00:0b brd ff:ff:ff:ff:ff:ff
        inet 172.25.X.11/16 brd 172.25.255.255 scope global eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::5054:ff:fe00:b/64 scope link
            valid_lft forever preferred_lft forever
```

5.2. Verifique la puerta de enlace predeterminada.

```
[student@serverX ~]$ ip route
default via 172.25.X.254 dev eth0 proto static metric 1024
172.25.X.0/24 dev eth0 proto kernel scope link src 172.25.X.11
```

5.3. Compruebe la dirección DNS.

```
[student@serverX ~]$ ping -c3 172.25.254.254
PING 172.25.254.254 (172.25.254.254) 56(84) bytes of data.
64 bytes from 172.25.254.254: icmp_seq=1 ttl=64 time=0.419 ms
64 bytes from 172.25.254.254: icmp_seq=2 ttl=64 time=0.598 ms
64 bytes from 172.25.254.254: icmp_seq=3 ttl=64 time=0.503 ms

--- 172.25.254.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.419/0.506/0.598/0.077 ms
```

6. Configure la conexión original para que no comience en el arranque y verifique que la conexión estática se use cuando se reinicie el sistema.

6.1. Inhabilite la conexión original para que no comience automáticamente en el arranque.

```
[student@serverX ~]$ sudo nmcli con mod "System eth0" \
> connection.autoconnect no
```

6.2. Reinicie el sistema.

```
[student@serverX ~]$ reboot
```

6.3. Visualice la conexión activa.

```
[student@serverX ~]$ nmcli con show --active
NAME      UUID                                  TYPE      DEVICE
static-eth0 f3e8dd32-3c9d-48f6-9066-551e5b6e612d 802-3-ethernet  eth0
```

Edición de archivos de configuración de red

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder modificar los parámetros de configuración de red mediante la edición de los archivos de configuración.

Modificación de la configuración de red

También se puede configurar la red editando los archivos de configuración de interfaz. Los archivos de configuración de interfaz controlan las interfaces de software para dispositivos de red individuales. En general, estos archivos se denominan **/etc/sysconfig/network-scripts/ifcfg-<name>**, donde <name> se refiere al nombre del dispositivo o a la conexión que controla el archivo de configuración. A continuación, se detallan las variables estándares que se encuentran en el archivo usado para la configuración estática o dinámica.

Opciones de configuración para el archivo ifcfg

Estática	Dinámica	Cualquiera de las opciones
BOOTPROTO=none	BOOTPROTO=dhcp	DEVICE=eth0
IPADDR0=172.25.X.10		NAME="System eth0"
PREFIX0=24		ONBOOT=yes
GATEWAY0=172.25.X.254		UUID=f3e8dd32-3...
DEFROUTE=yes		USERCTL=yes
DNS1=172.25.254.254		

En estos parámetros de configuración estáticos, las variables para la dirección IP, el prefijo y la puerta de enlace tienen un número al final. Esto permite que se asignen varios conjuntos de valores a la interfaz. La variable DNS también tiene un número que se usa para especificar el orden de la búsqueda cuando se especifican varios servidores.

Después de modificar los archivos de configuración, ejecute **nmcli con reload** para que NetworkManager lea los cambios de configuración. La interfaz todavía necesita reiniciarse para que se implementen los cambios.

```
[root@serverX ~]# nmcli con reload
[root@serverX ~]# nmcli con down "System eth0"
[root@serverX ~]# nmcli con up "System eth0"
```



Referencias

Página del manual (1)**nmcli**

Es posible encontrar información adicional en el capítulo sobre configuración de la red en la *Guía de administración de la red de Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Práctica: Edición de archivos de configuración de red

En este ejercicio de laboratorio, editarás archivos de configuración de red.

Resultados:

Una dirección de red adicional agregada a cada sistema.

Andes de comenzar

Restablezca sus sistemas serverX y desktopX.

- Como usuario raíz, edite **/etc/sysconfig/network-scripts/ifcfg-eth0** en serverX para agregar una dirección adicional de **10.0.X.1/24**.

- 1.1. Agregue una entrada al archivo para especificar la dirección IPv4.

```
[root@serverX ~]# echo "IPADDR1=10.0.X.1" >> /etc/sysconfig/network-scripts/ifcfg-eth0
```

- 1.2. Agregue una entrada al archivo para especificar el prefijo de red.

```
[root@serverX ~]# echo "PREFIX1=24" >> /etc/sysconfig/network-scripts/ifcfg-eth0
```

2. Active la dirección nueva.

- 2.1. Vuelva a cargar los cambios de configuración.

```
[root@serverX ~]# nmcli con reload
```

- 2.2. Reinicie la conexión con los parámetros de configuración nuevos.

```
[root@serverX ~]# nmcli con up "System eth0"
```

3. Como usuario raíz, edite **/etc/sysconfig/network-scripts/ifcfg-eth0** en desktopX para agregar una dirección adicional de **10.0.X.2/24** y cargue la nueva configuración.

- 3.1. Modifique el archivo para agregar la IPv4 y el prefijo de red.

```
[root@desktopX ~]# echo "IPADDR1=10.0.X.2" >> /etc/sysconfig/network-scripts/ifcfg-eth0
[root@desktopX ~]# echo "PREFIX1=24" >> /etc/sysconfig/network-scripts/ifcfg-eth0
```

- 3.2. Vuelva a cargar los cambios de configuración.

```
[root@desktopX ~]# nmcli con reload
```

3.3. Restablezca la conexión con los parámetros de configuración nuevos.

```
[root@desktopX ~]# nmcli con up "System eth0"
```

4. Pruebe la conectividad con las direcciones de red nuevas.

4.1. En serverX, verifique la dirección IP.

```
[root@serverX ~]# ip addr
```

4.2. En serverX, compruebe la dirección nueva de desktopX.

```
[root@serverX ~]# ping 10.0.X.2
```

4.3. En desktopX, verifique la dirección IP.

```
[root@desktopX ~]# ip addr
```

4.4. En desktopX, compruebe la dirección nueva de serverX.

```
[root@desktopX ~]# ping 10.0.X.1
```

Configuración de nombres de host y resolución de nombre

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder configurar y probar el nombre del host del sistema y la resolución de nombre.

Cambio de nombre del host del sistema

El comando **hostname** muestra o modifica provisoriamente el nombre del host totalmente calificado del sistema.

```
[root@desktopX ~]# hostname
desktopX.example.com
```

Puede especificarse un nombre del host estático en el archivo **/etc/hostname**. Se usa el comando **hostnamectl** para modificar este archivo y puede utilizarse para ver el estado del nombre del host totalmente calificado del sistema. Si este archivo no existe, el nombre del host se establece mediante una consulta de DNS invertida una vez que la interfaz tiene una dirección IP asignada.

```
[root@desktopX ~]# hostnamectl set-hostname desktopX.example.com
[root@desktopX ~]# hostnamectl status
    Static hostname: desktopX.example.com
          Icon name: computer
            Chassis: n/a
      Machine ID: 9f6fb63045a845d79e5e870b914c61c9
        Boot ID: aa6c3259825e4b8c92bd0f601089ddf7
  Virtualization: kvm
Operating System: Red Hat Enterprise Linux Server 7.0 (Maipo)
      CPE OS Name: cpe:/o:redhat:enterprise_linux:7.0:GA:server
        Kernel: Linux 3.10.0-97.el7.x86_64
      Architecture: x86_64
[root@desktopX ~]# cat /etc/hostname
desktopX.example.com
```



Importante

El nombre del host estático se guarda en **/etc/hostname**. Las versiones anteriores de Red Hat Enterprise Linux almacenaban el nombre del host como una variable en el archivo **/etc/sysconfig/network**.

Configuración de la resolución de nombre

El *sistema de resolución de nombres interno* se utiliza para convertir nombres de host en direcciones IP o a la inversa. Los contenidos del archivo **/etc/hosts** se verifican en primer lugar.

```
[root@desktopX ~]# cat /etc/hosts
```

```
127.0.0.1      localhost localhost.localdomain localhost4 localhost4.localdomain4
::1            localhost localhost.localdomain localhost6 localhost6.localdomain6

172.25.254.254 classroom.example.com
172.25.254.254 content.example.com
```

El comando **getent hosts hostname** puede usarse para probar la resolución de nombre del host con el archivo **/etc/hosts**.

Si no se encuentra una entrada en ese archivo, el sistema de resolución de nombres interno buscará la información en un servidor de nombres DNS. El archivo **/etc/resolv.conf** controla la forma en que se realiza esta consulta:

- **nameserver**: la dirección IP de un servidor de nombres que se consultará. Se pueden proporcionar hasta tres directivas de servidor de nombres para proporcionar copias de seguridad en caso de que una no funcione.
- **search**: una lista de nombres de dominio para probar con un nombre del host corto. Tanto este como el **domain** no deben configurarse en el mismo archivo; si esto ocurre, prevalece la última instancia. Vea **resolv.conf(5)** para obtener más detalles.

```
[root@desktopX ~]# cat /etc/resolv.conf
# Generated by NetworkManager
domain example.com
search example.com
nameserver 172.25.254.254
```

NetworkManager actualizará el archivo **/etc/resolv.conf** con los parámetros de configuración de DNS en los archivos de configuración de conexión. Use **nmcli** para modificar las conexiones.

```
[root@desktopX ~]# nmcli con mod ID ipv4.dns IP
[root@desktopX ~]# nmcli con down ID
[root@desktopX ~]# nmcli con up ID
[root@desktopX ~]# cat /etc/sysconfig/network-scripts/ifcfg-ID
...
DNS1=8.8.8.8
...
```

El comportamiento predeterminado de **nmcli con mod ID ipv4.dns IP** es reemplazar cualquier parámetro de configuración de DNS anterior con la nueva lista de IP provista. El símbolo +/- que está frente al argumento **ipv4.dns** agregará o eliminará una entrada individual.

```
[root@desktopX ~]# nmcli con mod ID +ipv4.dns IP
```

El comando de **host HOSTNAME** puede usarse para probar la conectividad del servidor DNS.

```
[root@desktopX ~]# host classroom.example.com
classroom.example.com has address 172.25.254.254
[root@desktopX ~]# host 172.25.254.254
254.254.25.172.in-addr.arpa domain name pointer classroom.example.com.
```



Importante

Si se usa DHCP, **/etc/resolv.conf** se reescribe automáticamente a medida que se inician las interfaces, a menos que usted especifique **PEERDNS=no** en los archivos de configuración de interfaz correspondientes. El cambio puede realizarse con **nmcli**.

```
[root@desktopX ~]# nmcli con mod "System eth0" ipv4.ignore-auto-dns yes
```



Referencias

Páginas del manual: **nmcli(5)**, **hostnamectl(1)**, **hosts(1)**, **getent(1)**, **host(1)** y **resolv.conf(5)**.

Es posible encontrar información adicional en el capítulo sobre configuración de nombres de host en la *Guía de administración de red de Red Hat Enterprise Linux para Red Hat Enterprise Linux 7*, que se puede encontrar en

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

Práctica: Configuración de nombres de hosts y resolución de nombres

En este ejercicio de laboratorio, configurará el nombre del host del sistema y la resolución del nombre.

Resultados:

Configuración personalizada del nombre del host y resolución del nombre.

Antes de comenzar

Restablezca su sistema serverX.

1. Visualice la configuración del nombre del host actual.

- 1.1. Muestre el nombre del host actual.

```
[student@serverX ~]$ hostname  
serverX.example.com
```

- 1.2. Muestre el estado del nombre del host.

```
[student@serverX ~]$ hostnamectl status  
Static hostname: n/a  
Transient hostname: serverX.example.com  
Icon name: computer  
Chassis: n/a  
Machine ID: 9f6fb63045a845d79e5e870b914c61c9  
Boot ID: d4ec3a2e8d3c48749aa82738c0ea946a  
Operating System: Red Hat Enterprise Linux Server 7.0 (Maipo)  
CPE OS Name: cpe:/o:redhat:enterprise_linux:7.0:GA:server  
Kernel: Linux 3.10.0-97.el7.x86_64  
Architecture: x86_64
```

2. Configure un nombre del host estático para que coincida con el nombre del host transitorio.

- 2.1. Cambie el nombre del host y el archivo de configuración del host. Reemplace la X con su número de estación y relacione el resultado del paso anterior.

```
[student@serverX ~]$ sudo hostnamectl set-hostname serverX.example.com
```

- 2.2. Visualice el archivo de configuración que proporciona el nombre del host al inicio de la red.

```
[student@serverX ~]$ cat /etc/hostname  
serverX.example.com
```

- 2.3. Muestre el estado del nombre del host.

```
[student@serverX ~]$ hostnamectl status
```

Capítulo 11. Administración de la red de Red Hat Enterprise Linux

```
Static hostname: serverX.example.com
Icon name: computer
Chassis: n/a
Machine ID: 9f6fb63045a845d79e5e870b914c61c9
Boot ID: d4ec3a2e8d3c48749aa82738c0ea946a
Operating System: Red Hat Enterprise Linux Server 7.0 (Maipo)
CPE OS Name: cpe:/o:redhat:enterprise_linux:7.0:GA:server
Kernel: Linux 3.10.0-97.el7.x86_64
Architecture: x86_64
```

3. Cambie temporalmente el nombre del host.

- 3.1. Cambie el nombre del host.

```
[student@serverX ~]$ sudo hostname testname
```

- 3.2. Muestre el nombre del host actual.

```
[student@serverX ~]$ hostname
testname
```

- 3.3. Visualice el archivo de configuración que proporciona el nombre del host al inicio de la red.

```
[student@serverX ~]$ cat /etc/hostname
serverX.example.com
```

- 3.4. Reinicie el sistema.

```
[student@serverX ~]$ reboot
```

- 3.5. Muestre el nombre del host actual.

```
[student@serverX ~]$ hostname
serverX.example.com
```

4. Agregue el sobrenombre local para el servidor del aula.

- 4.1. Busque la dirección IP de classroom.example.com.

```
[student@serverX ~]$ host classroom.example.com
classroom.example.com has address 172.25.254.254
```

- 4.2. Modifique **/etc/hosts**, de modo que el nombre **class** tenga la dirección IP 172.25.254.254 y se pueda usar para comunicarse con classroom.example.com.

```
[student@serverX ~]$ sudo vim /etc/hosts
[student@serverX ~]$ cat /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
172.25.254.254 classroom.example.com class
```

```
172.25.254.254 content.example.com
```

4.3. Busque la dirección IP de la clase.

```
[student@serverX ~]$ host class
Host class not found: 2(SERVFAIL)
[student@serverX ~]$ getent hosts class
172.25.254.254    classroom.example.com class
```

4.4. Aplique ping a la clase.

```
[student@serverX ~]$ ping -c3 class
PING classroom.example.com (172.25.254.254) 56(84) bytes of data.
64 bytes from classroom.example.com (172.25.254.254): icmp_seq=1 ttl=64
time=0.397 ms
64 bytes from classroom.example.com (172.25.254.254): icmp_seq=2 ttl=64
time=0.447 ms
64 bytes from classroom.example.com (172.25.254.254): icmp_seq=3 ttl=64
time=0.470 ms

--- classroom.example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.397/0.438/0.470/0.030 ms
```

Ejercicio de laboratorio: Administración de la red de Red Hat Enterprise Linux

En este ejercicio de laboratorio, configurará redes IPv4 básicas en sistemas Red Hat Enterprise Linux.

Resultados:

La primera interfaz tiene dos direcciones IPv4 estáticas configuradas.

Antes de comenzar

Restablezca su sistema desktopX.

1. Cree una conexión de red estática nueva con los valores de configuración que figuran en la tabla. Asegúrese de reemplazar la X con el número correcto para sus sistemas.

Parámetro	Parámetro
Nombre de la conexión	ejercicio de laboratorio
Dirección IP	172.25.X.10/16
Dirección de puerta de enlace	172.25.X.254
Dirección DNS	172.25.254.254

2. Configure la conexión nueva para que se inicie en forma automática. Otras conexiones no deberían iniciarse automáticamente.
3. Modifique la conexión nueva para que también use la dirección 10.0.X.1/24.
4. Configure el archivo **hosts** para que pueda hacerse referencia a 10.0.X.1 como "privada".
5. Reinicie el sistema y, luego, ejecute **lab network grade** para verificar la configuración.

Solución

En este ejercicio de laboratorio, configurará redes IPv4 básicas en sistemas Red Hat Enterprise Linux.

Resultados:

La primera interfaz tiene dos direcciones IPv4 estáticas configuradas.

Andes de comenzar

Restablezca su sistema desktopX.

- Cree una conexión de red estática nueva con los valores de configuración que figuran en la tabla. Asegúrese de reemplazar la X con el número correcto para sus sistemas.

Parámetro	Parámetro
Nombre de la conexión	ejercicio de laboratorio
Dirección IP	172.25.X.10/16
Dirección de puerta de enlace	172.25.X.254
Dirección DNS	172.25.254.254

```
[root@desktopX ~]# nmcli con add con-name lab iface eth0 type ethernet ip4
172.25.X.10/24 gw4 172.25.X.254
[root@desktopX ~]# nmcli con mod "lab" ipv4.dns 172.25.254.254
```

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

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

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

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

De manera alternativa:

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

- Configure el archivo **hosts** para que pueda hacerse referencia a 10.0.X.1 como "privada".

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

- Reinicie el sistema y, luego, ejecute **lab network grade** para verificar la configuración.

```
[root@desktopX ~]# lab network grade
```

Resumen

Conceptos de red

Enumerar características de redes de computadoras.

Validación de la configuración de red

Para determinar la configuración de red actual, use las utilidades básicas.

Configuración de red con nmcli

Administrar dispositivos de red con utilidades de la línea de comandos.

Edición de archivos de configuración de red

Modifique archivos de configuración de red.

Configuración de nombres de host y resolución de nombre

Muestre y cambie el nombre del host del sistema y la configuración de resolución de nombre.



CAPÍTULO 12

ARCHIVAR Y COPIAR ARCHIVOS ENTRE SISTEMAS

Visión general:	
Meta	Archivar y copiar archivos de un sistema a otro.
Objetivos	<ul style="list-style-type: none">• Usar TAR para crear documentos de archivos comprimidos nuevos y extraer documentos desde documentos de archivos existentes.• Copiar archivos en forma segura desde o hacia un sistema remoto que ejecuta sshd.• Sincronizar en forma segura el contenido de un archivo o directorio local con una copia remota.
Secciones	<ul style="list-style-type: none">• Administración de archivos TAR comprimidos (y práctica)• Copia de archivos entre sistemas en forma segura (y práctica)• Sincronización de archivos entre sistemas en forma segura (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">• Archivar y copiar archivos entre sistemas

Administración de archivos tar comprimidos

Objetivo

Tras finalizar esta sección, los estudiantes deberían poder usar tar para crear ficheros de archivos comprimidos nuevos y extraer ficheros desde ficheros de archivos existentes.

¿Qué es tar?

El archivado y la compresión de archivos es útil cuando se realizan copias de seguridad y se transfieren datos a través de una red. Uno de los comandos más antiguos y más usados para crear y trabajar con archivos de seguridad es el comando **tar**.

Con el comando **tar**, los usuarios pueden reunir grandes conjuntos de ficheros en un solo fichero (archivo). El archivo puede comprimirse con **gzip**, **bzip2** o **xz**.

El comando tar también puede enumerar el contenido de los archivos o extraer sus ficheros a su sistema actual. En esta sección, se incluyen ejemplos de cómo usar el comando **tar**.

Uso del comando tar

Para usar el comando **tar**, es necesario realizar una de las tres acciones que se indican a continuación:

- **c** (cree un archivo)
- **t** (enumere el contenido de un archivo)
- **x** (extraiga un archivo)

Las opciones más usadas son:

- **f file name** (nombre del fichero del archivo en el que se trabajará)
- **v** (exceso de palabras; se utiliza para ver qué ficheros se agregan o extraen del archivo)



nota

Un - inicial no es necesario para las opciones de tar.

Archivar ficheros y directorios con tar

Antes de crear un archivo tar, verifique que no haya otro archivo en el directorio con el mismo nombre del archivo que se creará. El comando **tar** sobrescribirá el archivo existente sin ningún comentario.

La primera opción para usar cuando se crea un archivo nuevo es la **c**, seguida de la opción **f**, luego un solo espacio, el nombre del fichero del archivo que se creará y, por último, la lista de los ficheros y directorios que deben agregarse al archivo. El archivo se crea en el directorio actual, a menos que se especifique lo contrario.

En el siguiente ejemplo, se crea un archivo con el nombre **archive.tar** que contiene fichero1, fichero2 y fichero3 en el directorio de inicio del usuario.

```
[user@host ~]# tar cf archive.tar file1 file2 file3
[user@host ~]# ls archive.tar
archive.tar
```



nota

Cuando se archivan ficheros con nombres de ruta absolutos, el / inicial de la ruta se elimina del nombre del archivo de manera predeterminada. Esta acción ayuda a evitar errores que pueden causar que se sobrescriban ficheros importantes. Por lo general, los ficheros se extraen según el directorio de trabajo actual del comando tar.

Para que tar pueda archivar los ficheros seleccionados, es obligatorio que el usuario que ejecute el comando tar pueda leer los ficheros. Por ejemplo, la creación de un archivo nuevo de la carpeta /etc y todo su contenido requiere privilegios de usuario raíz porque solo este tipo de usuario tiene permitido leer todos los archivos que están en esta carpeta. Un usuario sin privilegios podría crear un archivo de la carpeta /etc, pero el archivo omitiría los ficheros que no incluyan el permiso de lectura para el usuario y omitiría los directorios que no incluyan permiso de lectura y ejecución para el usuario.

Como usuario raíz, cree el archivo tar /root/etc.tar con el directorio /etc como contenido:

```
[root@host ~]# tar cf /root/etc.tar /etc
tar: Removing leading `/' from member names
[root@host ~]#
```



Importante

Si bien tar almacena la propiedad y los permisos de los archivos, existen otros atributos que no se almacenan en el archivo tar de manera predeterminada, como el contexto SELinux y las ACL. Para almacenar esos atributos ampliados en el archivo tar, se necesita la opción --xattrs cuando se crea un archivo.

Enumeración del contenido de un archivo tar

Para enumerar el contenido de un archivo, se necesitan las opciones t y f, además del archivo en que se trabajará.

Enumere el contenido del archivo /root/etc.tar:

```
[root@host ~]# tar tf /root/etc.tar
etc/
etc/fstab
etc/crypttab
etc/mtab
...
```

Extracción de un archivo creado con tar

Por lo general, un archivo tar debería extraerse en un directorio vacío para garantizar que no sobrescriba ningún archivo existente. Si los archivos son extraídos por el usuario root, **tar** intenta conservar el usuario original y la propiedad del grupo de los archivos. Si un usuario habitual extrae los archivos con **tar**, los archivos extraídos son propiedad de ese usuario.

Extraiga el archivo **/root/etc.tar** en el directorio **/root/etcbackup**:

```
[root@host ~]# mkdir /root/etcbackup
[root@host ~]# cd /root/etcbackup
[root@host etcbackup]# tar xf /root/etc.tar
```

De manera predeterminada, cuando se extraen ficheros de un archivo, el desenmascaramiento se elimina de los permisos de contenido del archivo. Esta es una medida de seguridad y evita que los archivos que se extraen con más frecuencia reciban permisos de ejecución de manera predeterminada. Para proteger los permisos de un fichero archivado, se usará la opción **p** cuando se extraiga un archivo.

Extraiga el archivo **/root/myscripts.tar** en el directorio **/root/scripts** y conserve los permisos de los archivos extraídos:

```
[root@host ~]# mkdir /root/scripts
[root@host ~]# cd /root/scripts
[root@host scripts]# tar xpf /root/myscripts.tar
```

Creación de un archivo tar comprimido

Existen tres métodos de compresión admitidos por el comando **tar**. La compresión gzip es la más rápida y antigua, y la que tiene mayor disponibilidad. Por lo general, la compresión bzip2 genera ficheros de archivo más pequeños comparados con gzip y tiene menor disponibilidad que gzip, mientras que el método de compresión xz es relativamente nuevo, pero en general ofrece la mejor relación de compresión de los métodos disponibles.



nota

La efectividad del algoritmo de compresión depende de la naturaleza exacta de los datos que se comprimen. Los ficheros de datos que ya están comprimidos, como los formatos de imagen comprimidos o archivos rpm, generalmente generan una relación de compresión baja.

Una práctica adecuada es usar un solo directorio de nivel superior, que puede contener otros directorios y ficheros, para simplificar la extracción de los ficheros de manera organizada.

Para crear un archivo comprimido, puede especificarse una de las siguientes opciones de **tar**:

- **z** para la compresión de gzip (filename.tar.gz o filename.tgz)
- **j** para la compresión de bzip2 (filename.tar.bz2)
- **J** para la compresión de xz (filename.tar.xz)

Cree un archivo tar (opción c) comprimido con gzip (opción z) **/root/etcbackup.tar.gz** del directorio **/etc** en serverX:

```
[root@serverX ~]$ tar czf /root/etcbackup.tar.gz /etc
```

Cree un archivo tar (opción c) comprimido con bzip2 (opción j) **/root/logbackup.tar.bz2** del directorio **/var/log** en serverX:

```
[root@serverX ~]$ tar cjf /root/logbackup.tar.bz2 /var/log
```

Cree un archivo tar (opción c) comprimido con xz (opción J) **/root/sshconfig.tar.xz** del directorio **/etc/ssh** en serverX:

```
[root@serverX ~]$ tar cJf /root/sshconfig.tar.xz /etc/ssh
```

Extracción de un archivo tar comprimido

El primer paso cuando se extrae un archivo tar comprimido es determinar el lugar donde se extraerán los ficheros archivados y, a continuación, crear y cambiar el directorio de destino. Para extraer correctamente el archivo, en general no es necesario usar la misma opción de compresión utilizada cuando se crea el archivo, ya que el comando **tar** determinará cuál es la compresión que se usó. Es válido agregar un método de descompresión a las opciones de **tar** de la siguiente manera:

Extraiga el contenido (opción x) de un archivo tar (opción z) comprimido con gzip con el nombre **/root/etcbackup.tar.gz** en el directorio **/tmp/etcbackup**:

```
[root@serverX ~]$ mkdir /tmp/etcbackup
[root@serverX ~]$ cd /tmp/etcbackup
[root@serverX etcbackup]$ tar xzf /root/etcbackup.tar.gz
```

Extraiga el contenido (opción x) de un archivo tar comprimido con bzip2 (opción j) con el nombre **/root/logbackup.tar.bz2** en el directorio **/tmp/logbackup**:

```
[root@serverX ~]$ mkdir /tmp/logbackup
[root@serverX ~]$ cd /tmp/logbackup
[root@serverX logbackup]# tar xjf /root/logbackup.tar.bz2
```

Extraiga el contenido (opción x) de un archivo tar comprimido con xz (opción J) con el nombre **/root/sshbackup.tar.xz** en el directorio **/tmp/sshbackup**:

```
[root@serverX ~]$ mkdir /tmp/sshbackup
[root@serverX ~]$ cd /tmp/sshbackup
[root@serverX sshbackup]# tar xJf /root/sshbackup.tar.xz
```



nota

La enumeración de un archivo **tar** comprimido funciona de la misma manera que la enumeración de un archivo **tar** sin comprimir.



nota

Además, **gzip**, **bzip2** y **xz** se pueden usar de manera independiente para comprimir archivos individuales. Por ejemplo, **gzip etc.tar** genera el archivo comprimido **etc.tar.gz**, mientras que **bzip2 abc.tar** genera el archivo comprimido **abc.tar.bz2** y **xz myarchive.tar** genera el archivo comprimido **myarchive.tar.xz**.

Los comandos de descompresión correspondientes son **gunzip**, **bunzip2** y **unxz**. Por ejemplo, **gunzip /tmp/etc.tar.gz** genera el archivo tar sin comprimir **etc.tar**, mientras que **bunzip2 abc.tar.bz2** genera el archivo tar sin comprimir **abc.tar** y **unxz myarchive.tar.xz** genera el archivo tar sin comprimir **myarchive.tar**.

Descripción general de las opciones de tar

El comando **tar** tiene varias opciones que puede usar. La siguiente tabla enumera algunas de las opciones más usadas y sus significados.

Descripción general de las opciones de tar

Opción	Significado
c	Cree un archivo nuevo.
x	Extráigalo de un fichero existente.
t	Enumere el contenido de un archivo.
v	Exceso de palabras: muestra cuáles son los archivos que se archivan o extraen.
f	Nombre del archivo: esta opción tiene que estar seguida del nombre del fichero del archivo que se usará o creará.
p	Conserve los permisos de los ficheros y directorios cuando se extrae un archivo sin eliminar el desenmascaramiento.
z	Usa compresión gzip (.tar.gz).
j	Use la compresión bzip2 (.tar.bz2). Generalmente, bzip2 logra una mejor relación de compresión que gzip .
J	Use la compresión xz (.tar.xz). Generalmente, xz logra una mejor relación de compresión que bzip2 .



Referencias

Páginas del manual: **tar** (1), **gzip** (1), **gunzip** (1), **bzip2** (1), **bunzip2** (1), **xz** (1) y **unxz** (1)

Práctica: Copia de seguridad y restauración de archivos a partir de un archivo tar

En este ejercicio de laboratorio, los estudiantes crearán y extraerán archivos con **tar**.

Resultados:

Los estudiantes realizarán la copia de seguridad de un árbol de directorios y extraerán el contenido de los archivos en otra ubicación.

- Como solo el usuario root puede leer todo el contenido del directorio **/etc**, realizaremos una copia de seguridad del directorio e iniciaremos sesión en serverX como usuario **root**.

```
[student@desktopX ~]$ ssh root@serverX
```

- Cree un archivo **/etc** usando la compresión **gzip** para realizar una copia de seguridad del directorio del archivo de configuración **/etc**. Guarde el archivo como **/tmp/etc.tar.gz**.

```
[root@serverX ~]# tar czf /tmp/etc.tar.gz /etc
```

- Compruebe que el archivo de configuración **etc.tar.gz** sea válido; para ello, descomprima el archivo en un directorio recientemente creado llamado **/backuptest** en serverX.

1. Cree el directorio de destino **/backuptest**.

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

2. Cambie al directorio **/backuptest**, en el que extraeremos los archivos del archivo **etc.tar.gz**.

```
[root@serverX ~]# cd /backuptest
```

3. Extraiga el archivo **etc.tar.gz** en el directorio **/backuptest**.

```
[root@serverX backuptest]# tar xzf /tmp/etc.tar.gz
```

Copia segura de archivos entre sistemas

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder copiar archivos de manera segura desde un sistema remoto que ejecute el servidor sshd y hasta él.

Copiar archivos desde una ubicación remota y hasta ella con scp.

El comando **ssh** es útil para ejecutar los comandos de shell en sistemas remotos en forma segura. También se puede utilizar para copiar archivos de una máquina a otra en forma segura. El comando **scp** transfiere archivos desde un host remoto hasta el sistema local o desde el sistema local hasta un host remoto. Utiliza el servidor SSH para la autenticación y la transferencia de datos cifrados.

Las ubicaciones remotas de sistemas de archivos siempre se especifican con el formato **[user@]host:/path** tanto para la ubicación de origen como para la de destino de los archivos que se transferirán. La parte **user@** es opcional y, si falta, se utiliza el usuario local actual que invoca el comando **scp**. Antes de que se inicie la transferencia, el usuario debe autenticarse con el servidor SSH con contraseña o claves de SSH.

El siguiente es un ejemplo de cómo copiar los archivos locales que se encuentran en **/etc/yum.conf** y **/etc/hosts** de manera segura en la cuenta student del sistema remoto serverX en el directorio **/home/student/**:

```
[student@desktopX ~]$ scp /etc/yum.conf /etc/hosts serverX:/home/student  
student@serverX's password: student  
      yum.conf                                100%   813      0.8KB/s  00:00  
      hosts                                    100%   227      0.2KB/s  00:00
```

Un usuario puede copiar un archivo desde una cuenta remota de una máquina remota en un sistema de archivos local con **scp**. En este ejemplo, copie el archivo **/etc/hostname** desde la cuenta **student** de la máquina serverX; en el directorio local **/home/student/**.

```
[student@desktopX ~]$ scp serverX:/etc/hostname /home/student/  
student@serverX's password: student  
      hostname                                 100%    22      0.0KB/s  00:00
```

Para copiar un árbol de directorios completo de manera recursiva, se encuentra disponible la opción **-r**. En el siguiente ejemplo, el directorio remoto **/var/log** en serverX se copia de manera recursiva en el directorio local **/tmp/** en desktopX. Para poder leer todos los archivos que se copiaron en el directorio **/tmp**, el usuario debe conectarse a la ubicación remota como **root**.

```
[student@desktopX ~]$ scp -r root@serverX:/var/log /tmp  
root@serverX's password: redhat  
...
```

Transferencia de archivos remota con **sftp**

Si se prefiere una herramienta interactiva para la carga de archivos en un servidor SSH o su descarga, puede utilizarse el comando **sftp**. Una sesión con **sftp** es similar a una sesión FTP clásica, solo que emplea el mecanismo de autenticación segura y la transferencia de datos cifrados del servidor SSH.

Para iniciar una sesión **sftp**, **sftp** espera una ubicación remota con el formato **[user@]host**, en el que la parte **user@** es opcional y, si falta, se utiliza el usuario que invoca el comando **sftp**. Para establecer la sesión **sftp**, es necesario realizar la autenticación con cualquiera de los métodos que acepta el servidor SSH.

```
[student@desktopX ~]$ sftp serverX
student@serverX's password: student
Connected to serverX.
sftp>
```

La sesión **sftp** acepta diversos comandos que funcionan de la misma manera en el sistema de archivos remoto que en el sistemas de archivos local, como **ls**, **cd**, **mkdir**, **rmdir** y **pwd**. Además, existen los comandos **put** y **get** para la carga y descarga de archivos. El comando **exit** finaliza la sesión **sftp**.

Cargue el archivo local **/etc/hosts** en el directorio recientemente creado **/home/student/hostbackup** en el host remoto serverX. La sesión **sftp** siempre supone que el comando **put** es seguido de un archivo en el sistema de archivos local y comienza en el directorio de inicio del usuario conectado; en este caso, **/home/student**:

```
sftp> mkdir hostbackup
sftp> cd hostbackup
sftp> put /etc/hosts
Uploading /etc/hosts to /home/student/hostbackup/hosts
/etc/hosts                                         100%   227      0.2KB/s   00:00
sftp>
```

Para descargar el archivo remoto **/etc/yum.conf** del host remoto en el directorio actual del sistema de archivos local, ejecute el comando **get /etc/yum.conf** y finalice la sesión **sftp** con el comando **exit**.

```
sftp> get /etc/yum.conf
Fetching /etc/yum.conf to yum.conf
/etc/yum.conf                                         100%   813      0.8KB/s   00:00
sftp> exit
[student@desktopX ~]$
```



Referencias

Páginas del manual: **scp(1)**, **sftp(1)**

Práctica: Copia de archivos por medio de la red con scp

En este trabajo de laboratorio, los estudiantes copiarán archivos desde un sistema remoto a un directorio local con **scp**.

Resultados:

Los estudiantes copiarán archivos desde un host remoto hacia un directorio que está en la máquina local.

1. Copie en forma remota el directorio **/etc/ssh** en la máquina serverX en el directorio **/home/student/serverbackup** creado recientemente en desktopX con **scp**.

- 1.1. Cree el directorio de destino **/home/student/serverbackup** en desktopX.

```
[student@desktopX ~]$ mkdir /home/student/serverbackup
```

- 1.2. En forma recursiva, copie el directorio **/etc/ssh** de serverX al directorio **/home/student/serverbackup** en desktopX con el comando **scp**. Tenga en cuenta que solo el usuario raíz puede leer todo el contenido del directorio **/etc/ssh**.

```
[student@desktopX ~]$ scp -r root@serverX:/etc/ssh /home/student/serverbackup
```

Sincronización de archivos entre sistemas en forma segura

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder sincronizar en forma eficiente y segura el contenido de un archivo o directorio local con una copia remota.

Sincronizar archivos y carpetas con rsync

Con la herramienta **rsync** también se pueden copiar archivos en forma segura de un sistema a otro. Se diferencia de scp en que si dos archivos o directorios son similares entre dos sistemas, rsync solo necesita copiar las diferencias entre los sistemas, mientras que scp necesita copiar todo.

Una de las ventajas de **rsync** es que puede copiar archivos entre un sistema local y un sistema remoto en forma segura y eficiente. Cuando la sincronización inicial de un directorio demora prácticamente el mismo tiempo que el copiado, cualquier sincronización posterior solo requerirá que se copien las diferencias mediante la red.

Una de las opciones más importantes de **rsync** es la opción **-n** para realizar un simulacro. Un simulacro es una imitación de lo que sucede cuando el comando se ejecuta de verdad. Mostrará los cambios que realizará cuando se ejecute el comando sin la opción de simulacro. Se recomienda realizar un simulacro de cualquier operación de **rsync** para garantizar que no se sobrescriba ni elimine ningún archivo.

Las dos opciones más usadas cuando se sincronizan archivos y carpetas con **rsync** son **-a** y **-v**. Mientras la opción **-v** agrega un exceso de palabras al resultado a medida que continúa la sincronización, la opción **-a** implica un "modo archivo" y habilita las siguientes opciones, todas al mismo tiempo:

- **-r**, sincronizar en forma recurrente todo el árbol de directorio
- **-l**, sincronizar los enlaces simbólicos
- **-p**, mantener los permisos
- **-t**, conservar las marcas de tiempo
- **-g**, conservar la propiedad del grupo
- **-o**, conservar al propietario de los archivos
- **-D**, sincronizar los archivos de dispositivo

Si bien la opción **-a** ya sincroniza enlaces simbólicos, existen otras opciones necesarias para conservar los enlaces duros ya que, de lo contrario, son tratados como archivos separados. La opción **-H** habilita la manipulación de enlaces duros; por lo tanto, el comando **rsync** identificará los enlaces físicos que están en la carpeta de origen y vinculará los archivos en consecuencia en la carpeta de destino, en lugar de solo copiarlos como archivos separados.



nota

La opción **-a** no sincroniza los permisos de archivo avanzados, como los contextos de archivos ACL o SELinux. Para habilitar la sincronización de ACL, se requiere la opción **-A** además de la opción **-a**, mientras que para sincronizar los contextos de SELinux de archivos de origen a archivos de destino, es necesario agregar la opción **-X**.

La manera básica de usar **rsync** es sincronizar dos carpetas locales. En el siguiente ejemplo, el directorio **/var/log** obtiene una copia sincronizada en la carpeta **/tmp**. El directorio **log** junto con su contenido se crea en el directorio **/tmp**.

```
[student@desktopX ~]$ su -  
Password: redhat  
[root@desktopX ~]# rsync -av /var/log /tmp  
...
```

Para sincronizar solo el contenido de una carpeta sin crearla en el directorio de destino, se necesita agregar una barra al final del directorio de origen. En este ejemplo, el directorio **log** no se crea en la carpeta **/tmp**. Solo se sincroniza el contenido del directorio **/var/log/** en la carpeta **/tmp**.

```
[root@desktopX ~]# rsync -av /var/log/ /tmp  
...
```



Importante

Cuando se ingrese el directorio de origen para **rsync**, es muy importante recordar si está presente la barra final en el nombre del directorio. Esto determinará si el directorio o solo el contenido del directorio se sincroniza en el destino. Nota: La terminación del tabulador agregará automáticamente una barra al final de los nombres de directorios.

Al igual que con **scp**, el comando **rsync** espera a que se especifiquen las ubicaciones del sistema de archivos remoto en el formato **[user@]host:/path**. En caso de que falte la parte **user@** opcional, se usa el usuario que invoca el comando **rsync** para conectarse a la ubicación remota. Se puede usar una ubicación remota como origen o destino. En el siguiente ejemplo, la carpeta local **/var/log** obtiene una copia sincronizada en el directorio **/tmp**, en la máquina serverX. Para que **rsync** sincronice la propiedad de los archivos transferidos, la ubicación de destino debe estar escrita como usuario root; en consecuencia, conéctese a serverX del sistema remoto como usuario root. El usuario root que se conecta debe autenticarse con el servidor SSH mediante cualquiera de los métodos aceptados; por ejemplo, contraseña o claves de SSH.

```
[root@desktopX ~]$ rsync -av /var/log serverX:/tmp  
root@serverX's password: redhat  
...
```

De la misma manera, la carpeta remota **/var/log** en serverX puede sincronizarse en el directorio local **/tmp** en desktopX:

```
[root@desktopX ~]$ rsync -av serverX:/var/log /tmp  
root@serverX's password: redhat  
...
```



Referencias

Página del manual (1)**rsync**

Práctica: Sincronización segura de dos directorios con rsync

En este trabajo de laboratorio, los estudiantes realizarán la sincronización de una carpeta con un sistema remoto mediante el uso de **rsync**.

Resultados:

Un directorio se sincronizará de una máquina remota a la máquina local. Después de que los archivos de la máquina remota se hayan cambiado, se volverán a sincronizar con la máquina local y solo las modificaciones se transferirán. Los dos sistemas terminarán con contenido idéntico en los directorios sincronizados con rsync.

1. De manera segura, cree una copia inicial del árbol de directorios **/var/log** en serverX en un directorio recientemente creado denominado **/serverlogs** en desktopX mediante el comando **rsync**.
 - 1.1. A fin de crear el directorio de destino **/serverlogs**, cambie a la cuenta del usuario raíz con el comando **su**.

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

- 1.2. Cree el directorio de destino **/serverlogs** en desktopX en el que los archivos de registro de serverX se sincronizarán.

```
[root@desktopX ~]# mkdir /serverlogs
```

- 1.3. Use el comando **rsync** para sincronizar el árbol de directorio **/var/log** en serverX con el directorio **/serverlogs** en desktopX. Tenga en cuenta que solo el usuario raíz puede leer todo el contenido del directorio **/var/log** en serverX. Todos los archivos serán transferidos en la sincronización inicial.

```
[root@desktopX ~]# rsync -av root@serverX:/var/log /serverlogs  
...
```

2. Como usuario raíz en serverX, ejecute **logger "Log files synchronized"** para obtener una nueva entrada en el archivo de registro **/var/log/messages** que refleje cuándo se realizó la última sincronización.

```
[root@desktopX ~]# ssh root@serverX 'logger "Log files synchronized"'  
Password: redhat  
[root@desktopX ~]#
```

3. Sincronice de manera segura el árbol de directorios **/var/log** en serverX con el directorio **/serverlogs** en desktopX nuevamente con el comando **rsync**. Observe que, en esta oportunidad, solo se transferirán los archivos de registro modificados.

```
[root@desktopX ~]# rsync -av root@serverX:/var/log /serverlogs  
...
```

Trabajo de laboratorio: Archivado y copia de archivos entre sistemas

En este trabajo de laboratorio, los estudiantes usarán **rsync**, **scp** y **tar** para archivar y realizar copias de seguridad de los contenidos de carpetas.

Resultados:

Los estudiantes realizarán la sincronización de una carpeta remota con un directorio local; luego se crea un archivo con la carpeta sincronizada como contenido; el archivo se copia en la máquina remota y se extrae en un directorio recientemente creado.

Antes de comenzar

Restablezca su sistema serverX.

1. Sincronice el árbol de directorio **/etc** en serverX con el directorio **/configsync** en desktopX.
2. En desktopX, cree un archivo con el nombre **/root/configfile-backup-&srv;.tar.gz** con el directorio **/configsync** como contenido, y copie el archivo en el directorio **/root** en serverX para fines de copias de seguridad con el comando **scp**.
3. Para preparar el árbol de directorio archivado a fin de compararlo con los archivos de configuración actualmente usados en forma activa en serverX, extraiga el contenido del archivo **/root/configfile-backup-&srv;.tar.gz** en el directorio **/tmp/savedconfig** en serverX.

Solución

En este trabajo de laboratorio, los estudiantes usarán **rsync**, **scp** y **tar** para archivar y realizar copias de seguridad de los contenidos de carpetas.

Resultados:

Los estudiantes realizarán la sincronización de una carpeta remota con un directorio local; luego se crea un archivo con la carpeta sincronizada como contenido; el archivo se copia en la máquina remota y se extrae en un directorio recientemente creado.

Andes de comenzar

Restablezca su sistema serverX.

1. Sincronice el árbol de directorio **/etc** en serverX con el directorio **/configsync** en desktopX.
 - 1.1. Para poder crear el directorio de destino **/configsync**, pase a la cuenta de usuario raíz usando **su**.

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

- 1.2. Cree el directorio de destino para los archivos de configuración en desktopX.

```
[root@desktopX ~]# mkdir /configsync
```

- 1.3. Use el comando **rsync** para sincronizar el árbol de directorio **/etc** en serverX con el directorio **/configsync** en desktopX. Tenga presente que solo el usuario raíz puede leer todo el contenido del directorio **/etc** en serverX.

```
[root@desktopX ~]# rsync -av root@serverX:/etc /configsync  
...
```

2. En desktopX, cree un archivo con el nombre **/root/configfile-backup-&rv;.tar.gz** con el directorio **/configsync** como contenido, y copie el archivo en el directorio **/root** en serverX para fines de copias de seguridad con el comando **scp**.

- 2.1. Guarde el directorio **/configsync** en el archivo **/root/configfile-backup-&rv;.tar.gz**.

```
[root@desktopX ~]# tar czf /root/configfile-backup-serverX.tar.gz /configsync
```

- 2.2. Cree una copia de seguridad de **/root/configfile-backup-&rv;.tar.gz** en serverX.

```
[root@desktopX configsync]# scp /root/configfile-backup-serverX.tar.gz  
root@serverX:/root  
Password: redhat  
...
```

Capítulo 12. Archivar y copiar archivos entre sistemas

3. Para preparar el árbol de directorio archivado a fin de compararlo con los archivos de configuración actualmente usados en forma activa en serverX, extraiga el contenido del archivo **/root/configfile-backup-&rv;.tar.gz** en el directorio **/tmp/savedconfig/** en serverX.

- 3.1. Conéctese a la máquina serverX; como usuario root con **ssh**.

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

- 3.2. Cree el directorio de destino **/tmp/savedconfig/**, en el que se extraerán los contenidos del archivo **/root/configfile-backup-&rv;.tar.gz**.

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

- 3.3. Cambie al directorio de destino **/tmp/savedconfig/** en serverX.

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

- 3.4. Extraiga el contenido del archivo **/root/configfile-backup-&rv;.tar.gz** en el directorio **/tmp/savedconfig/** en serverX.

```
[root@serverX savedconfig]# tar xzf /root/configfile-backup-serverX.tar.gz
```

Resumen

Administración de archivos tar comprimidos

El comando **tar** proporciona un conjunto de métodos de compresión diferentes para archivar ficheros y restablecerlos desde un archivo.

Copia segura de archivos entre sistemas

Además de proporcionar una shell remota segura, el servicio ssh también ofrece **scp** y **sftp** como modos seguros de transferir archivos desde un sistema remoto que ejecute el servidor SSH y hasta él.

Sincronización de archivos entre sistemas en forma segura

El comando **rsync** sincroniza archivos en forma segura y eficiente con una ubicación remota.



CAPÍTULO 13

INSTALACIÓN Y ACTUALIZACIÓN DE PAQUETES DE SOFTWARE

Descripción general	
Meta	Descargar, instalar, actualizar y administrar paquetes de software de Red Hat y repositorios de paquetes YUM.
Objetivos	<ul style="list-style-type: none">Registrar sistemas con su cuenta de Red Hat y autorizar las actualizaciones de software para los productos instalados.Explicar el significado de un paquete RPM y el modo en que los paquetes RPM se utilizan para administrar software en un sistema con Red Hat Enterprise Linux.Buscar, instalar y actualizar paquetes de software usando el comando yum.Habilitar y deshabilitar el uso de repositorios YUM de terceros o de Red Hat.Examinar los archivos de paquetes de software descargados e instalarlos.
Secciones	<ul style="list-style-type: none">Asignación de suscripciones a sistemas para actualizaciones de software (y práctica)Paquetes de software RPM y YUM (y práctica)Administración de actualizaciones de software con yum (y práctica)Habilitación de repositorios de software yum (y práctica)Cómo examinar archivos de paquetes RPM (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">Instalación y actualización de paquetes de software

Adjuntar sistemas a las suscripciones para actualizaciones de software

Objetivos

Registrar sistemas con su cuenta de Red Hat y autorizar las actualizaciones de software para los productos instalados.

Administración de suscripciones de Red Hat

La administración de la suscripción de Red Hat proporciona herramientas que se pueden usar para que los equipos tengan derecho a suscripciones de productos, de modo que los administradores puedan obtener actualizaciones de paquetes de software y buscar información sobre contratos de soporte y suscripciones usadas por sus sistemas. Las herramientas estándares, como **PackageKit** y **yum**, pueden obtener paquetes y actualizaciones de software mediante una red de distribución de contenido provista por Red Hat.

Existen cuatro tareas básicas que se completan con las herramientas de administración de suscripciones de Red Hat:

- **Registro**, que es un sistema que asocia ese sistema con una cuenta Red Hat. Esto permite al administrador de suscripciones realizar un inventario exclusivo del sistema. Cuando ya no se usa, es posible anular la suscripción del sistema.
- **Subscribir**, que es un sistema que autoriza las actualizaciones de productos de Red Hat seleccionados. Las suscripciones tienen niveles específicos de asistencia, fechas de vencimiento y repositorios predeterminados. Las herramientas pueden usarse para adjuntar en forma automática o seleccionar una autorización específica. A medida que necesiten cambios, es probable que se eliminen las suscripciones.
- **Habilite los repositorios** para proporcionar paquetes de software. De manera predeterminada, se habilitan varios repositorios con cada suscripción, pero otros repositorios, como las actualizaciones o el código de origen, pueden habilitarse o inhabilitarse según sea necesario.
- **Revise y rastree** las autorizaciones que están disponibles o se consumen. La información de suscripción puede visualizarse en forma local, en un sistema específico, ya sea en la página **Suscripciones** del portal del cliente de Red Hat o en el administrador de activos de suscripción (SAM).

Registro de un sistema

Para registrar un sistema con el servicio de administración de suscripciones, inicie **subscription-manager -gui** mediante la selección de **Applications > System Tools > Red Hat Subscription Manager** del menú GNOME principal. Ingrese la contraseña de usuario **root** cuando se le solicite autenticarse. Esta acción mostrará la ventana siguiente **Subscription Manager**.

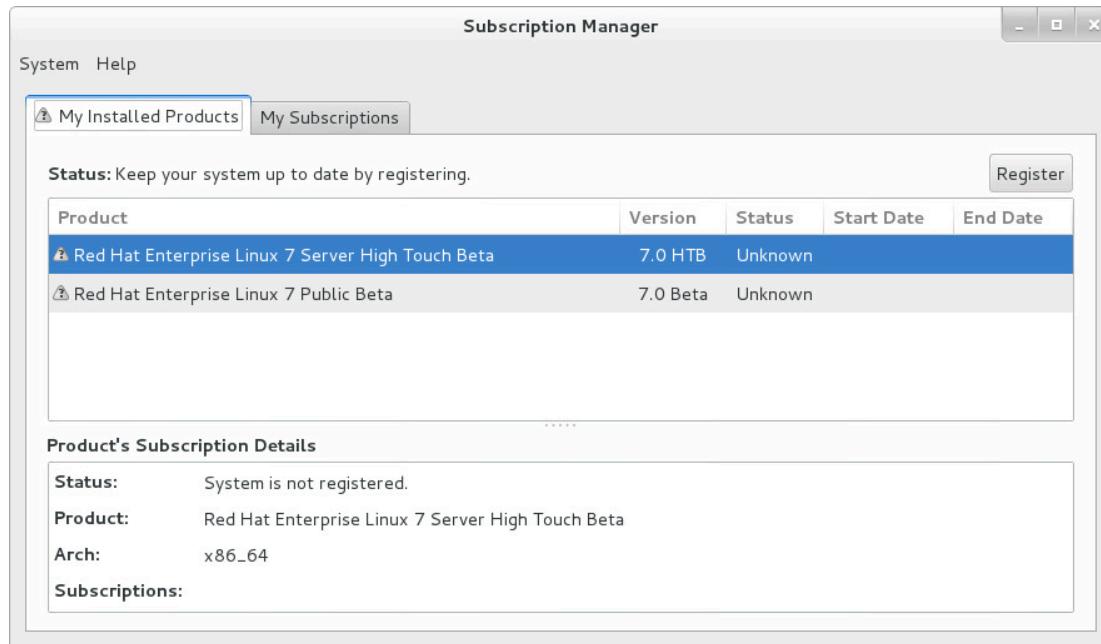
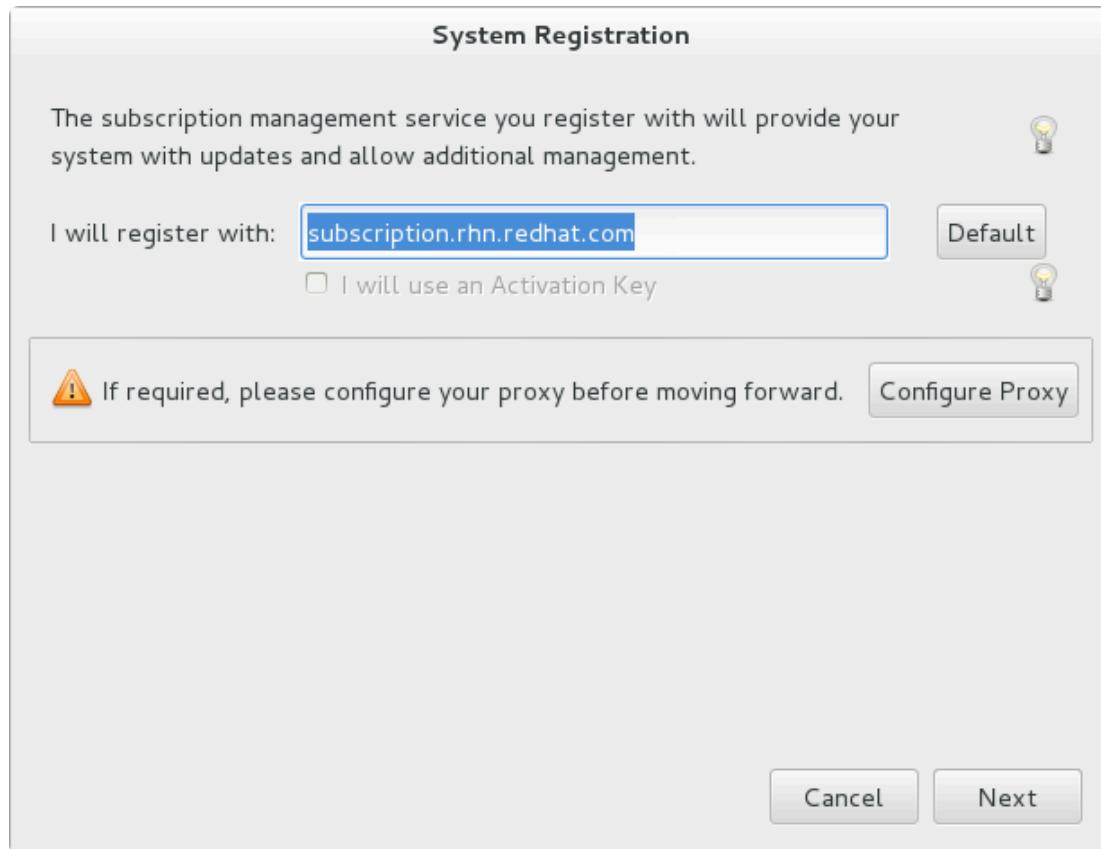


Figura 13.1: Ventana principal del administrador de suscripciones de Red Hat

Para registrar el sistema, haga clic en el botón **Register** situado en la esquina superior derecha de la ventana **Subscription Manager**. Esto abrirá el siguiente cuadro de diálogo:



Capítulo 13. Instalación y actualización de paquetes de software

Figura 13.2: Cuadro de diálogo de ubicación de servicio del administrador de suscripciones de Red Hat

Este cuadro de diálogo registra un sistema con un servidor de suscripción. El predeterminado (subscription.rhn.redhat.com) registra el servidor en la red de distribución de contenido "alojado" de Red Hat.

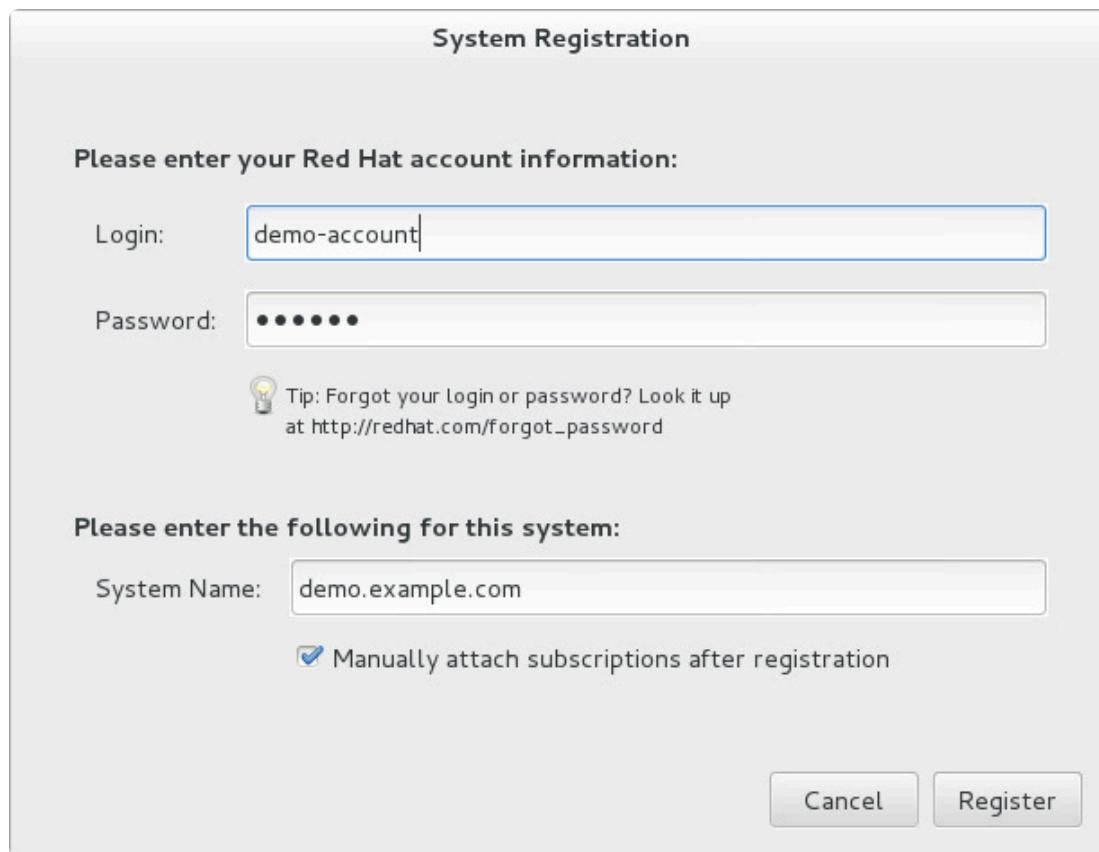


Figura 13.3: Cuadro de diálogo de información de cuenta del administrador de suscripciones de Red Hat

Haga clic en **Next** y a continuación, autentique con la cuenta Red Hat en que debe registrarse el sistema.

De manera predeterminada, el **administrador de suscripciones** intentará encontrar la mejor suscripción para este sistema a partir de todas las suscripciones disponibles. Si hay más de una suscripción disponible, o se necesita una suscripción específica, seleccione la casilla de verificación **Manually attach subscriptions after registration**. Con esta opción marcada, el **administrador de suscripciones** solo registrará el sistema y no le asignará automáticamente ninguna suscripción.

Haga clic en el botón **Register** para completar el registro.

Asignación de suscripciones

Para asignar suscripciones a un sistema, desplácese hasta la pestaña **All Available Subscriptions** en la ventana principal del **administrador de suscripciones** y, luego, haga clic en el botón **Update** para obtener una lista de las suscripciones disponibles.

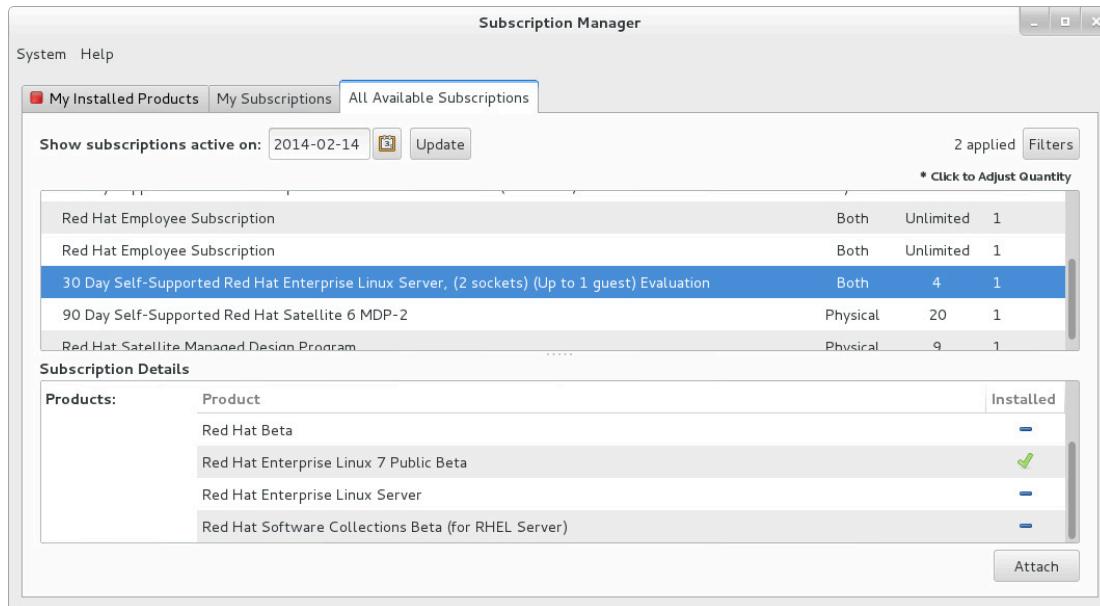


Figura 13.4: Pestaña All Available Subscriptions del administrador de suscripciones de Red Hat

A partir de esta lista, seleccione una o más suscripciones que deseé asignar al sistema y, luego, haga clic en el botón **Attach**.

Si hubiera más de un contrato para una suscripción específica, se abrirá un nuevo cuadro de diálogo donde se le pedirá que seleccione qué contrato desea usar. Tenga en cuenta que existen distintos contratos para sistemas *físicos* y *virtuales*.

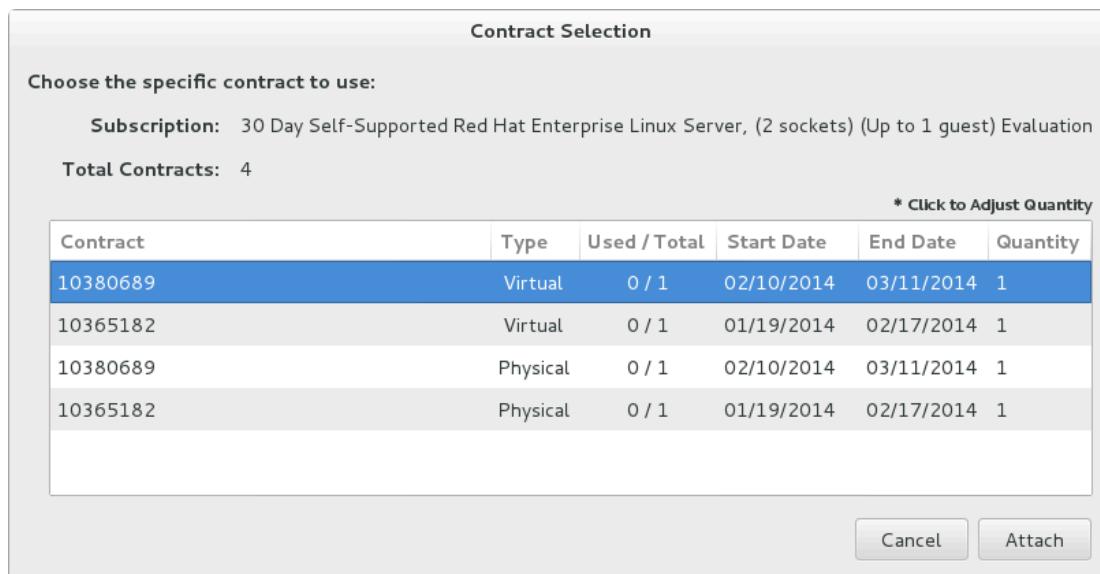


Figura 13.5: Cuadro de diálogo Contract Selection del administrador de suscripciones de Red Hat

Después de que se haya asignado una suscripción, cierre la ventana **Subscription Manager**. Acaba de suscribir su sistema y está listo para recibir actualizaciones o instalar software nuevo de Red Hat.

Automatizar registros y suscripciones

Para registrar un sistema sin usar un entorno gráfico, use **subscription-manager**(8). El comando **subscription-manager** puede adjuntar automáticamente un sistema a las suscripciones compatibles que mejor coincidan para el sistema.

- Registrar un sistema en una cuenta Red Hat:

```
[root@serverX ~]# subscription-manager register --username=yourusername --password=yourpassword
```

- Visualizar las suscripciones disponibles:

```
[root@serverX ~]# subscription-manager list --available | less
```

- Adjuntar automáticamente una suscripción:

```
[root@serverX ~]# subscription-manager attach --auto
```

- Visualizar las suscripciones consumidas:

```
[root@serverX ~]# subscription-manager list --consumed
```

- Eliminar la suscripción de un sistema:

```
[root@serverX ~]# subscription-manager unregister
```

nota

subscription-manager también se puede usar junto con *claves de activación*, que permiten el registro y la asignación de suscripciones definidas previamente, sin usar un nombre de usuario o una contraseña. Este método de registro puede ser muy útil para las instalaciones e implementaciones automáticas. Por lo general, las claves de activación son emitidas por un servicio de administración de suscripciones in situ, como el administrador de activos de suscripción; no se analizará en detalle en este curso.

Certificados de autorización

Una autorización es una suscripción que se adjuntó a un sistema. Los certificados digitales se usan para almacenar información actual sobre las autorizaciones en el sistema local. Una vez registrados, los certificados de autorización se almacenan en **/etc/pki** y en sus subdirectorios.

- **/etc/pki/product** contiene certificados que indican que hay productos Red Hat instalados en el sistema.
- **/etc/pki/consumer** contiene certificados que indican la cuenta Red Hat donde está registrado el sistema.

- **/etc/pki/entitlement** contiene certificados que indican cuáles son las suscripciones que están adjuntadas al sistema.

Los certificados pueden inspeccionarse en forma directa con la utilidad **rct**, pero generalmente las herramientas de **subscription-manager** son una manera más práctica para el usuario de examinar las suscripciones que están adjuntadas al sistema.



Importante

En un principio, las versiones anteriores de Red Hat Enterprise Linux admitían un método de administración de suscripciones distinto, el *RHN Classic*. RHN Classic no es compatible con Red Hat Enterprise Linux 7.

El método analizado en esta sección, *Administración de suscripciones de Red Hat*, es el único que se usa en RHEL 7 y es el método predeterminado usado por RHEL 6 después de RHEL 6.3, y por RHEL 5 después de RHEL 5.9. RHEL 4 solo admite el método antiguo. En las referencias que están al final de esta sección, se ofrece más información sobre ambos métodos.



Referencias

Páginas del manual: **subscription-manager-gui(8)**, **subscription-manager(8)**, **rct(8)**

Comenzar con la Administración de suscripciones de Red Hat
<https://access.redhat.com/site/articles/433903>

Administración de suscripciones de Red Hat: migración de RHN y satélite
https://access.redhat.com/site/documentation/en-US/Red_Hat_Subscription_Management/1/html-single/MigratingRHN/

Práctica: Administración de suscripciones de Red Hat

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

Habilitar repositorios	Registro
Revisar y hacer un seguimiento	Suscribir

Descripción	Tarea
Determinar la cantidad de suscripciones disponibles	
Habilitar un sistema para usar los productos Red Hat seleccionados	
Asignar un sistema a una cuenta de Red Hat	
Proporcionar paquetes de software	

Solución

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

Descripción	Tarea
Determinar la cantidad de suscripciones disponibles	Revisar y hacer un seguimiento
Habilitar un sistema para usar los productos Red Hat seleccionados	Suscribir
Asignar un sistema a una cuenta de Red Hat	Registro
Proporcionar paquetes de software	Habilitar repositorios

Paquetes de software RPM y yum

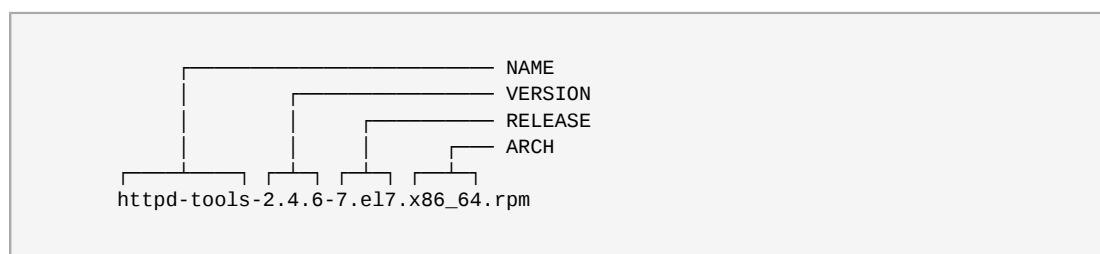
Objetivos

Tras finalizar esta sección, los estudiantes deberían poder explicar qué es un paquete RPM y cómo se utilizan los paquetes de este tipo para administrar software en un sistema con Red Hat Enterprise Linux.

Paquetes de software y RPM

Hace varios años, Red Hat desarrolló **RPM Package Manager**, que ofrece una manera estándar de colocar software en paquetes para su distribución. Administrar software como *paquetes RPM* es mucho más sencillo que trabajar con un software que simplemente se extrae de un fichero en un sistema de archivos. Esta solución permite que los administradores controlen qué archivos se instalaron con el paquete de software y cuáles deben quitarse si el software se desinstala, y que verifiquen que los paquetes compatibles estén presentes cuando se instale. La información sobre los paquetes instalados se almacena en una base de datos de RPM local en cada sistema. Todo el software proporcionado por Red Hat para Red Hat Enterprise Linux se ofrece como un paquete RPM.

Los archivos de paquetes RPM reciben su nombre de acuerdo con una combinación del paquete **name-version-release.architecture**:



- NAME es una o más palabras que describen los contenidos (httpd-tools).
- VERSION es el número de versión del software original (2.4.6).
- RELEASE es el número de lanzamiento del paquete que se basa en la versión y que es definido por el empaquetador, que es posible que no sea el desarrollador del software original (7.el7).
- ARCH es la arquitectura de procesador en la que se compiló el paquete para su ejecución. "noarch" indica que el contenido de este paquete no es específico de la arquitectura (x86_64).

Cuando se instalan paquetes de repositorios, solo se necesita el nombre de paquete. Se instalará el paquete con la versión superior. Si hay múltiples archivos con la misma versión, se instalará el paquete con el número de lanzamiento superior.

Cada paquete RPM es un fichero especial con tres componentes:

- Los archivos instalados con el paquete.

- Información sobre el paquete (metadatos), como el nombre, la versión, el lanzamiento y la arquitectura; un resumen y una descripción del paquete; determinación de si se necesita instalar otros paquetes; licencias; un registro de cambio del paquete; y otros detalles.
- Scripts que pueden ejecutarse cuando el paquete se instala, actualiza o quita, o que se activan cuando otros paquetes se instalan, actualizan o quitan.

Los paquetes RPM pueden llevar la firma digital de la organización que los colocó en paquete. Todos los paquetes de un origen particular llevan normalmente la firma de la misma clave privada GPG. Si el paquete se modifica o daña, la firma dejará de tener validez. De esta manera, el sistema podrá verificar la integridad de los paquetes antes de instalarlos. Todos los paquetes RPM lanzados por Red Hat llevan firma digital.

Actualizaciones y parches

Cuando Red Hat revisa el código fuente ascendente de un paquete de software, se genera un paquete RPM completo. Si un paquete se añade a un sistema, se necesita solo la última versión del paquete y no cada versión del paquete desde el primer lanzamiento. En el caso de sistemas que necesitan actualizaciones, se quita la versión anterior del paquete y se instala la versión nueva. Los archivos de configuración generalmente se conservan durante una actualización, pero el comportamiento exacto de un paquete en particular se define cuando se crea la nueva versión del paquete.

En la mayoría de los casos, solo una versión o un lanzamiento de un paquete puede instalarse a la vez. Generalmente, el proceso de instalación de RPM no permitirá que los archivos se sobrescriban. Si un paquete se crea de modo que no haya nombres de archivos en conflicto, pueden instalarse múltiples versiones. Este es el caso del paquete **kernel**. Como un kernel nuevo solo puede evaluarse mediante el inicio en ese kernel, el paquete está específicamente diseñado para que puedan instalarse múltiples versiones simultáneamente. Si el kernel nuevo no arranca, el kernel anterior sigue estando disponible.

Administrador de paquetes yum

Una vez instalado el sistema, los paquetes y las actualizaciones de software adicionales normalmente se instalan desde un *repositorio de paquetes* de red, la mayoría de las veces a través del servicio de administración de suscripciones de Red que se abordó en la sección anterior. El comando **rpm** puede utilizarse para instalar, actualizar, quitar y consultar paquetes RPM. Sin embargo, no resuelve dependencias de manera automática y todos los paquetes deben incluirse en una lista. Las herramientas como **PackageKit** y **yum** son aplicaciones front-end para **rpm** y se pueden utilizar para instalar paquetes individuales o *colecciones de paquetes* (a veces denominadas *grupos de paquetes*).

El comando **yum** permite buscar numerosos repositorios de paquetes y sus dependencias para que puedan instalarse de manera conjunta con la finalidad de atenuar los problemas de dependencia. El archivo de configuración principal para **yum** es **/etc/yum.conf** con archivos de configuración de repositorios adicionales ubicados en el directorio **/etc/yum.repos.d**. Los archivos de configuración de repositorio incluyen, como mínimo, una identificación de repositorio (en corchetes), un nombre y la ubicación de la URL del repositorio de paquetes. La URL puede apuntar a un directorio (archivo) local o recurso compartido de red remoto (http, ftp, etc.). Si la URL se pega en un navegador, los contenidos deben incluir los paquetes RPM, posiblemente en uno o más subdirectorios, y un directorio **repodata** con información sobre los paquetes disponibles.

El comando **yum** se utiliza para incluir en una lista repositorios, paquetes y grupos de paquetes:

```
[root@serverX ~]# yum repolist
Loaded plugins: langpacks
repo id          repo name           status
!rhel_dvd        Remote classroom copy of dvd      4,529
repolist: 4,529
[root@serverX ~]# yum list yum*
Loaded plugins: langpacks
Installed Packages
yum.noarch        3.4.3-118.2.el7      @anaconda/7.0
yum-langpacks.noarch 0.4.2-3.el7       @rhel_dvd
yum-metadata-parser.x86_64 1.1.4-10.el7     @anaconda/7.0
yum-rhn-plugin.noarch 2.0.1-4.el7       @rhel_dvd
yum-utils.noarch   1.1.31-24.el7      @rhel_dvd
Available Packages
yum-plugin-aliases.noarch 1.1.31-24.el7     rhel_dvd
yum-plugin-changelog.noarch 1.1.31-24.el7     rhel_dvd
yum-plugin-tmprepo.noarch 1.1.31-24.el7     rhel_dvd
yum-plugin-verify.noarch 1.1.31-24.el7     rhel_dvd
yum-plugin-versionlock.noarch 1.1.31-24.el7     rhel_dvd
[root@serverX ~]# yum list installed
Loaded plugins: langpacks
Installed Packages
GConf2.x86_64      3.2.6-8.el7       @rhel_dvd
ModemManager.x86_64 1.1.0-6.git20130913.el7 @rhel_dvd
ModemManager-glib.x86_64 1.1.0-6.git20130913.el7 @rhel_dvd
...
[root@serverX ~]# yum grouplist
...
Installed groups:
  Base
  Desktop Debugging and Performance Tools
  Dial-up Networking Support
  Fonts
  Input Methods
...
```

Referencias

Páginas del manual **yum(8)**, **yum.conf(5)**, **rpm(8)**, **rpm2cpio(8)** y **rpmkeys(8)**

Práctica: Paquetes de software RPM

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

Arquitectura	Changelog	Firma de GPG	Repositorio
Versión	Versión		

Descripción	Término
La versión de código fuente ascendente	
Lista de motivos para la construcción de cada paquete	
Versión del paquete construido	
Tipo de procesador requerido para un paquete específico	
Recopilación de paquetes RPM y grupos de paquetes	
Usado para verificar el origen y la integridad del paquete	

Solución

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

Descripción	Término
La versión de código fuente ascendente	Versión
Lista de motivos para la construcción de cada paquete	Changelog
Versión del paquete construido	Versión
Tipo de procesador requerido para un paquete específico	Arquitectura
Recopilación de paquetes RPM y grupos de paquetes	Repositorio
Usado para verificar el origen y la integridad del paquete	Firma de GPG

Administración de actualizaciones de software con yum

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder encontrar, instalar y actualizar paquetes de software mediante el uso del comando **yum**.

Trabajar con yum

yum es una herramienta eficaz de la línea de comando que puede usarse para administrar (instalar, actualizar, eliminar y consultar) los paquetes de software de modo más flexible. Los paquetes oficiales de Red Hat se descargan normalmente de la red de distribución de contenido de Red Hat. Si se registra un sistema en el servicio de administración de suscripciones, se configura automáticamente el acceso a los repositorios de software basado en las suscripciones que se adjuntan.

La búsqueda de software con yum

- **yum help** muestra la información de uso.
- **yum list** muestra los paquetes instalados y aquellos disponibles.

```
[root@serverX ~]# yum list 'http*'
Loaded plugins: langpacks
Available Packages
httpcomponents-client.noarch      4.2.5-4.el7          rhel_dvd
httpcomponents-core.noarch        4.2.4-6.el7          rhel_dvd
httpd.x86_64                      2.4.6-17.el7        rhel_dvd
httpd-devel.x86_64                2.4.6-17.el7        rhel_dvd
httpd-manual.noarch                2.4.6-17.el7        rhel_dvd
httpd-tools.x86_64                 2.4.6-17.el7        rhel_dvd
```

- **yum search KEYWORD** enumera paquetes por palabras clave que se encuentran en los campos de nombre y resumen solamente.

Para buscar paquetes que contienen "servidor web" en los campos nombre, resumen y descripción, utilice **search all**:

```
[root@serverX ~]# yum search all 'web server'
Loaded plugins: langpacks
=====
Matched: web server =====
freeradius.x86_64 : High-performance and highly configurable free RADIUS server
hsqldb.noarch : HyperSQL Database Engine
httpd.x86_64 : Apache HTTP Server
libcurl.i686 : A library for getting files from web servers
libcurl.x86_64 : A library for getting files from web servers
mod_revocator.x86_64 : CRL retrieval module for the Apache HTTP server
mod_security.x86_64 : Security module for the Apache HTTP Server
python-paste.noarch : Tools for using a Web Server Gateway Interface stack
```

- **yum info PACKAGE NAME** brinda información detallada sobre un paquete, que incluye el espacio en disco necesario para la instalación.

Capítulo 13. Instalación y actualización de paquetes de software

Para obtener información sobre el servidor HTTP Apache:

```
[root@serverX ~]# yum info httpd
Loaded plugins: langpacks
Available Packages
Name        : httpd
Arch        : x86_64
Version     : 2.4.6
Release     : 17.el7
Size        : 1.1 M
Repo        : rhel_dvd
Summary     : Apache HTTP Server
URL         : http://httpd.apache.org/
License     : ASL 2.0
Description : The Apache HTTP Server is a powerful, efficient, and extensible
              : web server.
```

- **yum provides PATHNAME** muestra paquetes que coinciden con el nombre de ruta especificado (que a menudo, incluye caracteres comodines).

Para encontrar paquetes que proporcionan el directorio **/var/www/html**, utilice lo siguiente:

```
[root@serverX ~]# yum provides /var/www/html
Loaded plugins: langpacks
httpd-2.4.6-17.el7.x86_64 : Apache HTTP Server
Repo       : rhel_dvd
Matched from:
Filename   : /var/www/html

1:php-pear-1.9.4-21.el7.noarch : PHP Extension and Application Repository
                                : framework
Repo       : rhel_dvd
Matched from:
Filename   : /var/www/html
```

Instalación y eliminación de software con yum

- **yum install PACKAGE NAME** obtiene e instala un paquete de software junto con cualquier tipo de dependencia.

```
[root@serverX ~]# yum install httpd
Loaded plugins: langpacks
Resolving Dependencies
--> Running transaction check
--> Package httpd.x86_64 0:2.4.6-17.el7 will be installed
--> Processing Dependency: httpd-tools = 2.4.6-17.el7 for package:
    httpd-2.4.6-17.el7.x86_64
--> Processing Dependency: /etc/mime.types for package: httpd-2.4.6-17.el7.x86_64
--> Processing Dependency: libapr-1.so.0()(64bit) for package:
    httpd-2.4.6-17.el7.x86_64
--> Processing Dependency: libaprutil-1.so.0()(64bit) for package:
    httpd-2.4.6-17.el7.x86_64
--> Running transaction check
--> Package apr.x86_64 0:1.4.8-3.el7 will be installed
--> Package apr-util.x86_64 0:1.5.2-6.el7 will be installed
```

```

--> Package httpd-tools.x86_64 0:2.4.6-17.el7 will be installed
--> Package mailcap.noarch 0:2.1.41-2.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package           Arch      Version       Repository   Size
=====
Installing:
httpd            x86_64    2.4.6-17.el7   rhel_dvd     1.1 M
Installing for dependencies:
apr              x86_64    1.4.8-3.el7    rhel_dvd     100 k
apr-util         x86_64    1.5.2-6.el7    rhel_dvd     90 k
httpd-tools      x86_64    2.4.6-17.el7   rhel_dvd     76 k
mailcap          noarch    2.1.41-2.el7   rhel_dvd     31 k

Transaction Summary
=====
Install 1 Package (+4 Dependent packages)

Total download size: 1.4 M
Installed size: 4.3 M
Is this ok [y/d/N]:
```

- **yum update PACKAGE NAME** obtiene e instala una nueva versión del paquete de software, incluidas las dependencias. Generalmente, el proceso intenta preservar los archivos de configuración, pero en algunos casos, se les cambiará el nombre si el empaquetador considera que el anterior no funcionará después de la actualización. Si no se especifica el PACKAGE NAME, instalará todas las actualizaciones relevantes.

```
[root@serverX ~]# yum update
```

Como un kernel nuevo solo puede evaluarse mediante el inicio en ese kernel, el paquete está específicamente diseñado para que puedan instalarse múltiples versiones simultáneamente. Si el kernel nuevo no arranca, el kernel anterior sigue estando disponible. El uso de **yum update kernel** producirá la *instalación* del kernel nuevo. Los archivos de configuración contienen una lista de paquetes que "siempre deben instalarse" aunque el administrador solicite una actualización.

Capítulo 13. Instalación y actualización de paquetes de software



nota

Utilice **yum list kernel** para detallar todos los núcleos instalados y disponibles. Para ver el kernel en funcionamiento actualmente, utilice el comando **uname**. La opción **-r** mostrará solamente la versión y el lanzamiento del kernel, y la opción **-a** mostrará el lanzamiento e información adicional del kernel.

```
[root@serverX ~]# yum list kernel
Loaded plugins: langpacks
Installed Packages
kernel.x86_64           3.10.0-123.0.1.el7          @anaconda/7.0
kernel.x86_64           3.10.0-84.el7            @rhel-7-server-hbt-
rpms
[root@serverX ~]# uname -r
3.10.0-123.el7.x86_64
[root@serverX ~]# uname -a
Linux demo.example.com 3.10.0-123.el7.x86_64 #1 SMP Tue Nov 26 16:51:22 EST
2013 x86_64 x86_64 x86_64 GNU/Linux
```

- **yum remove PACKAGE NAME** elimina un paquete de software instalado junto con cualquier paquete compatible.

```
[root@serverX ~]# yum remove httpd
```



Advertencia

yum remove quitará los paquetes detallados y *cualquier paquete que requiera los paquetes que se van a quitar* (y los paquetes que requieran esos paquetes, y así sucesivamente). Esto puede dar lugar a una eliminación inesperada de paquetes, por lo que debe verificar detenidamente la lista de paquetes que se quitarán.

Instalación y eliminación de grupos de software con yum

- **yum** también representa el concepto de grupos, que son *colecciones* de software relacionados e instalados en forma conjunta con un fin en particular. En Red Hat Enterprise Linux 7, hay dos tipos de grupos. Los grupos regulares son colecciones de paquetes. *Los grupos de entorno* son colecciones de otros grupos que incluyen sus propios paquetes. Puede que los paquetes o grupos provistos por un grupo sean *obligatorios* (se deben instalar si el grupo está instalado), *predeterminados* (generalmente se instalan si el grupo está instalado) u *opcionales* (no se instalan donde se encuentra el grupo, a menos que se solicite en forma específica).

Al igual que **yum list**, el comando **yum group list** (o **yum grouplist**) mostrará los nombres de grupos instalados o disponibles. Algunos grupos se instalan normalmente a través de grupos de entorno y se ocultan de manera predeterminada. Los grupos ocultos también pueden enumerarse con el comando **yum group list hidden**. Si se añade la opción **ids**, también se mostrará la ID del grupo. Los grupos pueden instalarse, actualizarse, removverse o consultarse, por nombre o ID.

```
[root@serverX ~]# yum group list
Loaded plugins: langpacks
Available environment groups:
Minimal install
Infrastructure Server
File and Print Server
Web Server
Virtualization Host
Server with GUI
Installed groups:
Base
Desktop Debugging and Performance Tools
Dial-up Networking Support
Fonts
Input Methods
Internet Browser
PostgreSQL Database server
Printing client
X Window System
Available Groups:
Additional Development
Backup Client
Backup Server
...
...
```

- La información sobre un grupo se muestra con **yum group info** (o con **yum groupinfo**). Incluye una lista de ID de grupos o nombres de paquetes obligatorios, predeterminados u opcionales. Los ID de grupos o los nombres de paquetes pueden tener un marcador al inicio.

Marcador	Significado
=	El paquete está instalado o fue instalado como parte del grupo.
+	El paquete no está instalado, se instalará si el grupo está instalado o actualizado.
-	El paquete no está instalado, no se instalará si el grupo está instalado o actualizado.
<i>Sin marcador</i>	El paquete está instalado, pero no se instaló a través del grupo.

```
[root@serverX ~]# yum group info "Identity Management Server"
Loaded plugins: langpacks

Group: Identity Management Server
Group-Id: identity-management-server
Description: Centralized management of users, servers and authentication policies.
Default Packages:
+389-ds-base
+ipa-admintools
+ipa-server
+pki-ca
Optional Packages:
+ipa-server-trust-ad
+nuxwdog
+slapi-nis
```

Capítulo 13. Instalación y actualización de paquetes de software

- El comando **yum group install** (o **yum groupinstall**) instalará un grupo que instalará sus paquetes obligatorios y predeterminados, y los paquetes de los que depende.

```
[root@serverX ~]# yum group install "Infiniband Support"
...
Transaction Summary
=====
Install 17 Packages (+7 Dependent packages)

Total download size: 9.0 M
Installed size: 33 M
Is this ok [y/d/N]:
...
```



Importante

En comparación con Red Hat Enterprise Linux 6 y con versiones anteriores, el comportamiento de los grupos **yum** ha cambiado en Red Hat Enterprise Linux 7. En RHEL 7, los grupos se tratan como *objetos* y son rastreados por el sistema. Si un grupo instalado se actualiza y el repositorio **yum** ha añadido paquetes nuevos obligatorios o predeterminados al grupo, dichos paquetes nuevos se instalarán en la actualización.

RHEL 6 y las versiones anteriores consideran la instalación de un grupo si todos sus paquetes obligatorios han sido instalados; o, en caso de que no tenga ningún paquete obligatorio, si ningún paquete predeterminado u opcional en el grupo se instaló. En RHEL 7, se considera la instalación de un grupo solo si **yum group install** se utilizó para su instalación. Como comando nuevo en RHEL 7, **yum group mark install GROUPNAME** puede utilizarse para marcar un grupo como instalado, y los paquetes faltantes y sus dependencias se instalarán en la próxima actualización.

Finalmente, RHEL 6 y las versiones anteriores no tenían la forma de dos palabras de los comandos **yum group**. Es decir que, en RHEL 6, el comando **yum grouplist** existía, pero el comando equivalente en RHEL 7 **yum group list** no.

Visualización del historial de transacciones

- Todas las transacciones de instalación y eliminación se registran en **/var/log/yum.log**.

```
[root@serverX ~]# tail -5 /var/log/yum.log
Feb 16 14:10:41 Installed: libnes-1.1.3-5.el7.x86_64
Feb 16 14:10:42 Installed: libmthca-1.0.6-10.el7.x86_64
Feb 16 14:10:43 Installed: libmlx4-1.0.5-7.el7.x86_64
Feb 16 14:10:43 Installed: libibcm-1.0.5-8.el7.x86_64
Feb 16 14:10:45 Installed: rdma-7.0_3.13_rc8-3.el7.noarch
```

- Un resumen de las transacciones de instalación y eliminación puede visualizarse con **yum history**.

YUM HISTORY				
ID	Login user	Date and time	Action(s)	Altered

history list				
6	Student User <student>	2014-02-16 14:09	Install	25
5	Student User <student>	2014-02-16 14:01	Install	1
4	System <unset>	2014-02-08 22:33	Install	1112 EE
3	System <unset>	2013-12-16 13:13	Erase	4
2	System <unset>	2013-12-16 13:13	Erase	1
1	System <unset>	2013-12-16 13:08	Install	266

- Una transacción puede anularse con las opciones **history undo**:

```
[root@serverX ~]# yum history undo 6
Loaded plugins: langpacks
Undoing transaction 6, from Sun Feb 16 14:09:51 2014
Install    dapl-2.0.39-2.el7.x86_64          @rhel-7-server-htb-rpms
Dep-Install graphviz-2.30.1-18.el7.x86_64   @rhel-7-server-htb-rpms
Dep-Install graphviz-tcl-2.30.1-18.el7.x86_64 @rhel-7-server-htb-rpms
Install    ibacm-1.0.8-4.el7.x86_64          @rhel-7-server-htb-rpms
Install    ibutils-1.5.7-9.el7.x86_64         @rhel-7-server-htb-rpms
Dep-Install ibutils-libs-1.5.7-9.el7.x86_64   @rhel-7-server-htb-rpms
...
...
```

Resumen de los comandos yum

Los paquetes pueden ubicarse, instalarse, actualizarse y eliminarse por nombre o por grupos de paquetes.

Tarea:	Comando:
Enumerar paquetes instalados y disponibles por nombre	yum list [NAME-PATTERN]
Enumerar grupos instalados y disponibles	yum grouplist
Buscar un paquete por palabra clave	yum search KEYWORD
Mostrar detalles de un paquete	yum info PACKAGE_NAME
Instalar un paquete	yum install PACKAGE_NAME
Instalar un grupo de paquetes	yum groupinstall "GROUPNAME"
Actualizar todos los paquetes	yum update
Eliminar un paquete	yum remove PACKAGE_NAME
Mostrar historial de transacciones	yum history



Referencias

Páginas del manual: **yum(1)**, **yum.conf(5)**

Puede encontrar información adicional sobre **yum** disponible en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Práctica: Instalación y actualización de software con yum

En este ejercicio de laboratorio, instalará y quitará paquetes y grupos de paquetes.

Resultados:

Explore cómo instalar y quitar paquetes con dependencias.

Antes de comenzar

Restablezca su sistema serverX.

1. Busque un paquete específico.

- 1.1. Intente ejecutar el comando **gnuplot**. Se le indicará que no está instalado.

```
[root@serverX ~]# gnuplot
bash: gnuplot: command not found...
```

- 1.2. Busque paquetes de trazado.

```
[root@serverX ~]# yum search plot
Loaded plugins: langpacks
=====
emacs-gnuplot.noarch : Emacs bindings for the gnuplot main application
gnuplot.x86_64 : A program for plotting mathematical expressions and data
gnuplot-common.x86_64 : The common gnuplot parts
python-matplotlib.x86_64 : Python 2D plotting library
texlive-pst-plot.noarch : Plot data using PStricks

Name and summary matches only, use "search all" for everything.
```

- 1.3. Obtenga más información sobre el paquete **gnuplot**.

```
[root@serverX ~]# yum info gnuplot
Name        : gnuplot
Arch       : x86_64
...
```

2. Instale el paquete **gnuplot**.

```
[root@serverX ~]# yum install -y gnuplot
...
Dependencies Resolved

=====
Package      Arch      Version      Repository      Size
=====
Installing:
  gnuplot      x86_64    4.6.2-3.el7   rhel_dvd      645 k
Installing for dependencies:
  gnuplot-common x86_64    4.6.2-3.el7   rhel_dvd      595 k

Transaction Summary
```

```
=====
Install 1 Package (+1 Dependent package)
...
```

3. Quite paquetes.

- 3.1. Intente quitar el paquete **gnuplot**, pero seleccione "no". ¿Cuántos paquetes se quitarán?

```
[root@serverX ~]# yum remove gnuplot
...
Removing:
gnuplot           x86_64      4.6.2-3.el7      @rhel_dvd      1.5 M
Transaction Summary
=====
Remove 1 Package

Installed size: 1.5 M
Is this ok [y/N]: n
```

- 3.2. Intente quitar el paquete **gnuplot-common**, pero seleccione "no". ¿Cuántos paquetes se quitarán?

```
[root@serverX ~]# yum remove gnuplot-common
...
Removing:
gnuplot-common     x86_64      4.6.2-3.el7      @rhel_dvd      1.4 M
Removing for dependencies:
gnuplot           x86_64      4.6.2-3.el7      @rhel_dvd      1.5 M
Transaction Summary
=====
Remove 1 Package (+1 Dependent package)

Installed size: 2.9 M
Is this ok [y/N]: n
```

4. Reúna información sobre el grupo de componentes "Compatibility Libraries" e instálelo en serverX.

- 4.1. Enumere todos los grupos de componentes disponibles.

```
[root@serverX ~]# yum grouplist
```

- 4.2. Obtenga más información acerca del grupo de componentes *Compatibility Libraries*, incluida una lista de los paquetes comprendidos.

```
[root@serverX ~]# yum groupinfo "Compatibility Libraries"
Loaded plugins: langpacks

Group: Compatibility Libraries
Group-Id: compat-libraries
Description: Compatibility libraries for applications built on previous
versions of Red Hat Enterprise Linux.
```

Capítulo 13. Instalación y actualización de paquetes de software

```
Mandatory Packages:
+compat-db47
+compat-glibc
+compat-libcap1
+compat-libf2c-34
+compat-libgfortran-41
+compat-libtiff3
+compat-openldap
+libpng12
+openssl098e
```

4.3. Instale el grupo de componentes *Compatibility Libraries*.

```
[root@serverX ~]# yum groupinstall "Compatibility Libraries"
Loaded plugins: langpacks
Resolving Dependencies
--> Running transaction check
---> Package compat-db47.x86_64 0:4.7.25-27.el7 will be installed
--> Processing Dependency: compat-db-headers = 4.7.25-27.el7 for package:
    compat-db47-4.7.25-27.el7.x86_64
...
Dependencies Resolved

=====
Package           Arch      Version       Repository
=====
Installing for group install "Compatibility Libraries":
compat-db47      x86_64   4.7.25-27.el7   rhel_dvd
libpng12         x86_64   1.2.50-6.el7   rhel_dvd
...
Installing for dependencies:
compat-db-headers noarch   4.7.25-27.el7   rhel_dvd
...

Transaction Summary
=====
Install 9 Packages (+3 Dependent packages)

Total download size: 5.5 M
Installed size: 21 M
Is this ok [y/d/N]: y
...
Installed:
  compat-db47.x86_64 0:4.7.25-27.el7
  compat-glibc.x86_64 1:2.12-4.el7
...

Dependency Installed:
  compat-db-headers.noarch 0:4.7.25-27.el7
  compat-glibc-headers.x86_64 1:2.12-4.el7

Complete!
```

5. Explore el historial y las opciones de anulación de **yum**.

5.1. Visualice el historial reciente de **yum**.

```
[root@serverX ~]# yum history
Loaded plugins: langpacks
ID      | Login user      | Date and time      | Action(s)      | Altered
-----
```

3 root <root>	2014-06-05 09:33	Install	12
2 root <root>	2014-06-05 09:30	Install	2
1 System <unset>	2014-06-02 20:27	Install	1112 EE
history list			

5.2. Confirme que la última transacción sea la instalación del grupo.

```
[root@serverX ~]# yum history info 3
Loaded plugins: langpacks
Transaction ID : 3
Begin time     : Thu Jun  5 09:33:19 2014
Begin rpmdb    : 1210:7c6b529424621773d5fe147315a53d558f726814
End time       :          09:33:40 2014 (21 seconds)
End rpmdb      : 1222:c283bc776b18b9578b87cdec68853f49b31ca0cc
User          : root <root>
Return-Code    : Success
Command Line   : groupinstall Compatibility Libraries
Transaction performed with:
  Installed    rpm-4.11.1-16.el7.x86_64 installed
  Installed    yum-3.4.3-117.el7.noarch installed
Packages Altered:
  Dep-Install  compat-db-headers-4.7.25-27.el7.noarch      @rhel_dvd
  Install      compat-db47-4.7.25-27.el7.x86_64            @rhel_dvd
...
history info
```

5.3. Utilice las opciones de anulación para quitar el último conjunto de paquetes instalado.

```
[root@serverX ~]# yum history undo 3
```

Habilitación de repositorios de software yum

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder habilitar e inhabilitar el uso del repositorio yum de Red Hat o de terceros.

Habilitación de repositorios de software de Red Hat

Si se registra un sistema en el servicio de administración de suscripciones, se configura automáticamente el acceso a los repositorios de software basado en las suscripciones que se adjuntan. Para ver todos los repositorios disponibles:

```
[root@serverX ~]# yum repolist all
Loaded plugins: langpacks
repo id                                repo name
status
rhel-7-server-debug-rpms/7Server/x86_64   Red Hat Enterprise Linux 7 Server (Debug
                                           RPMs)    disabled
rhel-7-server-rpms/7Server/x86_64          Red Hat Enterprise Linux 7 Server (RPMS)
                                           enabled: 5,071
rhel-7-server-source-rpms/7Server/x86_64   Red Hat Enterprise Linux 7 Server (Source
                                           RPMs)    disabled
repolist: 5,071
```

Habilite o inhabilite los repositorios con **yum-config-manager**. Esta acción cambiará el parámetro **habilitado** en el archivo **/etc/yum.repos.d/redhat.repo**.

```
[root@serverX ~]# yum-config-manager --enable rhel-7-server-debug-rpms
Loaded plugins: langpacks
=====
repo: rhel-7-server-debug-rpms
[reli-7-server-debug-rpms]
async = True
bandwidth = 0
base_persistdir = /var/lib/yum/repos/x86_64/7Server
baseurl = https://cdn.redhat.com/content/dist/rhel/server/7/7Server/x86_64/debug
cache = 0
cachedir = /var/cache/yum/x86_64/7Server/rhel-7-server-debug-rpms
check_config_file_age = True
cost = 1000
deltarpm_percentage =
enabled = 1
...
```

Habilitación de repositorios de software de terceros

Los repositorios de terceros son directorios de archivos de paquete de software provistos por una fuente que no es Red Hat y a la que se puede acceder mediante **yum** desde un sitio web, servidor FTP o sistema de archivos local. Los repositorios yum son utilizados por distribuidores de software diferentes a Red Hat, o se usan para pequeñas colecciones de paquetes locales. (Por ejemplo, Adobe ofrece parte de su software gratuito para Linux a través de un repositorio yum). El servidor del aula **content.example.com** aloja repositorios yum para esta clase.

Coloque un archivo en el directorio **/etc/yum.repos.d/** para habilitar el soporte para un nuevo repositorio de terceros. Los archivos de configuración de repositorio deben finalizar

en **.repo**. La definición de repositorio contiene la URL del repositorio, un nombre, si se debe usar GPG para comprobar las firmas del paquete y, en ese caso, la URL que apunta a la clave GPG de confianza.

Con **yum-config-manager**

Si se conoce la URL para el repositorio yum, puede crearse un archivo de configuración con **yum-config-manager**.

```
[root@serverX ~]# yum-config-manager --add-repo="http://dl.fedoraproject.org/pub/epel/7/x86_64/"
Loaded plugins: langpacks
adding repo from: http://dl.fedoraproject.org/pub/epel/7/x86_64/
[dl.fedoraproject.org_pub_epel_7_x86_64_]
name=added from: http://dl.fedoraproject.org/pub/epel/7/x86_64/
baseurl=http://dl.fedoraproject.org/pub/epel/7/x86_64/
enabled=1
```

Se creó un archivo en el directorio **/etc/yum.repos.d** con el resultado que se muestra. Este archivo ahora puede modificarse para proporcionar un nombre personalizado y la ubicación de la clave GPG. Los administradores deberían descargar la llave en un archivo local en lugar de permitir que **yum** la recupere de una fuente externa.

```
[EPEL]
name=EPEL 7
baseurl=http://dl.fedoraproject.org/pub/epel/7/x86_64/
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
```

Paquete de configuración de RPM para el repositorio

Algunos repositorios proporcionan este archivo de configuración y la clave pública de GPG como parte del paquete de RPM que puede descargarse e instalarse con **yum localinstall**. Un ejemplo de esto es el proyecto voluntario de Paquetes extra para Enterprise Linux (EPEL), que proporciona software no admitido por Red Hat, pero que es compatible con Red Hat Enterprise Linux.

Instalación del paquete de repositorio EPEL de Red Hat Enterprise Linux 7:

```
[root@serverX ~]# rpm --import http://dl.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL-7
[root@serverX ~]# yum install http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-2.noarch.rpm
```

A menudo, los archivos de configuración enumeran varias referencias de repositorio en un solo archivo. Cada referencia de repositorio comienza con un nombre de una sola palabra entre corchetes.

```
[root@serverX ~]# cat /etc/yum.repos.d/epel.repo
[epel]
name=Extra Packages for Enterprise Linux 7 - $basearch
#baseurl=http://download.fedoraproject.org/pub/epel/7/$basearch
mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=epel-7&arch=$basearch
failovermethod=priority
enabled=1
gpgcheck=0
```

```
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7

[epel-debuginfo]
name=Extra Packages for Enterprise Linux 7 - $basearch - Debug
#baseurl=http://download.fedoraproject.org/pub/epel/7/$basearch/debug
mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=epel-debug-7&arch=$basearch
failovermethod=priority
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
gpgcheck=1

[epel-source]
name=Extra Packages for Enterprise Linux 7 - $basearch - Source
#baseurl=http://download.fedoraproject.org/pub/epel/7/SRPMS
mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=epel-source-7&arch=$basearch
failovermethod=priority
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
gpgcheck=1
```

El parámetro **habilitado=0** puede incluirse de manera que se defina un repositorio, pero no se busque de manera predeterminada. Los repositorios pueden habilitarse o inhabilitarse en forma persistente con **yum-config-manager** o en forma provisoria con las opciones **--enablerepo=PATTERN** y **--disablerepo=PATTERN** en **yum**.



Advertencia

Antes de instalar los paquetes firmados, instale la clave GPG de RPM. Esta acción verificará que los paquetes pertenezcan a una clave que se haya importado.

De lo contrario, **yum** le advertirá que le falta la clave. (La opción **--nogpgcheck** puede usarse para omitir las claves GPG faltantes, pero esto podría provocar que se instalen paquetes adulterados o dudosos en el sistema y que, posiblemente, comprometan la seguridad).



Referencias

Es posible encontrar información adicional en la sección sobre la configuración de yum y repositorios yum en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Páginas del manual: **yum(5)**, **yum.conf(1)**, **yum-config-manager(1)**

Práctica: Habilitar repositorios de software

En este laboratorio, configurará su servidor para usar un repositorio **yum** separado a fin de obtener actualizaciones y desactualizar su equipo.

Resultados:

El sistema estará configurado para obtener actualizaciones de software de un servidor del aula y utilizará el último kernel de Linux.

Andes de comenzar

Restablezca su sistema serverX.

- Configure el sistema para obtener software de dos repositorios del aula.
 - Paquetes del aula proporcionados en http://content.example.com/rhel7.0/x86_64/rht
 - Actualizaciones proporcionadas en http://content.example.com/rhel7.0/x86_64/errata
- Utilice **yum-config-manager** para añadir el repositorio de paquetes del aula.

```
[root@serverX ~]# yum-config-manager --add-repo="http://content.example.com/rhel7.0/x86_64/rht"
Loaded plugins: langpacks
adding repo from: http://content.example.com/rhel7.0/x86_64/rht

[content.example.com_rhel7.0_x86_64_rht]
name=added from: http://content.example.com/rhel7.0/x86_64/rht
baseurl=http://content.example.com/rhel7.0/x86_64/rht
enabled=1
```

- Cree el archivo **/etc/yum.repos.d/errata.repo** para habilitar el repositorio "Actualizaciones" con el siguiente contenido:

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

- Utilice **yum-config-manager** para deshabilitar el repositorio de paquetes del aula.

```
[root@serverX ~]# yum-config-manager --disable
content.example.com_rhel7.0_x86_64_rht
Loaded plugins: langpacks
===== repo: content.example.com_rhel7.0_x86_64_rht =====
[content.example.com_rhel7.0_x86_64_rht]
...
enabled = 0
...
```

- Actualice todo el software relevante proporcionado mediante el uso de **yum update**.

```
[root@serverX ~]# yum update -y
```

Capítulo 13. Instalación y actualización de paquetes de software

4. Verifique que haya dos versiones de kernel instaladas. ¿Qué versión está actualmente en uso?

```
[root@serverX ~]# yum list kernel  
[root@serverX ~]# uname -r
```

5. Reinicie serverX y, luego, repita el paso anterior. ¿Qué versión está actualmente en uso?

```
[root@serverX ~]# yum list kernel  
[root@serverX ~]# uname -r
```

6. Indique el paquete **rht-system** y, luego, instálelo.

```
[root@serverX ~]# yum list rht*  
Loaded plugins: langpacks  
Available Packages  
rht-system.noarch 1.0.0-2.el7 updates  
[root@serverX ~]# yum -y install rht-system  
Loaded plugins: langpacks  
Resolving Dependencies  
...
```

Análisis de los archivos del paquete RPM

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder analizar e instalar los archivos de paquete descargados.

Análisis de paquetes descargados con rpm

La utilidad **rpm** es una herramienta de nivel bajo que es útil para obtener información acerca del contenido de los archivos de paquete y los paquetes instalados. Obtiene su información desde una base de datos local o de los propios archivos del paquete.

La forma general de una consulta es:

- **rpm -q [select-options] [query-options]**
- **rpm --query [select-options] [query-options]**

Consultas RPM: opciones de selección

- **-q -a**: todos los paquetes instalados
- **-q PACKAGE NAME**: PACKAGE NAME actualmente instalado

```
[root@serverX ~]# rpm -q yum
yum-3.4.3-118.el7.noarch
```

- **-q -p PACKAGEFILE.rpm**: archivo de paquete con el nombre PACKAGEFILE.rpm

```
[root@serverX ~]# rpm -q -p http://content.example.com/rhel7.0/x86_64/dvd/Packages/
yum-utils-1.1.31-24.el7.noarch.rpm
yum-utils-1.1.31-24.el7.noarch.rpm
```

- **-q -f FILENAME**: qué paquete proporciona el FILENAME

```
[root@serverX ~]# rpm -q -f /etc/yum.repos.d
yum-3.4.3-118.el7.noarch
```

Consultas de RPM: información sobre el contenido de los paquetes

- **-q**: especifica el nombre y la versión del paquete; comparar con **yum list**
- **-q -i**: información sobre el paquete; comparar con **yum info**
- **-q -l**: enumera los archivos instalados por el paquete especificado

```
[root@serverX ~]# rpm -q -l yum-rhn-plugin
/etc/yum/pluginconf.d/rhnplugin.conf
/usr/share/doc/yum-rhn-plugin-2.0.1
/usr/share/doc/yum-rhn-plugin-2.0.1/LICENSE
/usr/share/locale/af/LC_MESSAGES/yum-rhn-plugin.mo
```

Capítulo 13. Instalación y actualización de paquetes de software

...

- **-q -c**: enumera sólo los archivos de configuración

```
[root@serverX ~]# rpm -q -c yum-rhn-plugin
/etc/yum/pluginconf.d/rhnplugin.conf
```

- **-q -d**: enumera sólo los archivos de documentación

```
[root@serverX ~]# rpm -q -d yum-rhn-plugin
/usr/share/doc/yum-rhn-plugin-2.0.1/LICENSE
/usr/share/man/man5/rhnplugin.conf.5.gz
/usr/share/man/man8/rhnplugin.8.gz
/usr/share/man/man8/yum-rhn-plugin.8.gz
```

- **-q --scripts**: enumera los scripts de la shell que pueden ejecutarse una vez que se instaló o eliminó el paquete

```
[root@serverX ~]# rpm -q --scripts openssh-server
preinstall scriptlet (using /bin/sh):
getent group sshd >/dev/null || groupadd -g 74 -r sshd || :
getent passwd sshd >/dev/null || \
    useradd -c "Privilege-separated SSH" -u 74 -g sshd \
    -s /sbin/nologin -r -d /var/empty/sshd sshd 2> /dev/null || :
postinstall scriptlet (using /bin/sh):

if [ $1 -eq 1 ] ; then
    # Initial installation
    /usr/bin/systemctl preset sshd.service sshd.socket >/dev/null 2>&1 || :
fi
preuninstall scriptlet (using /bin/sh):

if [ $1 -eq 0 ] ; then
    # Package removal, not upgrade
    /usr/bin/systemctl --no-reload disable sshd.service sshd.socket > /dev/null
    2>&1 || :
    /usr/bin/systemctl stop sshd.service sshd.socket > /dev/null 2>&1 || :
fi
postuninstall scriptlet (using /bin/sh):

/usr/bin/systemctl daemon-reload >/dev/null 2>&1 || :
if [ $1 -ge 1 ] ; then
    # Package upgrade, not uninstall
    /usr/bin/systemctl try-restart sshd.service >/dev/null 2>&1 || :
fi
```

- **-q --changelog**: enumera la información de cambios para el paquete

```
[root@serverX ~]# rpm -q --changelog audit
* Thu Oct 03 2013 Steve Grubb <sgrubb@redhat.com> 2.3.2-3
  resolves: #828495 - semanage port should generate an audit event

* Thu Aug 29 2013 Steve Grubb <sgrubb@redhat.com> 2.3.2-2
  resolves: #991056 - ausearch ignores USER events with -ua option
  ...
```

Consulta de archivos de paquete:

```
[root@serverX ~]# wget http://classroom/pub/materials/wonderwidgets-1.0-4.x86_64.rpm
[root@serverX ~]# rpm -q -l -p wonderwidgets-1.0-4.x86_64.rpm
/etc/wonderwidgets.conf
/usr/bin/wonderwidgets
/usr/share/doc/wonderwidgets-1.0
/usr/share/doc/wonderwidgets-1.0/README.txt
```



nota

El comando **repoquery** también puede usarse para obtener información sobre paquetes y sus contenidos. La diferencia con **rpm** es que busca esa información en los repositorios yum, en lugar de hacerlo en la base de datos local de los paquetes instalados.

Uso de **yum** para instalar archivos de paquete locales

El comando **yum localinstall PACKAGEFILE.rpm** se puede usar para instalar los archivos de paquetes de manera directa. Automáticamente, descarga todas las dependencias que tiene el paquete desde cualquier repositorio **yum** configurado.

```
[root@serverX ~]# yum localinstall wonderwidgets-1.0-4.x86_64.rpm
[root@serverX ~]# rpm -q wonderwidgets
wonderwidgets-1.0-4.x86_64
```



nota

rpm -ivh PACKAGEFILE.rpm también se puede usar para instalar archivos de paquete. Sin embargo, el uso de **yum** ayuda a mantener un historial de transacciones que conserva **yum** (consulte **yum history**).



Advertencia

Tenga cuidado al instalar paquetes de terceros, no solo por el software que pueden instalar, sino también porque el RPM puede ejecutar scripts arbitrarios como usuario **root** durante el proceso de instalación.

Extracción de archivos de los paquetes RPM

Los archivos del paquete RPM pueden extraerse sin instalar el paquete con **cpio**, que es una herramienta para archivar, como **zip** o **tar**. Canalice los resultados de **rpm2cpio PACKAGEFILE.rpm** en **cpio -id** y extraerá todos los archivos almacenados en el paquete RPM. Se crearán árboles de subdirectorio, según sea necesario, con respecto al directorio de trabajo actual.

Seleccione los archivos que también puedan extraerse mediante la especificación de la ruta del archivo:

```
[root@serverX ~]# rpm2cpio wonderwidgets-1.0-4.x86_64.rpm | cpio -id "*txt"
11 blocks
[root@serverX ~]# ls -l usr/share/doc/wonderwidgets-1.0/
total 4
-rw-r--r--. 1 root root 76 Feb 13 19:27 README.txt
```

Resumen de los comandos de consulta **rpm**

Los paquetes instalados pueden consultarse directamente con el comando **rpm**. Agregue la opción **-p** para consultar un archivo de paquete antes de la instalación.

Tarea:	Comando:
Muestra información sobre el paquete.	rpm -q -i NAME
Enumera todos los archivos que están incluidos en el paquete.	rpm -q -l NAME
Enumera los archivos de configuración incluidos en un paquete.	rpm -q -c NAME
Enumera los archivos de documentación incluidos en un paquete.	rpm -q -d NAME
Muestra un resumen breve del motivo de lanzamiento del paquete nuevo.	rpm -q --changelog NAME
Muestra la secuencia de comandos de shell incluida en un paquete.	rpm -q --scripts NAME

Referencias

Páginas del manual **yum(8)**, **rpm(8)**, **repoquery(1)**, **rpm2cpio(8)** y **cpio(1)**

Práctica: Trabajar con los archivos de paquete del RPM

En este ejercicio de laboratorio, recopilará información sobre un paquete de terceros, extraerá los archivos que contiene y los instalará en el sistema serverX.

Resultados:

Se instaló en el sistema un paquete no provisto por un repositorio yum.

Andes de comenzar

Restablezca su sistema serverX.

1. Descargue *wonderwidgets-1.0-4.x86_64.rpm* de <http://classroom/pub/materials>.

```
[root@serverX ~]# wget http://classroom/pub/materials/wonderwidgets-1.0-4.x86_64.rpm
--2014-02-11 15:58:02--  http://classroom/pub/materials/
wonderwidgets-1.0-4.x86_64.rpm
Resolving classroom (classroom)... 172.25.0.254
Connecting to classroom (classroom)|172.25.0.254|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5000 (4.9K) [application/x-rpm]
Saving to: 'wonderwidgets-1.0-4.x86_64.rpm'

100%[=====] 5,000      --.-K/s   in 0s

2014-02-11 15:58:02 (381 MB/s) - 'wonderwidgets-1.0-4.x86_64.rpm' saved [5000/5000]
```

2. ¿Qué archivos contiene?

```
[root@serverX ~]# rpm -q -p wonderwidgets-1.0-4.x86_64.rpm -1
/etc/wonderwidgets.conf
/usr/bin/wonderwidgets
/usr/share/doc/wonderwidgets-1.0
/usr/share/doc/wonderwidgets-1.0/README.txt
```

3. ¿Qué scripts contiene?

```
[root@serverX ~]# rpm -q -p wonderwidgets-1.0-4.x86_64.rpm --scripts
```

4. ¿Cuánto espacio en disco usará al instalarlo?

```
[root@serverX ~]# rpm -q -p wonderwidgets-1.0-4.x86_64.rpm -i
Name        : wonderwidgets
Version     : 1.0
Release    : 4
Architecture: x86_64
Install Date: (not installed)
Group       : GLS/Applications
Size : 4849
License     : GPL
Signature   : (none)
Source RPM  : wonderwidgets-1.0-4.src.rpm
```

Capítulo 13. Instalación y actualización de paquetes de software

```
Build Date : Fri 03 Dec 2010 05:42:55 AM EST
Build Host : station166.rosemont.lan
Relocations : (not relocatable)
Vendor : Red Hat, Inc.
Summary : Demonstration package for use in GLS training.
Description :
A demonstration package that installs an executable, and a config file.
```

5. Use **yum localinstall** para instalar el paquete.

```
[root@serverX ~]# yum localinstall wonderwidgets-1.0-4.x86_64.rpm
Loaded plugins: langpacks
Examining wonderwidgets-1.0-4.x86_64.rpm: wonderwidgets-1.0-4.x86_64
Marking wonderwidgets-1.0-4.x86_64.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package wonderwidgets.x86_64 0:1.0-4 will be installed
---> Finished Dependency Resolution

Dependencies Resolved

=====
Package      Arch      Version   Repository      Size
=====
Installing:
wonderwidgets    x86_64    1.0-4        /wonderwidgets-1.0-4.x86_64  4.7 k

Transaction Summary
=====
Install 1 Package

Total size: 4.7 k
Installed size: 4.7 k
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : wonderwidgets-1.0-4.x86_64                               1/1
  Verifying  : wonderwidgets-1.0-4.x86_64                               1/1

Installed:
  wonderwidgets.x86_64 0:1.0-4

Complete!
```

Ejercicio de laboratorio: Instalación y actualización de paquetes de software

En este ejercicio de laboratorio, instalará y actualizará paquetes de software seleccionados.

Resultados:

Los paquetes nuevos y actualizados están instalados en el sistema.

Antes de comenzar

Restablezca su sistema serverX.

1. Cree el archivo **/etc/yum.repos.d/errata.repo** para habilitar el repositorio "Actualizaciones" que se encuentra en la máquina content. Este debe acceder al contenido que se encuentra en la siguiente URL: **http://&cntfqdn;/rhel7.0/x86_64/errata**. No controle las firmas de GPG.
2. Configure serverX para que respete cada requisito de software específico. Debe tener instaladas las versiones más recientes de los siguientes paquetes. No instale todas las actualizaciones. Instale solamente las actualizaciones para los paquetes enumerados, si están disponibles.
 - 2.1. **kernel** (paquete existente con una actualización)
 - 2.2. **xsane-gimp** (nuevo paquete)
 - 2.3. **rht-system** (paquete nuevo)
3. Por razones de seguridad, no debe tener instalado el paquete **wvdial**.
4. Cuando esté listo para revisar su trabajo, ejecute **lab software grade** en serverX.

Capítulo 13. Instalación y actualización de paquetes de software

Solución

En este ejercicio de laboratorio, instalará y actualizará paquetes de software seleccionados.

Resultados:

Los paquetes nuevos y actualizados están instalados en el sistema.

Antes de comenzar

Restablezca su sistema serverX.

1. Cree el archivo **/etc/yum.repos.d/errata.repo** para habilitar el repositorio "Actualizaciones" que se encuentra en la máquina content. Este debe acceder al contenido que se encuentra en la siguiente URL: http://&cntfqdn;/rhel7.0/x86_64/errata. No controle las firmas de GPG.

Cree el archivo **/etc/yum.repos.d/errata.repo** con el siguiente contenido:

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

2. Configure serverX para que respete cada requisito de software específico. Debe tener instaladas las versiones más recientes de los siguientes paquetes. No instale todas las actualizaciones. Instale solamente las actualizaciones para los paquetes enumerados, si están disponibles.

2.1. **kernel** (paquete existente con una actualización)

```
yum update kernel
```

2.2. **xsane-gimp** (nuevo paquete)

```
yum install xsane-gimp
```

2.3. **rht-system** (paquete nuevo)

```
yum install rht-system
```

3. Por razones de seguridad, no debe tener instalado el paquete **wvdial**.

```
yum remove wvdial
```

4. Cuando esté listo para revisar su trabajo, ejecute **lab software grade** en serverX.

```
[student@serverX ~]$ lab software grade
```

Resumen

Adjuntar sistemas a las suscripciones para actualizaciones de software

El registro de sistemas permite el acceso a actualizaciones de software para productos instalados.

Paquetes de software RPM y yum

Los paquetes RPM, que se agrupan en repositorios yum, proporcionan un método uniforme para realizar el seguimiento de instalaciones y actualizaciones de software.

Administración de actualizaciones de software con yum

`yum` se utiliza para instalar y actualizar paquetes de software.

Habilitación de repositorios de software yum

Los repositorios para `yum` se configuran en el directorio `/etc/yum.repos.d`.

Análisis de los archivos del paquete RPM

Los paquetes descargados fuera de los repositorios yum pueden ser consultados e instalados con `rpm`.



CAPÍTULO 14

ACCESO A LOS SISTEMAS DE ARCHIVOS DE LINUX

Descripción general	
Meta	Acceder a sistemas de archivos existentes y examinarlos en un sistema con Red Hat Enterprise Linux.
Objetivos	<ul style="list-style-type: none">Identificar la jerarquía del sistema de archivos.Acceder al contenido de los sistemas de archivos.Usar enlaces duros y enlaces simbólicos para crear múltiples nombres.Buscar archivos en sistemas de archivos montados.
Secciones	<ul style="list-style-type: none">Identificación de dispositivos y sistemas de archivos (y práctica)Montaje y desmontaje de sistemas de archivos (y práctica)Creación de enlaces entre archivos (y práctica)Búsqueda de archivos en el sistema (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">Acceso a los sistemas de archivos de Linux

Identificación de dispositivos y sistemas de archivos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder identificar un directorio en la jerarquía de sistemas de archivos y el dispositivo de almacenamiento en el que está almacenado.

Conceptos de la administración del almacenamiento

Un sistema de archivos es una estructura organizada de directorios y archivos que contienen datos que residen en un dispositivo de almacenamiento, como una partición o un disco físico. La jerarquía de sistemas de archivos abordada anteriormente reúne todos los sistemas de archivos en un árbol de directorios con una sola raíz: el directorio /. La ventaja de esta disposición es que la jerarquía existente puede extenderse en cualquier momento mediante la adición de una partición o un disco nuevo que contenga un sistema de archivos compatible a fin de añadir espacio en disco en cualquier parte del árbol del sistema de archivos. El proceso mediante el cual se añade un sistema de archivos nuevo al árbol de directorios existente se denomina *montaje*. El directorio en el que se monta el sistema de archivos nuevo se conoce como *punto de montaje*. Este concepto es muy diferente del empleado en un sistema Microsoft Windows, en el que un sistema de archivos nuevo se representa como una letra de unidad separada.

Los discos duros y los dispositivos de almacenamiento normalmente se dividen en fragmentos más pequeños llamados *particiones*. Una partición es una forma de compartimentar un disco. Sus diferentes partes pueden formatearse con diferentes sistemas de archivos o utilizarse con fines distintos. Por ejemplo, una partición puede contener un directorio de inicio de un usuario mientras que otra puede contener registros y datos del sistema. Si un usuario llena la partición del directorio de inicio con datos, la partición del sistema puede seguir teniendo espacio disponible. La colocación de datos en dos sistemas de archivos separados en dos particiones diferentes colabora con la planificación del almacenamiento de datos.

Los dispositivos de almacenamiento se representan con un tipo de archivo especial denominado *dispositivo de bloque*. El dispositivo de bloque se almacena en el directorio /dev. En Red Hat Enterprise Linux, el primer disco duro SCSI, PATA/SATA o USB detectado es /dev/sda, el segundo es /dev/sdb, y así sucesivamente. Este nombre representa el disco en su totalidad. La primera partición primaria en /dev/sda es /dev/sda1, la segunda es /dev/sda2 y así sucesivamente.

Un listado extenso del archivo de dispositivo /dev/vda en serverX revela que su tipo de archivo especial es b, que significa "dispositivo de bloque":

```
[student@serverX ~]$ ls -l /dev/vda
brw-rw----. 1 root disk 253, 0 Mar 13 08:00 /dev/vda
```



nota

Una excepción son los discos duros en máquinas virtuales que generalmente se muestran como **/dev/vd<letter>** o **/dev/xvd<letter>**.

Otra manera de organizar discos y particiones es mediante la *administración de volúmenes lógicos* (LVM). Con LVM, uno o más dispositivos de bloque pueden agregarse a un grupo de almacenamiento denominado *grupo de volúmenes*. El espacio en disco se pone a disposición con uno o más *volúmenes lógicos*. Un volumen lógico es el equivalente a una partición que reside en un disco físico. Tanto el grupo de volúmenes como el volumen lógico tienen nombres que se asignan tras su creación. Para el grupo de volúmenes, existe un directorio con el mismo nombre que el grupo de volúmenes en el directorio **/dev**. Debajo de ese directorio, se ha creado un enlace simbólico con el mismo nombre que el volumen lógico. Por ejemplo, el archivo de dispositivo que representa el volumen lógico **mylv** en el grupo de volúmenes **myvg** es **/dev/myvg/mylv**.

Se debe observar que LVM utiliza el controlador de kernel del *Asignador de dispositivos* (DM). El enlace simbólico de arriba **/dev/myvg/mylv** apunta al nodo del dispositivo de bloque **/dev/dm-number**. La asignación del *número* es secuencial y comienza con cero (0). Hay otro enlace simbólico para cada volumen lógico en el directorio **/dev/mapper** con el nombre **/dev/mapper/myvg-mylv**. El acceso al volumen lógico puede usar generalmente cualquiera de los nombres del enlace simbólico, consistente y confiable, debido a que el nombre **/dev/dm-number** puede variar con cada arranque.

Examinar sistemas de archivos

Para obtener una descripción general sobre los puntos de montaje de sistemas de archivos y la cantidad de espacio libre disponible, ejecute el comando **df**. Cuando el comando **df** se ejecuta sin argumentos, arrojará un informe con el espacio en disco total, el espacio en disco usado y el espacio en disco libre en todos los sistemas de archivos regulares montados. Arrojará un informe sobre los sistemas locales y remotos, y el porcentaje de espacio en disco total que se está empleando.

Visualizar los sistemas de archivos y los puntos de montaje en la máquina serverX.

```
[student@serverX ~]$ df
Filesystem      1K-blocks    Used   Available Use% Mounted on
/dev/vda1        6240256  4003760   2236496  65% /
devtmpfs          950536      0    950536   0% /dev
tmpfs            959268     80    959188   1% /dev/shm
tmpfs            959268    2156    957112   1% /run
tmpfs            959268      0    959268   0% /sys/fs/cgroup
```

La partición en la máquina serverX muestra un sistema de archivos real, que está montado en **/**. Esto es frecuente en el caso de máquinas virtuales. Los dispositivos **tmpfs** y **devtmpfs** son sistemas de archivos en la memoria del sistema. Todos los archivos escritos en **tmpfs** o en **devtmpfs** desaparecen después de que se reinicia el sistema.

A fin de mejorar la legibilidad de los tamaños de los resultados, hay dos opciones diferentes *legibles por el ojo humano* : **-h** o **-H**. La diferencia entre estas dos opciones es que **-h** informará en KiB (2^{10}), MiB (2^{20}), o GiB (2^{30}), mientras que la opción **-H** informará en unidades SI: KB (10^3), MB (10^6), GB (10^9), etc. Los fabricantes de discos duros normalmente usan las unidades SI cuando anuncian sus productos.

Capítulo 14. Acceso a los sistemas de archivos de Linux

Muestre un informe sobre los sistemas de archivos en la máquina serverX con todas las unidades convertidas a formato legible por el ojo humano:

```
[student@serverX ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        6.0G  3.9G  2.2G  65% /
devtmpfs         929M    0  929M   0% /dev
tmpfs            937M   80K  937M   1% /dev/shm
tmpfs            937M  2.2M  935M   1% /run
tmpfs            937M    0  937M   0% /sys/fs/cgroup
```

Para obtener información más detallada sobre el espacio utilizado por un árbol de directorios en particular, puede usar el comando **du**. El comando **du** ofrece las opciones **-h** y **-H** para convertir el resultado a formato legible por el ojo humano. El comando **du** muestra el tamaño de todos los archivos en el árbol de directorios actual de modo recursivo.

Muestre un informe sobre el uso del disco para el directorio **/root** en serverX:

```
[root@serverX ~]# du /root
4 /root/.ssh
4 /root/.cache/dconf
4 /root/.cache
4 /root/.dbus/session-bus
4 /root/.dbus
0 /root/.config/ibus/bus
0 /root/.config/ibus
0 /root/.config
14024 /root
```

Muestre un informe sobre el uso del disco en formato legible por el ojo humano, para el directorio **/var/log** en serverX:

```
[root@serverX ~]# du -h /var/log
...
4.9M /var/log/sa
68K /var/log/prelink
0 /var/log/qemu-ga
14M /var/log
```

Referencias

Páginas del manual: **df(1)**, **du(1)**

Práctica: Identificación de los dispositivos y sistemas de archivos

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

/dev/sda2	/dev/sdb3	/dev/sdc	/dev/vdb	/dev/vdb3
/dev/vg_install/lv_home				

Descripción	Archivo de dispositivo
El archivo de dispositivo de un disco rígido SATA que reside en /dev .	
El archivo de dispositivo de la segunda partición en el primer disco rígido SATA en /dev .	
El archivo de dispositivo de un volumen lógico en /dev .	
El archivo de dispositivo del segundo disco en una máquina virtual en /dev .	
El archivo de dispositivo de la tercera partición en el segundo disco rígido SATA en /dev .	
El archivo de dispositivo de la tercera partición en el segundo disco en una máquina virtual en /dev .	

Solución

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

Descripción	Archivo de dispositivo
El archivo de dispositivo de un disco rígido SATA que reside en /dev .	/dev/sdc
El archivo de dispositivo de la segunda partición en el primer disco rígido SATA en /dev .	/dev/sda2
El archivo de dispositivo de un volumen lógico en /dev .	/dev/vg_install/lv_home
El archivo de dispositivo del segundo disco en una máquina virtual en /dev .	/dev/vdb
El archivo de dispositivo de la tercera partición en el segundo disco rígido SATA en /dev .	/dev/sdb3
El archivo de dispositivo de la tercera partición en el segundo disco en una máquina virtual en /dev .	/dev/vdb3

Montaje y desmontaje de sistemas de archivos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder acceder al contenido de sistemas de archivos mediante la adición y la eliminación de sistemas de archivos de la jerarquía de sistemas de archivos.

Montaje manual de sistemas de archivos

Un sistema de archivos que reside en un dispositivo SATA/PATA o SCSI debe montarse manualmente para acceder a él. El comando **mount** permite que el usuario root monte manualmente un sistema de archivos. El primer argumento del comando **mount** especifica el sistema de archivos que se debe montar. El segundo argumento especifica el directorio de destino en el que se pone a disposición el sistema de archivos después de su montaje. El directorio de destino se conoce como punto de montaje.

El comando **mount** espera el argumento correspondiente al sistema de archivos en una de dos maneras diferentes:

- El archivo de dispositivo de la partición que contiene el sistema de archivos, que reside en **/dev**.
- El *UUID*, identificador único universal del sistema de archivos.



nota

En la medida en que un sistema de archivos no se recrea, el *UUID* no cambia. El archivo de dispositivo puede cambiar, por ejemplo, si se modifica el orden de los dispositivos o si se añaden dispositivos adicionales al sistema.

El comando **blkid** ofrece una descripción general de las particiones existentes con un sistema de archivos en ellas y el *UUID* del sistema de archivos, así como también el sistema de archivos utilizado para formatear la partición.

```
[root@serverX ~]# blkid  
/dev/vda1: UUID="46f543fd-78c9-4526-a857-244811be2d88" TYPE="xfs"
```



nota

Un sistema de archivos puede montarse en un directorio existente. El directorio **/mnt** existe de manera predeterminada y proporciona un punto de entrada para los puntos de montaje. Se utiliza para el montaje manual de discos. Se recomienda crear un subdirectorio en **/mnt** y usarlo como punto de montaje, a menos que haya un motivo para montar el sistema de archivos en otra ubicación específica en la jerarquía del sistema de archivos.

Capítulo 14. Acceso a los sistemas de archivos de Linux

Monte por archivo de dispositivo de la partición que contiene el sistema de archivos.

```
[root@serverX ~]# mount /dev/vdb1 /mnt/mydata
```

Monte el sistema de archivos por ID única universal, o UUID, del sistema de archivos.

```
[root@serverX ~]# mount UUID="46f543fd-78c9-4526-a857-244811be2d88" /mnt/mydata
```



nota

Si el directorio que funciona como punto de montaje no está vacío, no se podrá acceder a los archivos que existen en ese directorio en la medida en que el sistema de archivos esté montado en él. Todos los archivos escritos en el directorio de punto de montaje terminan en el sistema de archivos montado en él.

Desmontaje de sistemas de archivos

Para desmontar un sistema de archivos, el comando **umount** espera el punto de montaje como argumento.

Cambie al directorio **/mnt/mydata**. Intente desmontar el dispositivo montado en el punto de montaje **/mnt/mydata**. Ocurrirá un error.

```
[root@serverX ~]# cd /mnt/mydata
[root@serverX mydata]# umount /mnt/mydata
umount: /mnt/mydata: target is busy.
        (In some cases useful info about processes that use
         the device is found by lsof(8) or fuser(1))
```

No se puede realizar el desmontaje si un proceso accede al punto de montaje. Para que el comando **umount** se ejecute correctamente, el proceso debe dejar de acceder al punto de montaje.

El comando **lsof** enumera todos los archivos abiertos y el proceso que accede a ellos en el directorio proporcionado. Resulta útil identificar los procesos que actualmente impiden un correcto desmontaje del sistema de archivos.

```
[root@serverX mydata]# lsof /mnt/mydata
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
bash    1593 root cwd DIR  253,2       6  128 /mnt/mydata
lsof    2532 root cwd DIR  253,2      19  128 /mnt/mydata
lsof    2533 root cwd DIR  253,2      19  128 /mnt/mydata
```

Una vez que se identifican los procesos, puede tomarse una medida, como esperar a que finalice el proceso o enviar una señal SIGTERM o SIGKILL al proceso. En este caso, basta con cambiar el directorio en funcionamiento actual por un directorio fuera del punto de montaje.

```
[root@serverX mydata]# cd
[root@serverX ~]# umount /mnt/mydata
```



nota

Una causa frecuente por la cual el sistema de archivos en el punto de montaje está ocupado es que el directorio en funcionamiento actual de un aviso de la shell se encuentra debajo del punto de montaje activo. El proceso que accede al punto de montaje es **bash**. El cambio a un directorio fuera del punto de montaje permite el desmontaje del dispositivo.

Acceso a dispositivos de almacenamiento extraíbles

El entorno de escritorio gráfico monta automáticamente los medios extraíbles, como memorias y dispositivos flash USB, cuando se conectan. El punto de montaje para el medio extraíble es `/run/media/<user>/<label>`. El valor de `<user>` es el usuario registrado en el entorno gráfico. El valor de `<label>` es el nombre que se le asignó al sistema de archivos cuando se creó.



Advertencia

Para extraer medios USB del sistema de manera segura, primero hay que desmontarlos y, luego, extraerlos físicamente de la ranura USB para sincronizar el sistema de archivos. La extracción de un dispositivo de almacenamiento USB sin desmontar el sistema de archivos en él puede ocasionar la pérdida de datos.



Referencias

Páginas del manual: **mount(8)**, **umount(8)**, **lsblk(8)**

Práctica: Montar y desmontar sistemas de archivos

En este ejercicio de laboratorio, montará y desmontará sistemas de archivos.

Resultados:

El usuario identifica y monta un nuevo sistema de archivos en un punto de montaje especificado, luego lo desmonta.

Antes de comenzar

Restablezca su sistema serverX. Ejecute el script **lab fs setup** antes de empezar el ejercicio.

1. Se ha agregado una nueva partición con un sistema de archivos al segundo disco (vdb) en su máquina serverX. Monte la partición disponible recientemente mediante UUID en el punto de montaje creado recientemente **/mnt/newspace**.
 - 1.1. Use **blkid** para descubrir el UUID de la partición agregada recientemente, **vdb1**, en serverX.

```
[root@serverX ~]# blkid  
/dev/vda1: UUID="46f543fd-78c9-4526-a857-244811be2d88" TYPE="xfs"  
/dev/vdb1: UUID="7c5e3fbb-34eb-4431-a4a5-9b887c1b6866" TYPE="xfs"
```

- 1.2. Cree el punto de montaje **/mnt/newspace** en serverX.

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

- 1.3. Monte el sistema de archivos mediante UUID en el directorio **/mnt/newspace** de la máquina serverX.

```
[root@serverX ~]# mount UUID="7c5e3fbb-34eb-4431-a4a5-9b887c1b6866" /mnt/  
newspace
```

2. Cambie al directorio **/mnt/newspace** y cree un directorio nuevo, **/mnt/newspace/newdir**, con un archivo vacío, **/mnt/newspace/newdir/newfile**, en serverX.

- 2.1. Cambie al directorio **/mnt/newspace** en serverX.

```
[root@serverX ~]# cd /mnt/newspace
```

- 2.2. Cree un nuevo directorio **/mnt/newspace/newdir** en serverX.

```
[root@serverX newspace]# mkdir newdir
```

- 2.3. Cree un nuevo archivo vacío, **/mnt/newspace/newdir/newfile**, en serverX.

```
[root@serverX newspace]# touch newdir/newfile
```

3. Desmonte el sistema de archivos montado en el directorio **/mnt/newspace** en serverX.
 - 3.1. Intente desmontar **/mnt/newspace**, mientras el directorio actual en la shell aún es **/mnt/newspace** en serverX.

```
[root@serverX newspace]# umount /mnt/newspace
```

- 3.2. Cambie el directorio actual en la shell a **/root**.

```
[root@serverX newspace]# cd  
[root@serverX ~]#
```

- 3.3. Desmonte correctamente **/mnt/newspace** en serverX.

```
[root@serverX ~]# umount /mnt/newspace
```

Creación de enlaces entre archivos

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder usar enlaces duros y blandos para que múltiples nombres apunten al mismo archivo.

Administración de enlaces entre archivos

Creación de enlaces duros

Un enlace duro es una nueva entrada en el directorio que hace referencia a un archivo existente en el sistema de archivos. Todos los archivos de un sistema de archivos tienen un enlace duro nuevo de manera predeterminada. En lugar de copiar un archivo, puede crearse un enlace duro que haga referencia al mismo archivo y así ahorrar espacio. Un enlace duro nuevo debe tener un nombre de archivo diferente si se crea en el mismo directorio que el enlace duro existente o debe residir en un directorio distinto. Todos los enlaces duros que apuntan al mismo archivo tienen iguales permisos, valor de enlace, propiedades de usuario o grupo, sellos de fecha y hora, y contenido de archivo. Los enlaces duros que apuntan al contenido del mismo archivo deben estar en el mismo sistema de archivos.

El comando **ls -l** muestra el valor del enlace posterior a los permisos y anterior al propietario de un archivo.

```
[root@serverX ~]# echo "Hello World" > newfile.txt
[root@serverX ~]# ls -l newfile.txt
-rw-r--r--. 1 root root 0 Mar 11 19:19 newfile.txt
```

El comando **ln** crea enlaces duros nuevos a archivos existentes. El comando espera un archivo existente como el primer argumento, seguido por uno o más enlaces duros adicionales. Los enlaces duros pueden residir en cualquier parte siempre que estén en el mismo sistema de archivos que el archivo existente. Después de que se crea un enlace duro nuevo, no existe manera de saber cuál de los enlaces duros existentes es el original.

Cree un enlace duro **newfile-link2.txt** para el archivo existente **newfile.txt** en el directorio **/tmp**.

```
[root@serverX ~]# ln newfile.txt /tmp/newfile-hlink2.txt
[root@serverX ~]# ls -l newfile.txt /tmp/newfile-hlink2.txt
-rw-rw-r--. 2 root root 12 Mar 11 19:19 newfile.txt
-rw-rw-r--. 2 root root 12 Mar 11 19:19 newfile-hlink2.txt
```

Incluso si se elimina el archivo original, el contenido del archivo continúa estando disponible siempre y cuando exista un enlace duro como mínimo.

```
[root@serverX ~]# rm -f newfile.txt
[root@serverX ~]# ls -l /tmp/newfile-link2.txt
-rw-rw-r--. 1 root root 12 Mar 11 19:19 /tmp/newfile-link2.txt
[root@serverX ~]# cat /tmp/newfile-link2.txt
Hello World
```



Importante

Todos los enlaces duros que hacen referencia al mismo archivo tienen iguales permisos, conteo de enlace, propiedades de usuario o grupo, sellos de fecha y hora, y contenido de archivo. Si se modifica algún dato en un enlace duro, todos los demás enlaces duros que apuntan al mismo archivo también mostrarán el dato nuevo.

Creación de enlaces blandos

El comando **ln -s** permite crear un enlace blando, que también se conoce como "enlace simbólico". Un enlace blando no es un archivo regular, sino un tipo de archivo especial que apunta a un archivo o a un directorio existente. A diferencia de los enlaces duros, los enlaces blandos pueden apuntar a un directorio, y el objetivo al que apunta un enlace blando puede estar en un sistema de archivos diferente.

```
[root@serverX ~]# ln -s /root/newfile-link2.txt /tmp/newfile-symlink.txt
[root@serverX ~]# ls -l newfile-link2.txt /tmp/newfile-symlink.txt
lrwxrwxrwx. 1 root root 11 Mar 11 20:59 /tmp/newfile-symlink.txt -> /root/newfile-link2.txt
-rw-rw-r--. 1 root root 12 Mar 11 19:19 newfile-link2.txt
```

Cuando se elimina el archivo original, el enlace blando sigue apuntando al archivo, pero el destino desaparece. Un enlace blando que apunta a un archivo que falta recibe el nombre de "enlace blando colgante".

```
[root@serverX ~]# rm -f newfile-link2.txt
[root@serverX ~]# ls -l /tmp/newfile-symlink.txt
lrwxrwxrwx. 1 root root 11 Mar 11 20:59 /tmp/newfile-symlink.txt -> newfile-link2.txt
[root@serverX ~]# cat /tmp/newfile-symlink.txt
cat: /tmp/newfile-symlink.txt: No such file or directory
```

Un enlace blando puede apuntar a un directorio. El enlace blando funciona como un directorio. Si cambia el directorio del enlace blando con el comando **cd**, obtendrá el funcionamiento esperado.

Cree un enlace blando **/root/configfiles** que apunte al directorio **/etc**.

```
[root@serverX ~]# ln -s /etc /root/configfiles
[root@serverX ~]# cd /root/configfiles
[root@serverX configfiles]# pwd
/root/configfiles
```



Referencias

Página del manual (1)**ln**

Práctica: Creación de enlaces entre archivos

En este ejercicio de laboratorio, creará enlaces duros y blandos.

Resultados:

El usuario crea un enlace duro y uno blando.

1. Cree un enlace duro adicional **/root/qmp-manual.txt** para el archivo existente **/usr/share/doc/qemu-kvm/qmp-commands.txt** en serverX.

- 1.1. Cree el enlace duro **/root/qmp-manual.txt**. Establezca su enlace con el archivo **/usr/share/doc/qemu-kvm/qmp-commands.txt**.

```
[root@serverX ~]# ln /usr/share/doc/qemu-kvm/qmp-commands.txt /root/qmp-manual.txt
```

- 1.2. Verifique el conteo de enlaces en el enlace **/root/qmp-manual.txt** recientemente creado.

```
[root@serverX ~]# ls -l /root/qmp-manual.txt
-rw-r--r--. 2 root root 63889 Nov 11 02:58 /root/qmp-manual.txt
```

- 1.3. Verifique el conteo de enlaces en el archivo original **/usr/share/doc/qemu-kvm/qmp-commands.txt**.

```
[root@serverX ~]# ls -l /usr/share/doc/qemu-kvm/qmp-commands.txt
-rw-r--r--. 2 root root 63889 Nov 11 02:58 /usr/share/doc/qemu-kvm/qmp-commands.txt
```

2. Cree el enlace blando **/root/tempdir** que apunta al directorio **/tmp** en serverX.

- 2.1. Cree el enlace blando **/root/tempdir**. Establezca su enlace con **/tmp**.

```
[root@serverX ~]# ln -s /tmp /root/tempdir
```

- 2.2. Verifique el enlace recientemente creado con **ls -l**.

```
[root@serverX ~]# ls -l /root
lrwxrwxrwx. 1 root root 4 Mar 13 08:42 tempdir -> /tmp
```

Localización de archivos en el sistema

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder buscar archivos en los sistemas de archivos montados usando los comandos **find** y **locate**.

Herramientas para buscar archivos

Un administrador de sistemas necesita herramientas para buscar archivos que coincidan con ciertos criterios en el sistema de archivos. En esta sección, se analizan dos comandos que pueden buscar archivos en el sistema de archivos. El comando **locate** busca una base de datos generada previamente para nombres de archivos o rutas de archivos y arroja los resultados instantáneamente. El comando **find** busca el sistema de archivos en tiempo real mediante un rastreo del sistema de archivos.

Localización de archivos por nombre con **locate**

El comando **locate** arroja resultados de búsqueda en función de la ruta o el nombre de archivos de la base de datos de **locate**. La base de datos almacena información de la ruta y el nombre de archivos.

Al buscar entradas como un usuario regular, los resultados solo se arrojan en los casos en que el usuario que solicita la búsqueda mediante **locate** tenga permisos de lectura en el árbol del directorio que contiene el elemento correspondiente.

Busque archivos con "passwd" en el nombre o la ruta en árboles de directorio legibles por el usuario student en serverX.

```
[student@serverX ~]$ locate passwd
/etc/passwd
/etc/passwd-
/etc/pam.d/passwd
/etc/security/opasswd
/usr/bin/gpasswd
/usr/bin/grub2-mkpasswd-pbkdf2
/usr/bin/lpASSWORD
/usr/bin/passwd
/usr/bin/userpasswd
/usr/bin/vino-passwd
/usr/bin/vncpasswd
```

Los resultados se presentan incluso cuando la ruta o el nombre de archivo es solo una coincidencia parcial con la consulta de búsqueda.

```
[root@serverX ~]# locate image
/home/myuser/boot.image
/home/someuser/my_family_image.png
/home/student/myimages-vacation/picture.png
```

La opción **-i** realiza una búsqueda que distingue entre mayúsculas y minúsculas. Con esta opción, todas las combinaciones posibles de letras en mayúsculas y minúsculas coinciden con la búsqueda.

```
[student@serverX ~]$ locate -i messages
...
/usr/share/vim/vim74/lang/zh_TW/LC_MESSAGES
/usr/share/vim/vim74/lang/zh_TW/LC_MESSAGES/vim.mo
/usr/share/vim/vim74/lang/zh_TW.UTF-8/LC_MESSAGES
/usr/share/vim/vim74/lang/zh_TW.UTF-8/LC_MESSAGES/vim.mo
/usr/share/vim/vim74/syntax/messages.vim
/usr/share/vim/vim74/syntax/msmessages.vim
/var/log/messages
```

La opción **-n** limita el número de resultados de búsqueda arrojados por **locate**. El siguiente ejemplo limita los resultados de búsqueda arrojados por **locate** a las primeras cinco coincidencias.

```
[student@serverX ~]$ locate -n 5 snow.png
/usr/share/icons/HighContrast/16x16/status/weather-snow.png
/usr/share/icons/HighContrast/22x22/status/weather-snow.png
/usr/share/icons/HighContrast/24x24/status/weather-snow.png
/usr/share/icons/HighContrast/256x256/status/weather-snow.png
/usr/share/icons/HighContrast/32x32/status/weather-snow.png
```

nota

La base de datos **locate** se actualiza automáticamente todos los días. El usuario root puede realizar una actualización de la base de datos con el comando **updatedb**.

```
[root@serverX ~]# updatedb
```

Búsqueda de archivos con find

El comando **find** realiza una búsqueda en tiempo real en los sistemas de archivos locales para encontrar archivos que coincidan con los criterios de los argumentos de la línea de comandos. El comando **find** busca archivos del sistema de archivos como su cuenta de usuario. El usuario que invoca el comando **find** debe tener permiso de lectura y ejecución en un directorio para examinar su contenido.

El primer argumento para el comando **find** es el directorio en que se realizará la búsqueda. Si el argumento del directorio se omite, **find** comenzará la búsqueda en el directorio actual y buscará coincidencias en todos los subdirectorios.

Para buscar el directorio de inicio del usuario student, dé a **find** un directorio de inicio /**home/student**. Para buscar en todo el sistema, proporcione un directorio de inicio de /.

nota

find posee una gran cantidad de opciones para describir exactamente qué tipo de archivo se debe buscar. Las búsquedas se pueden basar en el nombre del archivo, el tamaño del archivo, el sello de tiempo de la última modificación y otras características de archivos en cualquier combinación.

La opción **-name** seguida del nombre de un archivo busca archivos que coincidan con el nombre de archivo dado y arroja coincidencias exactas. Para buscar archivos denominados **sshd_config** en el directorio / y todos los subdirectorios en serverX, ejecute lo siguiente:

```
[root@serverX ~]# find / -name sshd_config
/etc/ssh/sshd_config
```

Los comodines están disponibles para buscar el nombre de un archivo y arroja todos los resultados que son coincidencias parciales. Al usar comodines, es importante poner entre comillas el nombre del archivo para evitar que el terminal interprete el comodín.

En el siguiente ejemplo, se buscan archivos en el directorio / en serverX que finalicen en **.txt**:

```
[root@serverX ~]# find / -name '*.txt'
/etc/pki/nssdb/pkcs11.txt
/etc/brltty/brl-lt-all.txt
/etc/brltty/brl-mb-all.txt
/etc/brltty/brl-md-all.txt
/etc/brltty/brl-mn-all.txt
...
```

Para buscar archivos en **/etc/** que contengan **pass** en cualquier parte del nombre en serverX, ejecute lo siguiente:

```
[root@serverX ~]# find /etc -name '*pass*'
/etc/passwd
/etc/passwd-
/etc/fonts/conf.d/60-overpass.conf
/etc/selinux/targeted/modules/active/modules/passenger.pp
/etc/security/opasswd
/etc/pam.d/passwd
/etc/pam.d/password-auth-ac
/etc/pam.d/password-auth
/etc/pam.d/gdm-password
```

Para realizar una búsqueda que no distinga entre mayúsculas y minúsculas de un nombre de archivo determinado, use la opción **-iname**, seguida del nombre del archivo que desea buscar. Para realizar una búsqueda que no distinga entre mayúsculas y minúsculas de archivos que tengan **messages** en el nombre, en el directorio / en serverX, ejecute lo siguiente:

```
[root@serverX ~]# find / -iname '*messages*'
/var/log/messages
/usr/lib64/python2.7/site-packages/orca/notification_messages.py
/usr/lib64/python2.7/site-packages/orca/notification_messages.pyc
/usr/lib64/python2.7/site-packages/orca/notification_messages.pyo
/usr/share/locale/aa/LC_MESSAGES
/usr/share/locale/ab/LC_MESSAGES
/usr/share/locale/ace/LC_MESSAGES
```

find puede buscar archivos en base a la propiedad o los permisos. Las opciones útiles al buscar por propietario son **-user** y **-group**, que buscan por nombre, y **-uid** y **-gid**, que buscan por ID.

Capítulo 14. Acceso a los sistemas de archivos de Linux

Busque archivos de propiedad del usuario *student* en el directorio **/home/student** en serverX.

```
[student@serverX ~]$ find -user student  
./.bash_logout  
./.bash_profile  
./.bashrc  
./.ssh  
...
```

Busque archivos de propiedad del grupo *estudiante* en el directorio **/home/student** en serverX.

```
[student@serverX ~]$ find -group student  
./.bash_logout  
./.bash_profile  
./.bashrc  
./.ssh  
...
```

Busque archivos de propiedad del usuario con la ID *1000* en el directorio **/home/student** en serverX.

```
[student@serverX ~]$ find -uid 1000  
./.bash_logout  
./.bash_profile  
./.bashrc  
./.ssh  
...
```

Busque archivos de propiedad del grupo con ID *1000* en el directorio **/home/student** en serverX.

```
[student@serverX ~]$ find -gid 1000  
./.bash_logout  
./.bash_profile  
./.bashrc  
./.ssh  
...
```

Busque archivos de propiedad del usuario *root* y el grupo *mail* en la máquina serverX.

```
[root@serverX ~]# find / -user root -group mail  
/var/spool/mail  
/var/spool/mail/root
```

Se utiliza la opción **-perm** para buscar archivos con una serie de permisos particulares. Los permisos se pueden describir como valores octales, con alguna combinación de 4, 2 y 1 para lectura, escritura y ejecución. Los permisos deben estar precedidos por el signo **/** o el signo **-**.

Un permiso numérico precedido por **/** coincidirá con archivos que tengan al menos un bit de usuario, grupo u otro, para esa serie de permisos. Un archivo con permisos **r--r--r--**

no coincide con /222, pero uno con **rw-r--r--** sí. Un signo menos - antes de un permiso significa que las tres instancias de ese bit deben estar activadas; por lo tanto, ningún ejemplo anterior coincidirá, pero algo como **rw-rw-rw-** sí lo hará.

Para utilizar un ejemplo más complejo, el siguiente comando debe coincidir con cualquier archivo para el cual el usuario tiene permisos de lectura, escritura y ejecución, los miembros del grupo tienen permisos de lectura y escritura, y los demás tienen acceso de solo lectura:

```
[root@serverX ~]# find /home -perm 764
```

Para que coincidan los archivos para los cuales el usuario tiene al menos permisos de escritura y ejecución, y el grupo tiene por lo menos permisos de lectura y los demás tienen por lo menos acceso de lectura:

```
[root@serverX ~]# find /home -perm -324
```

Para que coincidan los archivos para los cuales el usuario tiene permisos de lectura, o el grupo tiene por lo menos permisos de lectura o los demás tienen por lo menos acceso de lectura:

```
[root@serverX ~]# find /home -perm /442
```

Cuando se utiliza con / o bien -, un valor de **0** funciona como un comodín, ya que significa "un permiso de por lo menos nada".

Para que coincida con cualquier archivo en el directorio **/home/student** para el cual los demás tienen al menos acceso de lectura en serverX, ejecute lo siguiente:

```
[student@serverX ~]$ find -perm -004
```

Encuentre todos los archivos en el directorio **/home/student** donde **other** tiene permisos de escritura en serverX.

```
[student@serverX ~]$ find -perm -002
```

El comando **find** puede buscar archivos que coincidan con un tamaño especificado con la opción **-size**, seguida de un valor numérico y la unidad.

Las unidades que se usarán con la opción **-size** son las siguientes:

- k, para kilobyte
- M, para megabyte
- G, para gigabyte

Busque archivos con un tamaño de *exactamente* 10 megabytes.

```
[student@serverX ~]$ find -size 10M
```

Busque archivos con un tamaño *mayor* que 10 gigabytes.

Capítulo 14. Acceso a los sistemas de archivos de Linux

```
[student@serverX ~]$ find -size +10G
```

Detalle todos los archivos con un tamaño *menor* que 10 kilobytes.

```
[student@serverX ~]$ find -size -10k
```



Importante

Los modificadores de la unidad **-size** redondean todo para arriba a unidades enteras. Por ejemplo, **find -size 1M** mostrará archivos de un tamaño menor que 1 MB porque redondea todos los archivos para arriba a 1 MB.

La opción **-mmin**, seguida de la hora en minutos, busca todos los archivos para los cuales se ha cambiado su contenido exactamente en el momento dado en el pasado.

Para encontrar todos los archivos para los cuales se había modificado su contenido exactamente hace 120 minutos en serverX, ejecute:

```
[root@serverX ~]# find / -mmin 120
```

El modificador **+** delante de la cantidad de minutos busca todos los archivos en **/** que han sido modificados hace más de 200 minutos.

```
[root@serverX ~]# find / -mmin +200
```

El modificador **-** cambia la búsqueda para buscar todos los archivos en el directorio **/** que han sido modificados hace menos de 150 minutos.

```
[root@serverX ~]# find / -mmin -150
```

La opción **-type** limita el alcance de la búsqueda a un tipo de archivo dado, como lo siguiente:

- **f**, para archivo regular
- **d**, para directorio
- **l**, para enlace simbólico
- **b**, para dispositivo de bloques

Busque todos los directorios en la carpeta **/etc** en serverX.

```
[root@serverX ~]# find /etc -type d  
/etc  
/etc/tmpfiles.d  
/etc/systemd  
/etc/systemd/system  
/etc/systemd/system/getty.target.wants  
...
```

Busque todos los enlaces simbólicos en el sistema serverX.

```
[root@serverX ~]# find / -type l
```

Genere una lista de dispositivos de bloques en el directorio **/dev** en serverX:

```
[root@serverX ~]# find /dev -type b  
/dev/vda1  
/dev/vda
```

La opción **-links** seguida de un número busca todos los archivos que tienen un determinado conteo de enlaces duros. El número puede ser precedido por un modificador **+** para buscar archivos con un conteo más alto que el conteo de enlaces físicos dado. Si el número es precedido por un modificador **-**, la búsqueda se limita a todos los archivos con un conteo de enlaces físicos que sea menor que el número dado.

Busque todos los archivos regulares con más de un enlace físico en la máquina serverX.

```
[root@serverX ~]# find / -type f -links +1
```



Referencias

Páginas del manual: **locate(1)**, **updatedb(1)**, **find(8)**

Práctica: Búsqueda de archivos en el sistema

En este ejercicio de laboratorio, los estudiantes buscarán archivos en el sistema de archivos local.

Resultados:

El usuario buscará archivos con los comandos **locate** y **find**.

- Utilice el comando "locate" para buscar diversos archivos en la máquina serverX.

- Aunque la base de datos en la que se realiza la búsqueda se actualiza a diario de manera automática, asegúrese de que esté actualizada; para ello, inicie una actualización manual en serverX.

```
[root@serverX ~]# updatedb
```

- Busque el archivo de configuración **logrotate.conf** en serverX.

```
[root@serverX ~]# locate logrotate.conf
/etc/logrotate.conf
/usr/share/man/man5/logrotate.conf.5.gz
```

- Busque el archivo de configuración **networkmanager.conf** en serverX e ignore la distinción entre mayúsculas y minúsculas.

```
[root@serverX ~]# locate -i networkmanager.conf
/etc/NetworkManager/NetworkManager.conf
/etc/dbus-1/system.d/org.freedesktop.NetworkManager.conf
/usr/share/man/man5/NetworkManager.conf.5.gz
```

- Use el comando **find** a fin de realizar búsquedas en tiempo real en la máquina serverX de acuerdo con los siguientes requisitos:

- Busque todos los archivos en el directorio **/var/lib** que sean propiedad del usuario **chrony** en serverX.

```
[root@serverX ~]# find /var/lib -user chrony
/var/lib/chrony
```

- Enumere todos los archivos en el directorio **/var** que sean propiedad del usuario **root** y del grupo **mail**.

```
[root@serverX ~]# find /var -user root -group mail
/var/spool/mail
/var/spool/mail/root
```

- Enumere todos los archivos en el directorio **/usr/bin** que tengan un tamaño superior a 50 kilobytes.

```
[root@serverX ~]# find /usr/bin -size +50k
```

```
/usr/bin/pre-grohtml  
/usr/bin/iconv  
/usr/bin/localedef  
/usr/bin/rpcgen  
/usr/bin/less  
...
```

- 2.4. Busque todos los archivos en el directorio **/home/student** que no se hayan modificado en los últimos 120 minutos en serverX.

```
[root@serverX ~]# find /home/student -mmin +120  
/home/student  
/home/student/.bash_logout  
/home/student/.bash_profile  
/home/student/.bashrc  
/home/student/.ssh  
...
```

- 2.5. Busque todos los archivos en el directorio **/tmp** que se hayan modificado en los últimos 240 minutos en serverX.

```
[root@serverX ~]# find /tmp -mmin -240  
/tmp  
/tmp/.X11-unix  
/tmp/.X11-unix/X0  
/tmp/.ICE-unix  
...
```

Ejercicio de laboratorio: Acceso a los sistemas de archivos de Linux

En este ejercicio de laboratorio, los estudiantes montarán un sistema de archivos local, lo revisarán y trabajarán con enlaces simbólicos.

Resultados:

- Generar un informe de uso del disco.
- Montar un sistema de archivos.
- Crear un enlace simbólico.
- Buscar archivos en el sistema de archivos local.

Andes de comenzar

Restablezca su sistema serverX.

Ejecute la **lab fs setup** para configurar la máquina del servidor para el ejercicio.

1. Genere un informe de uso del disco con el comando **du** del directorio **/var/log** en serverX y guarde el resultado en el archivo **/tmp/results.txt**.
2. Identifique y monte un sistema de archivos agregado recientemente por UUID en el directorio **/mnt/myfreespace** en serverX.
3. Cree el enlace blando **/root/myfreespace**, que apunta al directorio **/mnt/myfreespace** en serverX.
4. Busque todos los enlaces simbólicos en serverX que incluyan **freespace** en su nombre.

Solución

En este ejercicio de laboratorio, los estudiantes montarán un sistema de archivos local, lo revisarán y trabajarán con enlaces simbólicos.

Resultados:

- Generar un informe de uso del disco.
- Montar un sistema de archivos.
- Crear un enlace simbólico.
- Buscar archivos en el sistema de archivos local.

Andes de comenzar

Restablezca su sistema serverX.

Ejecute la **lab fs setup** para configurar la máquina del servidor para el ejercicio.

1. Genere un informe de uso del disco con el comando **du** del directorio **/var/log** en serverX y guarde el resultado en el archivo **/tmp/results.txt**.

```
[root@serverX ~]# du /var/log >/tmp/results.txt
```

2. Identifique y monte un sistema de archivos agregado recientemente por UUID en el directorio **/mnt/myfreespace** en serverX.

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

```
[root@serverX ~]# blkid  
/dev/vda1: UUID="46f543fd-78c9-4526-a857-244811be2d88" TYPE="xfs"  
/dev/vdb1: UUID="a84f6842-ec1d-4f6d-b767-b9570f9fc0" TYPE="xfs"
```

- 2.2. Cree el punto de montaje **/mnt/myfreespace** en serverX.

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

- 2.3. Monte el sistema de archivos mediante UUID en el directorio **/mnt/myfreespace** de la máquina serverX.

```
[root@serverX ~]# mount UUID="a84f6842-ec1d-4f6d-b767-b9570f9fc0" /mnt/  
myfreespace
```

3. Cree el enlace blando **/root/myfreespace**, que apunta al directorio **/mnt/myfreespace** en serverX.

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

4. Busque todos los enlaces simbólicos en serverX que incluyan **freespace** en su nombre.

```
[root@serverX ~]# find / -type l -name '*freespace*'  
/root/myfreespace
```

Resumen

Identificación de dispositivos y sistemas de archivos

Los dispositivos de almacenamiento se representan como diferentes archivos de dispositivo.

Montaje y desmontaje de sistemas de archivos

El acceso al contenido de sistemas de archivos en dispositivos de almacenamiento interno y externo es importante.

Creación de enlaces entre archivos

El manejo de los enlaces a archivos existentes permite ahorrar espacio en el sistema de archivos.

Localización de archivos en el sistema

La búsqueda de archivos es importante para varias tareas administrativas.



CAPÍTULO 15

USO DE SISTEMAS VIRTUALIZADOS

Descripción general	
Meta	Crear y usar máquinas virtuales que tengan Red Hat Enterprise Linux a través de la máquina virtual basada en el kernel (KVM) y libvirt.
Objetivos	<ul style="list-style-type: none">Instalar un sistema Red Hat Enterprise Linux como host para el funcionamiento de máquinas virtuales.Realizar una instalación interactiva de Red Hat Enterprise Linux en una máquina virtual.
Secciones	<ul style="list-style-type: none">Administración de un host de virtualización local (y práctica)Instalación de una máquina virtual nueva (y práctica)
Prueba del capítulo	<ul style="list-style-type: none">Uso de sistemas virtualizados

Administración de un host de virtualización local

Objetivos

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

- Describir las plataformas de virtualización de Red Hat y compararlas.
- Instalar Red Hat Enterprise Linux como sistema host de virtualización.

Virtualización de sistema y Red Hat Enterprise Linux

La máquina virtual basada en el kernel (KVM) es una solución de virtualización completa creada como parte del kernel Red Hat Enterprise Linux estándar. Puede ejecutar múltiples sistemas operativos de invitado Windows y Linux sin modificar. El hipervisor de KVM en Red Hat Enterprise Linux se administra con la API *libvirt* y con sus utilidades, como ***virt-manager*** y ***virsh***. Como Red Hat Enterprise Linux es la base de Red Hat Enterprise Virtualization y la plataforma OpenStack de Red Hat, KVM es un componente que se incluye en todos los productos de la infraestructura en nube de Red Hat.

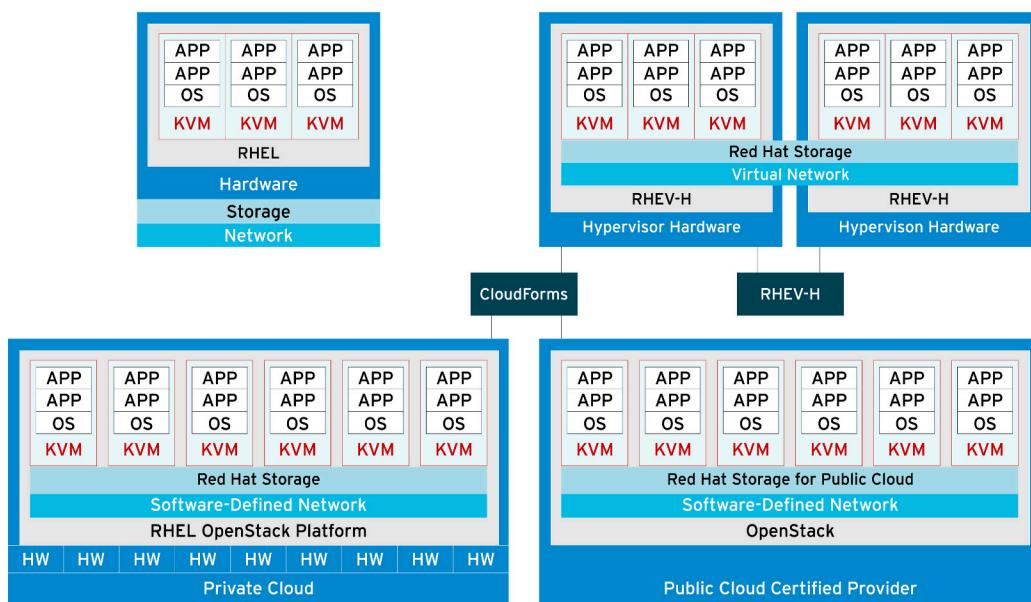


Figura 15.1: KVM en toda la infraestructura en nube de Red Hat

KVM proporciona la tecnología de máquina virtual (VM) en todos los productos Red Hat, que van desde instancias físicas independientes de Red Hat Enterprise Linux hasta la plataforma en nube OpenStack. Si comenzamos desde la esquina superior izquierda de la figura anterior, observamos lo siguiente:

- **Sistemas físicos (heredados):** las instalaciones de Red Hat Enterprise Linux en hardware heredado proporcionan virtualización KVM, con las limitaciones físicas de los sistemas individuales, y son administradas por utilidades de libvirt, como ***virt-manager***. Las

instancias de Red Hat Enterprise Linux también pueden alojarse directamente en el programa Red Hat Certified Cloud Provider a través de Red Hat Cloud Access.

Red Hat Enterprise Linux normalmente se configura como un *thick host*, un sistema que admite VM y que, al mismo tiempo, presta otros servicios locales y de red, aplicaciones y funciones de administración.

- **Red Hat Enterprise Virtualization (RHEV)**: Admite instancias de KVM en múltiples sistemas Red Hat Enterprise Virtualization Hypervisor (RHEV-H) y ofrece migración de KVM, redundancia y alta disponibilidad administrada por RHEV Manager (RHEV-M).

Red Hat Enterprise Virtualization Hypervisor es un *thin host*, una versión optimizada y minimizada con destreza de Red Hat Enterprise Linux dedicada específicamente al aprovisionamiento y al soporte de las VM invitadas.

- **Plataforma RHEL OpenStack**: Arquitectura de nube privada de Red Hat que emplea la plataforma OpenStack integrada y optimizada en una base Red Hat Enterprise Linux con KVM, administrada por el panel OpenStack de Red Hat (componente de Horizon) o por Red Hat CloudForms.
- **OpenStack en nube pública**: Arquitectura de nube pública de OpenStack implementada en el programa Red Hat Certified Cloud Provider y administrada por el componente Horizon de OpenStack o por Red Hat CloudForms.x
- **Nube híbrida**: Las utilidades de administración de nube de Red Hat CloudForms permiten administrar y realizar la migración de instancias de KVM en Red Hat RHEV y en arquitecturas OpenStack, además de realizar la transición de instancias de KVM con plataformas VMware y OpenStack de terceros.

Las configuraciones de instancias de KVM son compatibles en todos los productos de Red Hat. Los requisitos, los parámetros y los procedimientos para la instalación son los mismos en las plataformas admitidas.

Configuración de un sistema físico Red Hat Enterprise Linux como host de virtualización
Red Hat Enterprise Linux puede configurarse como host de virtualización para poder realizar tareas de desarrollo, pruebas o capacitación, o cuando se necesite trabajar en múltiples sistemas operativos simultáneamente. Los hosts Red Hat Enterprise Linux proporcionan la capacidad de instalar software adicional en la plataforma host según sea necesario, como agentes y utilidades de monitoreo, servicios de red, almacenamiento especializado y otras herramientas de desarrollo que quizás no sea adecuado instalar en hipervisores Red Hat Enterprise Virtualization dedicados.

Las instalaciones de Red Hat Enterprise Linux también otorgan un acceso más sencillo a herramientas de administración de recursos y de ajuste (como **tuned** y **cgroups**). En comparación, los hipervisores RHEV-H ofrecen alta seguridad y ajuste automático, lo que limita la personalización iniciada por el administrador del sistema por diseño. Cuando se necesita un mayor control administrativo y el riesgo del desempeño es aceptable, Red Hat Enterprise Linux funciona como una plataforma KVM independiente flexible. Se puede realizar la migración o la transición de las instancias de KVM creadas en RHEL a plataformas KVM más adecuadas a medida que las necesidades de la empresa aumenten.

Al preparar un sistema Red Hat Enterprise Linux para convertirse en un host de virtualización, es necesario verificar que se cumplan los requisitos mínimos del sistema e instalar una selección de paquetes de host de virtualización.

Capítulo 15. Uso de sistemas virtualizados

Requisitos del sistema recomendados:

- Procesador de un núcleo o tecnología Hyper-Threading para permitir la máxima cantidad de CPU virtualizadas en una máquina virtual de invitado y uno para el host.
- 2 GB de RAM y RAM adicional para las máquinas virtuales.
- 6 GB de espacio en disco para el host y el espacio en disco necesario para cada máquina virtual. La mayoría de los sistemas operativos de invitados necesitan 6 GB de espacio en disco como mínimo; sin embargo, los requisitos de espacio de almacenamiento real dependen del formato de imagen de cada invitado.

El hipervisor KVM requiere un procesador Intel con las extensiones Intel VT-x e Intel 64 para los sistemas basados en x86, o un procesador AMD con las extensiones AMD-V y AMD64. A fin de verificar que el hardware del sistema host admite las extensiones correctas, consulte **/proc/cpuinfo**.

```
[root@serverX ~]# grep --color -E "vmx|svm" /proc/cpuinfo
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx lm constant_tsc
arch_perfmon pebs bts rep_good aperfmpf perf pni dtes64 monitor ds_cpl vmx smx est
tm2 ssse3 cx16 xtpr pdcm sse4_1 xsave lahf_lm dts tpr_shadow vnmi flexpriority
```

La característica No eXecute (NX), denominada eXecute Disable (XD) por Intel y Enhanced Virus Protection por AMD, no es necesaria para crear un host en Red Hat Enterprise Linux, pero sí es necesaria para un hipervisor Red Hat Enterprise Virtualization (RHEV-H).

```
[root@serverX ~]# grep --color -E "nx" /proc/cpuinfo
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx lm constant_tsc
arch_perfmon pebs bts rep_good aperfmpf perf pni dtes64 monitor ds_cpl vmx smx est
tm2 ssse3 cx16 xtpr pdcm sse4_1 xsave lahf_lm dts tpr_shadow vnmi flexpriority
```

La creación de un host de virtualización con RHEL requiere, al menos, los paquetes **qemu-kvm** y **qemu-img** para proporcionar el emulador de KVM de nivel de usuario y el administrador de imágenes de disco.

```
[root@serverX ~]# yum install qemu-kvm qemu-img
```

También se recomiendan paquetes de administración de virtualización adicionales:

- **python-virtinst**: Proporciona el comando `virt-install` para la creación de máquinas virtuales.
- **libvirt**: Proporciona las bibliotecas de host y servidor para la interacción con hipervisores y sistemas host.
- **libvirt-python**: Contiene un módulo que permite que las aplicaciones Python usen la API libvirt.
- **virt-manager**: Ofrece la herramienta gráfica Virtual Machine Manager para la administración de VM, que emplea la biblioteca libvirt-client como la API de administración.
- **libvirt-client**: Proporciona las bibliotecas y API de cliente para el acceso a servidores libvirt, incluida la herramienta de la línea de comandos `virsh` para administrar y controlar VM.

```
[root@serverX ~]# yum install virt-manager libvirt libvirt-python python-virtinst
libvirt-client
```

El programa de instalación gráfica **anaconda** actualizado para Red Hat Enterprise Linux 7 brinda una mejor compatibilidad para la instalación de RHEL a fin de que cumpla ciertos fines específicos. Una instalación de **anaconda** ya no ofrece la posibilidad de seleccionar paquetes de RPM individuales (solo entornos básicos y complementos adecuados para la base seleccionada), lo que elimina las especulaciones y deriva en configuraciones más simples. Los administradores de sistemas pueden instalar de todos modos, cualquier otro paquete de RPM que deseen una vez finalizada una instalación; para ello, deben usar las herramientas de instalación de RPM estándar (como **yum** o GNOME PackageKit).

A fin de crear un host de virtualización durante una instalación gráfica de Red Hat Enterprise Linux, seleccione el entorno básico **Virtualization Host** que aparece en el panel izquierdo de la pantalla **anaconda Software Selection**. Seleccione la casilla de verificación de complementos **Virtualization Platform** ubicada en el panel derecho para incluir las herramientas y las utilidades de administración, como se muestra en la siguiente figura.

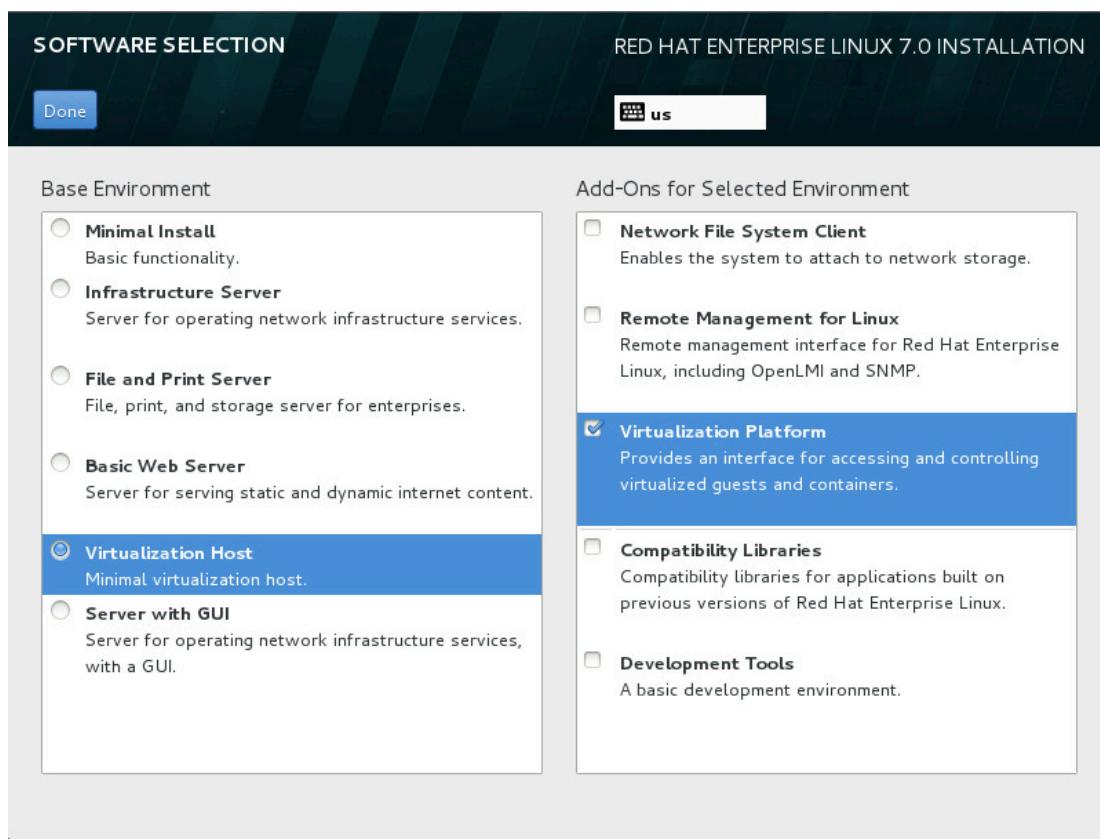


Figura 15.2: Creación de un host de virtualización durante una instalación gráfica

Administración de máquinas virtuales

El paquete libvirt es una API de virtualización independiente de hipervisor que permite administrar máquinas virtuales de manera segura al proporcionar la capacidad de aprovisionar, crear, modificar, controlar, migrar y detener máquinas virtuales en un solo host. El paquete libvirt proporciona API para enumerar, monitorear y usar los recursos disponibles en el host administrado, que incluyen CPU, memoria, almacenamiento y redes.

Capítulo 15. Uso de sistemas virtualizados

Las herramientas de administración que utilizan libvirt pueden acceder a los sistemas host de manera remota usando protocolos seguros.

Red Hat Enterprise Linux emplea herramientas basadas en libvirt de manera predeterminada para la administración de virtualización. Se incluye compatibilidad con el hipervisor RHEL 5 Xen y con KVM en RHEL 5, 6 y 7. Estas herramientas de administración utilizan libvirt:

- **virsh**: La herramienta de la línea de comandos virsh es una alternativa para la aplicación gráfica virt-manager. Los usuarios sin privilegios pueden usar virsh en modo de solo lectura o con acceso de usuario root para disponer de todas las funciones administrativas. El comando virsh es ideal para crear scripts para la administración de virtualización.
- **virt-manager**: Es una herramienta de escritorio gráfico que permite acceder a consolas de invitado y que se usa para crear máquinas virtuales, realizar su migración, su configuración y hacer tareas administrativas. Tanto los hipervisores locales como los remotos pueden administrarse desde una sola interfaz.
- **RHEV-M**: Red Hat Enterprise Virtualization Manager proporciona una plataforma de administración central para recursos físicos y virtuales, que permite iniciar, detener, crear y migrar máquinas virtuales entre hosts. RHEV-M también administra los componentes de almacenamiento y red de un centro de datos, y otorga acceso remoto seguro a la consola de invitado gráfica.

Inicie el Administrador de máquina virtual desde el menú **Applications > System Tools > Virtual Machine Manager**, o ejecute el comando **virt-manager** desde la shell. Use esta interfaz para iniciar o apagar máquinas virtuales, asignar memoria y recursos de CPU, monitorear el rendimiento y conectarse a la consola de las máquinas virtuales.

La herramienta de la línea de comandos **virsh** ofrece las mismas funciones que **virt-manager**. Utilice **virsh** como shell interactiva para realizar subcomandos, como editar, enumerar, iniciar, detener y destruir. Los siguientes ejemplos ilustran los comandos **virsh** ejecutados como comandos independientes desde la shell:

```
[root@foundationX ~]# virsh list
  Id  Name      State
  --  --
  1  desktop   running
  2  server    running

[root@foundationX ~]# virsh destroy server
[root@foundationX ~]# virsh list --all
  Id  Name      State
  --  --
  1  desktop   running
 - server    shut off

[root@foundationX ~]# virsh start server
[root@foundationX ~]# virsh list
  Id  Name      State
  --  --
  1  desktop   running
  2  server    running
```

virsh tiene subcomandos para tareas de administración adicionales:

- connect: Establece la conexión con un host KVM local o remoto usando la sintaxis **qemu:///host**

- nodeinfo: Arroja información básica sobre el host, incluidas las CPU y la memoria.
- autostart: Configura un dominio KVM para que se inicie junto con el host.
- console: Establece la conexión con la consola *serial* virtual de un invitado.
- create: Crea un dominio a partir de un archivo de configuración XML y lo inicia.
- define: Crea un dominio a partir de un archivo de configuración XML, pero no lo inicia.
- undefine: Anula la definición de un dominio. Si el dominio está activo, se elimina su configuración.
- edit: Edita el archivo de configuración XML para un dominio, que afectará el siguiente inicio del invitado.
- reboot: Reinicia el dominio como si el comando **reboot** hubiera sido ejecutado desde el interior del guest.
- shutdown: Apaga correctamente el dominio como si el comando **shutdown** hubiera sido ejecutado desde el interior del invitado.
- screenshot: Realiza una captura de pantalla de la consola del dominio actual y la almacena en un archivo.



Referencias

Es posible encontrar información adicional en la introducción y en el capítulo sobre requisitos del sistema en la *Guía de implementación y administración de virtualización de Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Guía de administración de la virtualización de Red Hat Enterprise

- Sección 1. Aspectos básicos

Guía de introducción sobre la plataforma Red Hat Enterprise Linux OpenStack 4

- Sección 1: Introducción

Páginas del manual: **virsh(1)**, **virt-manager(1)**

Práctica: Administración de un host de virtualización local

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

comenzar	crear	define (definir)	destroy (destruir)
reboot (reiniciar)	shutdown (parar)	undefine (sin definir)	

Propósito	virsh subcommand (virsh subcomando)
Arrancar una máquina virtual configurada existente	
Detener inmediatamente una máquina virtual; es similar a desconectarla	
Eliminar de manera permanente la configuración de una máquina virtual	
Usar una configuración XML para crear y arrancar una máquina virtual	
Usar una configuración XML para crear una máquina virtual	
Detener correctamente y reiniciar una máquina virtual	
Detener correctamente una máquina virtual	

Solución

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

Propósito	virsh subcommand (virsh subcomando)
Arrancar una máquina virtual configurada existente	comenzar
Detener inmediatamente una máquina virtual; es similar a desconectarla	destroy (destruir)
Eliminar de manera permanente la configuración de una máquina virtual	undefine (sin definir)
Usar una configuración XML para crear y arrancar una máquina virtual	crear
Usar una configuración XML para crear una máquina virtual	define (definir)
Detener correctamente y reiniciar una máquina virtual	reboot (reiniciar)
Detener correctamente una máquina virtual	shutdown (parar)

Instalación de una máquina virtual nueva

Objetivos

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

- Elaborar una configuración de máquina virtual.
- Instalar Red Hat Enterprise Linux en una instancia de máquina virtual nueva.

Creación de una máquina virtual

Las máquinas virtuales pueden realizar las mismas tareas que los sistemas físicos. Los administradores de sistema toman decisiones sobre el tamaño y la configuración del sistema con, fundamentalmente, los mismos criterios que para los sistemas físicos, que incluyen el rol de la máquina del invitado y la carga proyectada del sistema. Las consideraciones de preparación deben incluir los requisitos de CPU y memoria, el tipo de E/S y la cantidad esperada de clientes, el acceso al almacenamiento público o exclusivo, las expectativas de tamaño actuales y futuras, el ancho de banda y los requisitos de latencia. Los componentes de disco y red necesarios deben configurarse en el host virtual antes de crear el invitado.

Inicie el Administrador de máquina virtual desde el menú **Applications > System Tools > Virtual Machine Manager**, o ejecute el comando **virt-manager** como root. Haga clic en el botón **Create a new virtual machine** para abrir el asistente **New VM**. Antes de continuar, asegúrese de que **virt-manager** pueda acceder a los medios de instalación (ya sean locales o por medio de la red).

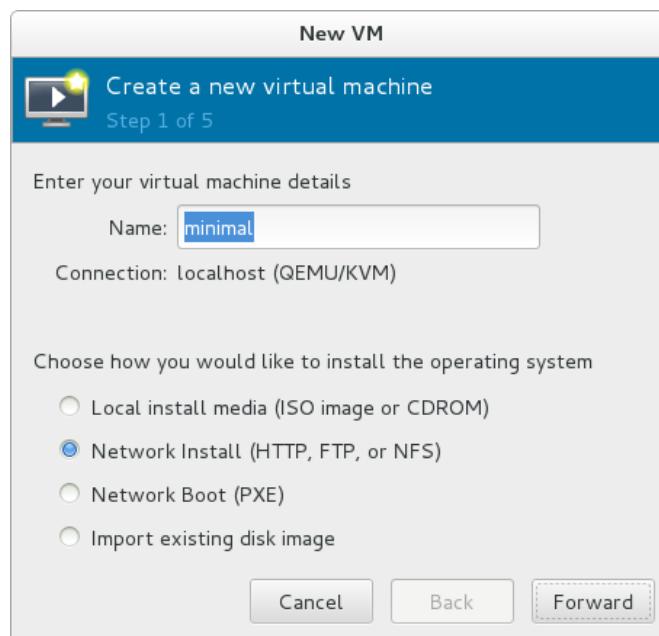


Figura 15.3: Crear una máquina virtual (paso 1 de 5)

Seleccione un nombre para la máquina virtual, que se use como nombre de dominio de configuración. El nombre del host del sistema se configura más adelante, durante la instalación del sistema operativo. Las opciones para el tipo de instalación dependen de los

recursos que se preparan. Por ejemplo, en el host virtual o en los medios físicos, debe estar disponible un DVD del sistema operativo antes de seleccionar **Local install media**, o debe tener disponible un servidor de instalación de red cuando seleccione **Network Boot (PXE)**. En este punto, se elige la opción de compartir y acceder a los medios de instalación con cualquier protocolo de archivo compartido.

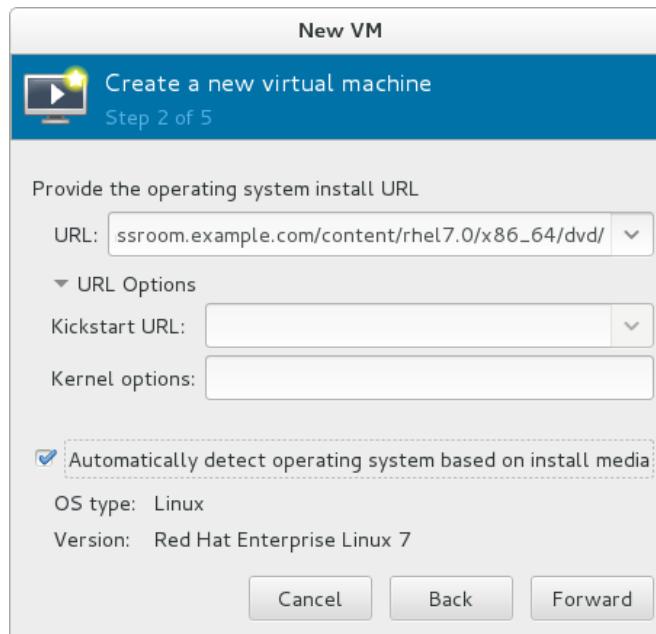


Figura 15.4: Crear una máquina virtual (paso 2 de 5)

Ingrese la **URL** para el recurso de red de medios de instalación. Configure un **tipo de SO** y una **versión** para este invitado. Cuando tenga acceso al medio de instalación, si selecciona la opción **Detectar sistema operativo en forma automática**, se completarán estos campos. Si los campos no se completan o son incorrectos, solucione los medios de instalación antes de continuar. Las opciones de **Kickstart** permiten las instalaciones sin atención; se necesita un servidor Kickstart y un archivo de configuración de cliente configurado previamente.



Figura 15.5: Crear una máquina virtual (paso 3 de 5)

Configure la cantidad adecuada de **Memoria y CPU**. Red Hat Enterprise Linux 7 requiere como mínimo una CPU y 1024 MB de memoria.

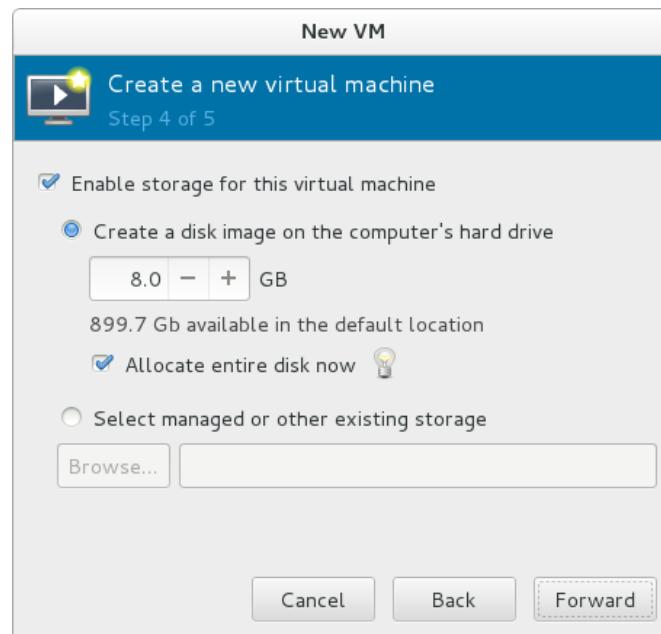


Figura 15.6: Crear una máquina virtual (paso 4 de 5)

Asigne almacenamiento a la máquina virtual del invitado. En el caso de la imagen de disco creada, si asigna ahora, obtendrá un beneficio de rendimiento pequeño, mientras que si asigna más adelante, puede ahorrar espacio en el disco que todavía no necesita. Para **Seleccionar almacenamiento administrado u otro existente**, en primer lugar necesita tener una imagen de disco preparada, un dispositivo físico o un volumen lógico antes de comenzar esta instalación.

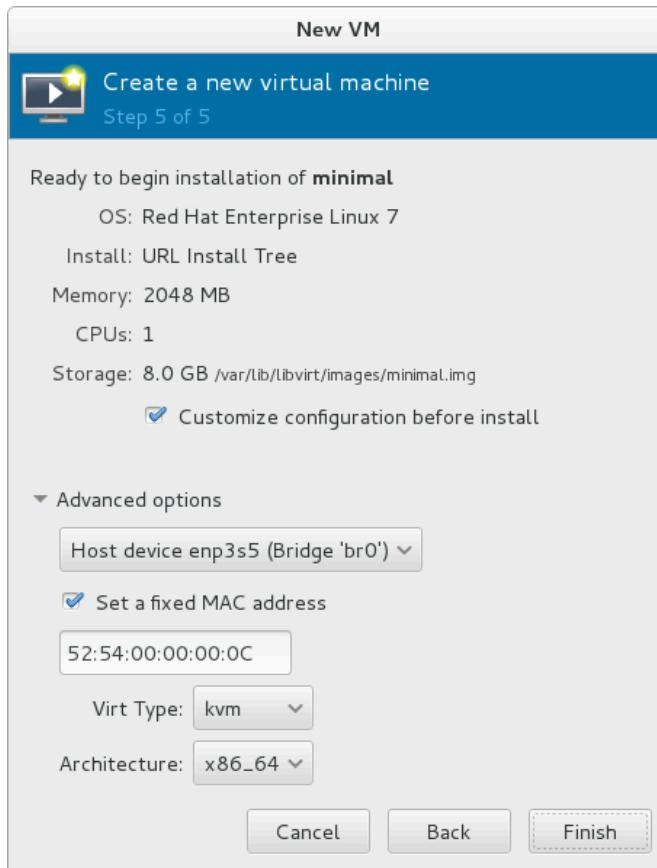


Figura 15.7: Crear una máquina virtual (paso 5 de 5)

Verifique los parámetros de configuración de la máquina virtual en la mitad superior de la ventana de diálogo. Abra **Advanced options** para configurar las redes. Las máquinas virtuales se pueden configurar como invitados privados utilizando *Traducción de direcciones de red* (NAT), o se les puede asignar la apariencia de acceso directo a subredes utilizando el puente previamente configurado del host virtual.

El asistente **New VM** genera automáticamente una dirección MAC en el rango 52:54:00 para invitados virtuales. Use la dirección MAC aleatoria provista o reemplace la dirección con una que se adapte a los requisitos del entorno. A menos que este seleccionada la casilla de verificación **Customize configuration before install**, la creación de la máquina virtual comenzará cuando se presione el botón **Finish**.



nota

En entornos de producción, las bases de datos DNS y DHCP se configuran previamente con nombres de host y direcciones IP reservadas que se asignan a las direcciones MAC a fin de centralizar y coordinar la administración del sistema virtual de toda la empresa. En un entorno de capacitación de Red Hat, el servidor DNS del aula fue completado con direcciones MAC y nombres exclusivos para los sistemas de invitado de estudiantes anticipados. Use la dirección MAC adecuada, como se lo indique el instructor o las instrucciones del ejercicio.

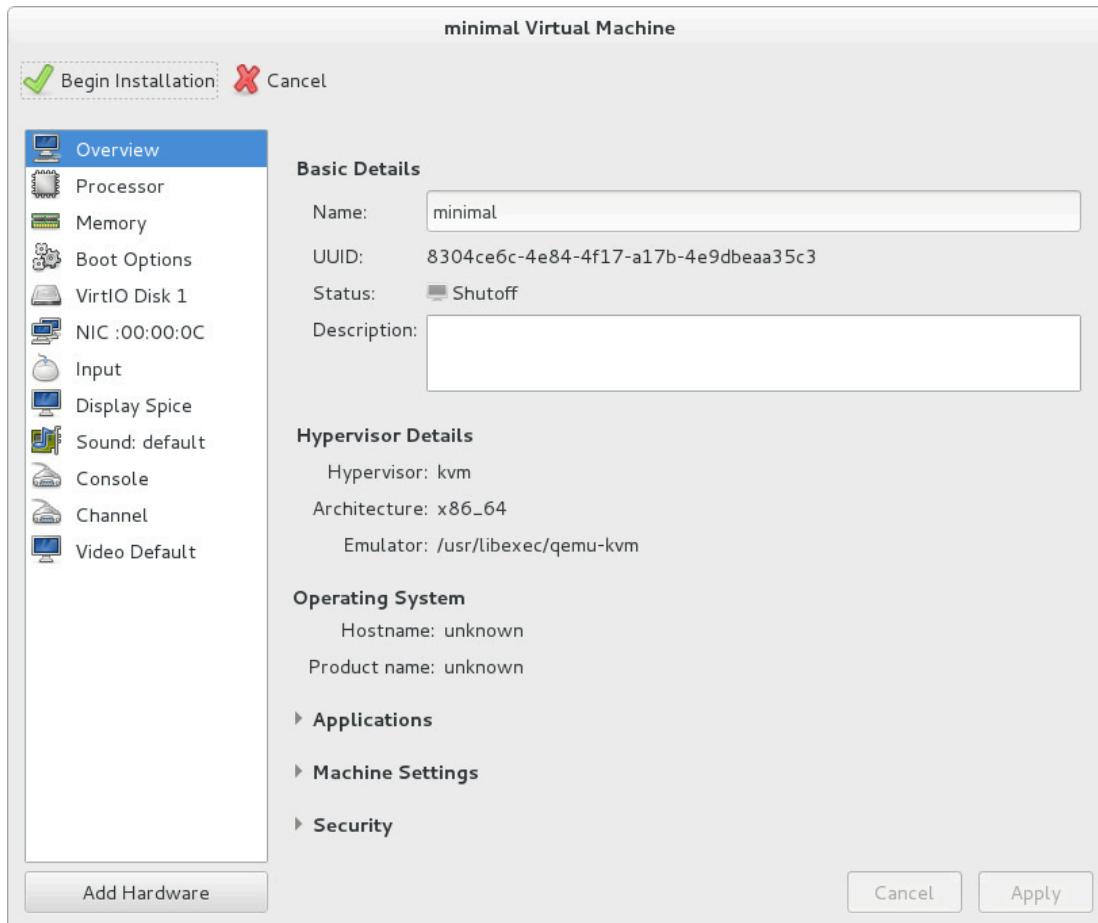


Figura 15.8: Crear una máquina virtual y personalizar la configuración

Si seleccionó la casilla de verificación **Customize configuration before install** en el último paso del asistente **New VM**, aparecerá la pantalla de detalle *domain_nameVirtual Machine*. Los administradores pueden realizar otras modificaciones o corregir la configuración antes de que comience la instalación. En esta etapa puede configurarse el hardware complementario, como gráficos y otras tarjetas de complemento, discos e interfaces de red.

Cuando se haya completado la personalización, presione **Begin Installation** en el extremo superior izquierdo.

Una vez que haya finalizado la instalación, los administradores pueden regresar a esta misma pantalla de detalles para modificar o corregir la máquina virtual. En esta sección también se encuentra la opción de iniciar automáticamente la máquina virtual cuando arranca el host físico.

Instalación Red Hat Enterprise Linux

Se recomienda que Red Hat Enterprise Linux se instale con la interfaz gráfica, conocida como **anaconda**. Si anaconda detecta que comenzó una instalación en modo de texto donde es posible una conexión de VNC, solicitará una verificación. La instalación con modo de texto es más simple, pero algunas opciones que están disponibles en modo de gráfico no están disponibles en modo de texto.

Durante la instalación de RHEL7 en una máquina física, se brindan dos consolas virtuales. La primera consola virtual tiene cinco ventanas provistas por el multiplexor del terminal de software **tmux**. La segunda consola virtual se utiliza para mostrar la interfaz gráfica de **anaconda**. Las múltiples ventanas **tmux** en la primera consola virtual proporcionan información, como mensajes de diagnóstico, y la capacidad para ingresar comandos desde un aviso de shell.

Durante la instalación, la siguiente tabla enumera las consolas virtuales, las ventanas **tmux** y las teclas que se deben presionar para alternar entre dichas consolas. Los accesos directos del teclado se realizan mediante dos acciones. Presione **Ctrl+b** y, al soltar estas teclas, presione la tecla numeral de la ventana a la que desea acceder.

Descripción de las consolas virtuales

Consola	Acceso directo del teclado	Contenido
1	Ctrl+Alt+F1	La consola principal del instalador utiliza las ventanas tmux para la instalación de texto y los registros de anaconda
2	Ctrl+b 1	Si se lo selecciona, la ventana principal tmux para anaconda muestra el instalador de texto; de lo contrario, muestra la depuración del comando general o resultados de advertencia de la GUI del instalador que se está ejecutando
3	Ctrl+b 2	Aviso de shell con acceso al usuario root
4	Ctrl+b 3	Registro de instalación: muestra mensajes almacenados en /tmp/anaconda.log
5	Ctrl+b 4	Registro de almacenamiento: muestra mensajes en los dispositivos de almacenamiento relacionados desde los servicios del kernel y del sistema que están almacenados en /tmp/storage.log
6	Ctrl+b 5	Registro de programa: muestra los mensajes de las utilidades de otro sistema y está almacenado en /tmp/program.log
7	Ctrl+Alt+F6	La consola predeterminada con GUI del instalador



Nota

La tabla de referencia anterior está en línea con las versiones de RHEL7. No obstante, puede haber otras consolas virtuales activas, a las que se puede acceder entre Ctrl+Alt+F2 y Ctrl+Alt+F5, pero solo para compatibilidad heredada.

En la pantalla **Welcome to Red Hat Enterprise Linux 7.0**, seleccione el idioma que usará durante la instalación. Después de la instalación, los usuarios seleccionan su idioma preferido en el nuevo inicio de sesión de la cuenta.

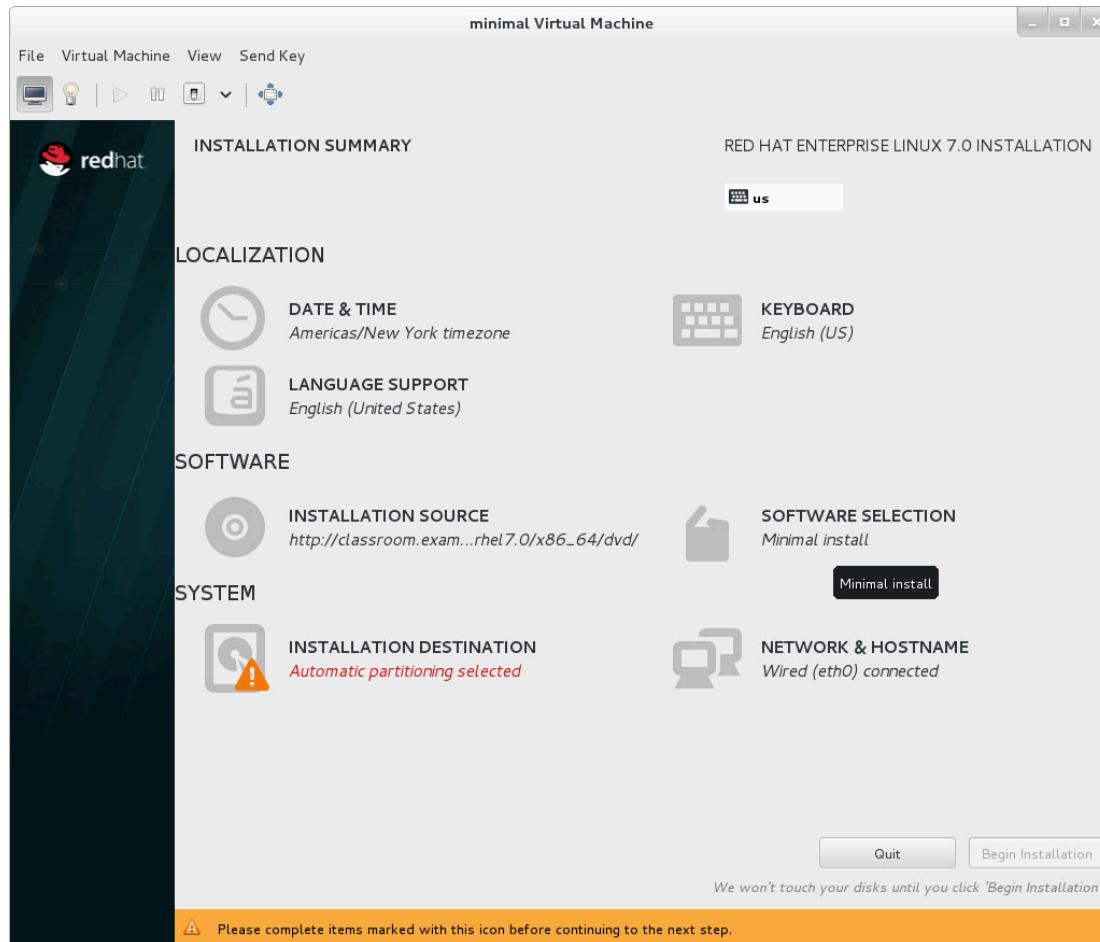


Figura 15.9: Instalador de anaconda: resumen de instalación

Aparece la pantalla **anaconda Resumen de instalación**. Desde esta pantalla central, pueden proporcionarse las personalizaciones de instalación antes de que comience la instalación. El instalador permite la configuración de los elementos de instalación en cualquier orden. Seleccione un elemento para ver o editar. Cuando se complete un elemento o esté pensado para completarse más adelante, presione **Done** para regresar a esta pantalla central.

Solo los elementos que están marcados con un símbolo de advertencia son obligatorios. La barra de estado naranja en la parte inferior de la pantalla advierte que estos elementos deben completarse antes de que comience la instalación. Una vez que se completen los elementos requeridos, presione el botón **Begin Installation**. Si presiona el botón **Quit** se interrumpe la instalación. Se conservará la configuración de la máquina virtual, pero no podrá arrancar hasta que se reinicie y complete la instalación del sistema operativo.

Según sea necesario, complete los siguientes elementos:

- **Fecha y hora:** seleccione la ciudad con un clic en el mapa interactivo o selecciónela de la lista desplegable. Especifique la zona de huso horario incluso al utilizar el protocolo de hora de red (NTP). Pueden ignorarse los mensajes que reclamen que el NTP no está configurado, en caso de que no haya un servidor de NTP disponible.
- **Compatibilidad de idioma:** seleccione los idiomas que instalará, además del idioma predeterminado ya especificado. Se pueden seleccionar varios idiomas y regiones.

- **Teclado:** este elemento permite agregar otros diseños de teclado, además del que se incluye con el idioma predeterminado.
- **Fuente de instalación:** durante los pasos de creación de la máquina virtual se seleccionó la fuente de instalación y no debe modificarse.
- **Selección de software:** de manera predeterminada, el instalador de gráficos selecciona el entorno de instalación mínimo y proporciona solo paquetes esenciales para ejecutar Red Hat Enterprise Linux. En la selección de software, elija de una lista de otros entornos de base con un clic en el botón de radio para ver los entornos disponibles enumerados en el panel izquierdo. Luego, seleccione complementos para el entorno elegido de las casillas de verificación del panel derecho.
- **Destino de instalación:** seleccione y divida los discos donde se instalará Red Hat Enterprise Linux. Este elemento espera que un administrador comprenda los esquemas de partición y los criterios de selección del sistema de archivos. El botón de radio predeterminado para la partición automática asignará los dispositivos de almacenamiento seleccionados usando todo el espacio disponible. Si no hay otros sistemas operativos ya instalados en este equipo o ha elegido no preservar sistemas operativos instalados anteriormente, **anaconda** automáticamente instala GRUB2 como el cargador de arranque.
- **Network & host name:** las conexiones de red detectadas se enumeran en el panel izquierdo. Haga clic en una conexión enumerada para mostrar más detalles. Para configurar una conexión de red en forma manual, haga clic en el botón **Configure** en el extremo inferior derecho. Aparece un diálogo para configurar la conexión seleccionada. Las opciones de configuración dependen del hardware de red disponible. En esta sección, solo deben configurarse las conexiones de red requeridas para la instalación.

Una vez que se complete la personalización de la instalación, presione **Begin Installation**.

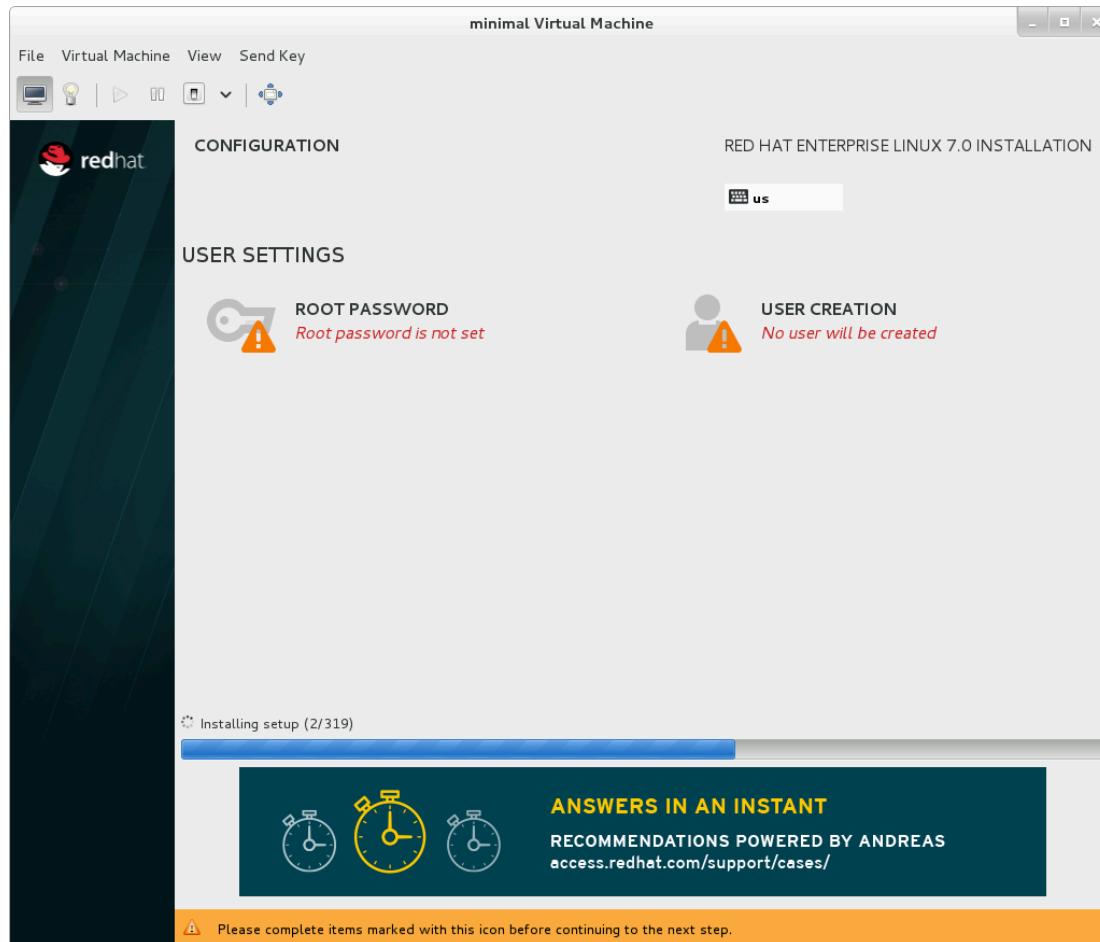


Figura 15.10: Instalador de Anaconda: configuración

Aparece la pantalla **anaconda Configuration** (Configuración). La instalación ya se inició; Red Hat Enterprise Linux informa el progreso cerca de la parte inferior de la pantalla a medida que instala los paquetes seleccionados en el sistema.

Según sea necesario, complete los siguientes elementos:

- **Contraseña de root:** el programa de instalación solicita que se configure una contraseña de root para el sistema. La etapa final del proceso de instalación no continuará hasta que se ingrese la contraseña de root.
- **Creación de usuario:** use la cuenta de root solo para la administración del sistema. Cree una cuenta que no sea de root para uso general. Aunque se recomienda realizar durante la instalación, este paso es opcional y puede realizarse después de que se completa la instalación.

Cuando la instalación indique que se completó, presione **Reboot**. Después de que se haya completado la secuencia de encendido normal de la máquina, Red Hat Enterprise Linux se carga e inicia en forma oculta, detrás de una pantalla de gráficos que muestra una barra de progreso. Si se instaló un escritorio de gráficos, aparece el inicio de sesión de GUI. Inicie sesión como el usuario que creó durante la instalación o como root. Aparece la pantalla **anaconda Initial Setup**.

Según sea necesario, complete los siguientes elementos:

- **Información de licencia:** el programa de instalación le pide que acepte los términos de la licencia.
- **Creación de usuario:** aparece solo si todavía no se creó una cuenta de usuario no root.

Una vez que se completen las tareas de configuración inicial, presione **Finish Installation**. Aparece la utilidad **FirstBoot** y le pide que ingrese la información de configuración final para este sistema. Use esta utilidad para:

- Configurar el mecanismo de volcado de memoria Kdump.
- Configure la fecha y la hora del sistema.
- Registre la máquina con la red Red Hat mediante la administración de suscripciones.

La instalación de Red Hat Enterprise Linux ahora está completa. El sistema está listo para el inicio de sesión y el uso normal.



Referencias

Es posible encontrar información adicional para la creación de la máquina virtual del invitado en la sección sobre la creación de invitados con **virt-manager** en la *Guía de administración e implementación de la virtualización de Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en

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

Página del manual (1)**virt-manager**

Se puede consultar información adicional del entorno de instalación en la sección sobre instalación y arranque en las *Notas de versión* de Red Hat Enterprise Linux 7, disponibles en

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

Práctica: Instalación de una máquina virtual nueva

A continuación se incluyen los pasos que deben seguirse para instalar Red Hat Enterprise Linux con la interfaz gráfica **anaconda**. Indique el orden en que deben seguirse los pasos.

- a. Proporcionar la ubicación de la fuente y el tipo de sistema operativo.
- b. Modificar los parámetros de localización para fecha y hora, idioma y teclado.
- c. Proporcionar los parámetros del sistema para la partición del disco, redes y nombre del host.
- d. Configurar el almacenamiento para esta máquina virtual.
- e. Ingresar la configuración de la CPU y la memoria.
- f. Proporcionar la configuración del usuario para una contraseña root y una contraseña que no sea root.
- g. Asignar un nombre a la máquina virtual y seleccionar una fuente de instalación.
- h. Seleccionar el software que se debe instalar.
- i. Configurar las opciones de red para la instalación.

Solución

A continuación se incluyen los pasos que deben seguirse para instalar Red Hat Enterprise Linux con la interfaz gráfica **anaconda**. Indique el orden en que deben seguirse los pasos.

- 2 a. Proporcionar la ubicación de la fuente y el tipo de sistema operativo.
- 6 b. Modificar los parámetros de localización para fecha y hora, idioma y teclado.
- 8 c. Proporcionar los parámetros del sistema para la partición del disco, redes y nombre del host.
- 4 d. Configurar el almacenamiento para esta máquina virtual.
- 3 e. Ingresar la configuración de la CPU y la memoria.
- 9 f. Proporcionar la configuración del usuario para una contraseña root y una contraseña que no sea root.
- 1 g. Asignar un nombre a la máquina virtual y seleccionar una fuente de instalación.
- 7 h. Seleccionar el software que se debe instalar.
- 5 i. Configurar las opciones de red para la instalación.

Prueba del capítulo: Uso de sistemas virtualizados

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

Los roles de servidor de	OpenStack en nube pública
Plataforma RHEL OpenStack	RHEV-M
Red Hat Enterprise Linux	Red Hat Enterprise Virtualization
virt-manager	

Descripción de la configuración	Producto de Red Hat
Hardware de un único sistema que proporciona compatibilidad con KVM	
Hardware de varios sistemas que proporciona redundancia virtualizada	
Hardware de varios sistemas que presta servicios de nube privada	
Proveedor de nube que presta servicios de nube pública	
Utilidad de administración para hosts KVM independientes	

Descripción de la configuración	Producto de Red Hat
Utilidad de administración para plataforma de virtualización de varios hosts	
Utilidad de administración para todas las plataformas de virtualización y nube combinadas	

Solución

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

Descripción de la configuración	Producto de Red Hat
Hardware de un único sistema que proporciona compatibilidad con KVM	Red Hat Enterprise Linux
Hardware de varios sistemas que proporciona redundancia virtualizada	Red Hat Enterprise Virtualization
Hardware de varios sistemas que presta servicios de nube privada	Plataforma RHEL OpenStack
Proveedor de nube que presta servicios de nube pública	OpenStack en nube pública
Utilidad de administración para hosts KVM independientes	virt-manager
Utilidad de administración para plataforma de virtualización de varios hosts	RHEV-M
Utilidad de administración para todas las plataformas de virtualización y nube combinadas	Los roles de servidor de

Resumen

Administración de un host de virtualización local

Preparación y creación de una infraestructura de virtualización con Red Hat Enterprise Linux.

Instalación de una máquina virtual nueva

Elabore componentes de sistema virtuales e instale Red Hat Enterprise Linux en máquinas virtuales KVM.



CAPÍTULO 16

REVISIÓN COMPLETA

Descripción general	
Meta	Poner en práctica y demostrar los conocimientos y las habilidades que se aprendieron en Red Hat System Administration I.
Objetivos	<ul style="list-style-type: none">• Poner en práctica las habilidades aprendidas en Red Hat System Administration I.
Trabajo de laboratorio	<ul style="list-style-type: none">• Revisión completa

Revisión integral de Red Hat System Administration I

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 I

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, Acceso a la línea de comandos

Iniciar sesión en el sistema Linux y ejecutar comandos simples usando la shell.

- Utilizar la sintaxis de la shell Bash para ingresar comandos en una consola Linux.
- Iniciar aplicaciones en un entorno de escritorio GNOME.
- Utilizar funciones de Bash para ejecutar comandos desde un aviso de shell con menos pulsaciones de tecla.

Capítulo 2, Administración de archivos desde la línea de comandos

Copiar, mover, crear, eliminar y organizar archivos mientras se trabaja desde el aviso de la shell Bash.

- Identificar el objetivo de directorios importantes en un sistema Linux.
- Especificar archivos usando nombres de rutas absolutas y relativas.
- Crear, copiar, mover y quitar archivos y directorios usando utilidades de la línea de comandos.
- Hacer coincidir uno o más nombres de archivo con expansión de shell como argumentos de comandos de la shell.

Capítulo 3, Obtención de ayuda en Red Hat Enterprise Linux

Resolver problemas a través de sistemas de ayuda en línea y las utilidades de asistencia de Red Hat.

- Usar man, el lector del manual de Linux.
- Usar pinfo, el lector de información de GNU.
- Usar la documentación del paquete Red Hat Package Manager (RPM)
- Usar el comando redhat-support-tool.

Capítulo 4, Creación, visualización y edición de archivos de texto

Crear, visualizar y editar archivos de texto desde un resultado de comando o en un editor.

- Redirigir el resultado de texto de un programa a un archivo o a otro programa.

- Editar archivos de texto existentes y crear archivos nuevos a partir de avisos de shell con un editor de texto.
- Copiar texto desde una ventana gráfica a un archivo de texto con un editor de texto que se ejecute en un entorno gráfico.

Capítulo 5, Administración de usuarios y grupos de Linux local

Administrar usuarios y grupos de Linux local y administrar directivas de contraseña locales.

- Explicar la función de los usuarios y grupos en un sistema Linux y cómo son entendidos por la computadora.
- Ejecutar comandos como superusuario para administrar el sistema Linux.
- Crear, modificar, bloquear y eliminar cuentas de usuario definidas a nivel local.
- Crear, modificar y eliminar cuentas de grupo definidas a nivel local.
- Bloquear cuentas en forma manual o mediante la configuración de una directiva de antigüedad de contraseña en el archivo de contraseña shadow.

Capítulo 6, Control de acceso a archivos con permisos del sistema de archivos Linux

Configurar los permisos del sistema de archivos Linux en los archivos e interpretar los efectos de seguridad de los distintos parámetros de configuración de permisos.

- Explicar cómo funciona el modelo de permisos de archivo Linux.
- Cambiar los permisos y la propiedad de los archivos con las herramientas de línea de comando.
- Configurar un directorio en el que los archivos creados recientemente puedan ser escritos en forma automática por los miembros del grupo propietario del directorio, usando permisos especiales y configuración de default umask.

Capítulo 7, Administración y control de procesos Linux

Evaluar y controlar procesos que se ejecutan en un sistema Red Hat Enterprise Linux.

- Enumerar e interpretar la información básica sobre los procesos que se ejecutan en el sistema.
- Controlar procesos en la sesión de la shell utilizando el control de trabajo de Bash.
- Finalizar y controlar los procesos utilizando señales.
- Monitorear el uso de recursos y la carga del sistema debido a la actividad del proceso.

Capítulo 8, Control de servicios y demonios

Controlar y monitorear servicios de red y demonios del sistema con systemd.

- Enumerar los demonios del sistema y los servicios de red iniciados por el servicio systemd y las unidades socket.
- Controlar los demonios del sistema y los servicios de red con **systemctl**.

Capítulo 9, Configuración y protección del servicio OpenSSH

Configurar acceso seguro a la línea de comandos en sistemas remotos con OpenSSH

- Inicie sesión en un sistema remoto usando ssh para ejecutar comandos desde el aviso de shell.

Capítulo 16. Revisión completa

- Configure ssh para permitir inicios de sesión seguros sin contraseña mediante el uso de un archivo de clave de autenticación privada.
- Personalice la configuración de sshd para limitar los inicios de sesión directos como root o para deshabilitar la autenticación con contraseña.

Capítulo 10, Análisis y almacenamiento de registros

Ubicar e interpretar correctamente archivos de registro del sistema relevantes para la solución de problemas.

- Describir la arquitectura básica syslog en Red Hat Enterprise Linux 7.
- Interpretar entradas en archivos syslog relevantes para la solución de problemas o revisar el estado del sistema.
- Buscar e interpretar entradas en el journal de systemd para solucionar problemas o revisar el estado del sistema.
- Configurar systemd-journald para almacenar el diario en disco en lugar de almacenarlo en memoria.
- Mantener una sincronización de tiempos y configuración de zona horaria precisas para garantizar sellos de tiempo correctos en los registros del sistema.

Capítulo 11, Administración de la red de Red Hat Enterprise Linux

Configurar la red IPv4 básica en los sistemas Red Hat Enterprise Linux.

- Explicar los conceptos fundamentales de la red de computadora.
- Realizar una prueba y revisar la configuración de red actual con las utilidades básicas.
- Administrar la configuración de la red y los dispositivos con **nmcli** y NetworkManager.
- Modificar la configuración de la red mediante la edición de los archivos de configuración.
- Configurar y probar el nombre del host del sistema y la resolución de nombre.

Capítulo 12, Archivar y copiar archivos entre sistemas

Archivar y copiar archivos de un sistema a otro.

- Usar TAR para crear documentos de archivos comprimidos nuevos y extraer documentos desde documentos de archivos existentes.
- Copiar archivos en forma segura desde o hacia un sistema remoto que ejecuta sshd.
- Sincronizar en forma segura el contenido de un archivo o directorio local con una copia remota.

Capítulo 13, Instalación y actualización de paquetes de software

Descargar, instalar, actualizar y administrar paquetes de software de Red Hat y repositorios de paquetes YUM.

- Registrar sistemas con su cuenta de Red Hat y autorizar las actualizaciones de software para los productos instalados.
- Explicar el significado de un paquete RPM y el modo en que los paquetes RPM se utilizan para administrar software en un sistema con Red Hat Enterprise Linux.
- Buscar, instalar y actualizar paquetes de software usando el comando **yum**.

- Habilitar y deshabilitar el uso de repositorios YUM de terceros o de Red Hat.
- Examinar los archivos de paquetes de software descargados e instalarlos.

Capítulo 14, Acceso a los sistemas de archivos de Linux

Acceder a sistemas de archivos existentes y examinarlos en un sistema con Red Hat Enterprise Linux.

- Identificar la jerarquía del sistema de archivos.
- Acceder al contenido de los sistemas de archivos.
- Usar enlaces duros y enlaces simbólicos para crear múltiples nombres.
- Buscar archivos en sistemas de archivos montados.

Capítulo 15, Uso de sistemas virtualizados

Crear y usar máquinas virtuales que tengan Red Hat Enterprise Linux a través de la máquina virtual basada en el kernel (KVM) y libvirt.

- Instalar un sistema Red Hat Enterprise Linux como host para el funcionamiento de máquinas virtuales.
- Realizar una instalación interactiva de Red Hat Enterprise Linux en una máquina virtual.



Referencias

Obtenga información acerca de más clases disponibles de Red Hat en
| <http://www.redhat.com/training/>

Trabajo de laboratorio: Revisión integral

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

Resultados:

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

Andes de comenzar

Reinic peace la máquina de serverX.

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

1. Use comandos Bash para completar las siguientes tareas en la máquina serverX:
 - Muestre las 12 primeras líneas del archivo **/usr/bin/clean-binary-files** y envíe el resultado al archivo **/home/student/headtail.txt**.
 - Muestre las últimas nueve líneas del archivo **/usr/bin/clean-binary-files** y agregue el resultado al archivo **/home/student/headtail.txt**.
2. Existen 10 sistemas Linux nuevos que requieren de archivos de documentos de cambios. Complete las siguientes tareas en serverX para crearlos:
 - Cree los archivos vacíos con el nombre de archivo **system_changes-machineY-month_Z.txt** en el directorio **/home/student** en la máquina serverX como usuario student. Reemplace Y con el número de máquina y reemplace Z con los meses *jan*, *feb* y *mar*.
 - Cree el directorio **/home/student/syschanges** con los subdirectorios **jan**, **feb** y **mar**.
 - Clasifique todos los archivos recién creados por mes en el subdirectorio correspondiente.
 - Elimine todos los archivos creados recientemente relacionados con las máquinas 9 y 10 porque el hardware fue reemplazado en forma permanente.
3. Use las páginas de manual para investigar cómo desactivar el uso de colores en el resultado. Incluya la opción relevante del comando **ls** en el archivo de texto **/home/student/lscolor.txt** en serverX.
4. Copie el archivo **/home/student/vimfile.txt** a **/home/student/longlisting.txt** en serverX. Use el editor **vim** para cambiar el archivo **/home/student/longlisting.txt** según los siguientes requisitos:
 - Elimine la columna de propietario de archivo. No elimine ningún espacio.
 - Elimine las filas **Documents** y **Pictures**.
 - Guarde el archivo cuando haya finalizado la edición.
5. Cambie la configuración y agregue usuarios nuevos y un grupo nuevo, según los siguientes requisitos:

- Cambie los parámetros de configuración del sistema predeterminados para los usuarios creados recientemente a fin de garantizar que sus contraseñas se cambien por lo menos cada 60 días.
 - Cree un grupo nuevo con el nombre **instructores** con un GID de 30 000.
 - Cree tres usuarios nuevos: **gorwell**, **rbradbury** y **dadams**, con la contraseña **firstpw**.
 - Agregue los usuarios nuevos al grupo **instructors** complementario. El grupo principal debería permanecer como el grupo privado del usuario.
 - Configure las tres cuentas recientemente creadas para que venzan en 60 días a partir de hoy.
 - Cambie la directiva de contraseña para la cuenta **gorwell** a fin de solicitar una contraseña nueva cada 10 días.
 - Obligue a los tres usuarios creados recientemente a que cambien sus contraseñas la primera vez que inicien sesión.
6. Cree el directorio compartido **/home/instructors** en serverX según los siguientes requisitos:
 - El directorio es propiedad del usuario root y los instructores del grupo.
 - Establezca los permisos en el directorio **/home/instructors** para que tenga el SETGID bit establecido en el directorio, para que el propietario y el grupo tengan permisos totales de lectura, escritura y ejecución, y otros usuarios tengan permiso de lectura del directorio.
 7. Determine el proceso que usa la mayoría de los recursos del CPU en serverX y finalícelo.
 8. Detenga el servicio de impresión cups que está actualmente en ejecución en serverX. El servicio no debería iniciarse en forma automática en el arranque del sistema.
 9. Configure el servicio ssh en serverX según los siguientes requisitos:
 - El usuario student en serverX puede iniciar sesión con una llave pública SSH en la cuenta student en desktopX.
 - Inhabilite el inicio de sesión de **ssh** para el usuario root y la autenticación de SSH con contraseña en serverX.
 10. Su máquina serverX ha sido reubicada en las Bahamas. Tiene que implementar los siguientes cambios en la máquina serverX:
 - Cambie la zona horaria en la máquina serverX para que coincida con Bahamas y verifique que la zona horaria se haya modificado en forma adecuada.
 11. Registre el comando para mostrar todas las entradas del journal de **systemd** registradas entre las 9:05:00 y las 9:15:00 en el archivo **/home/student/systemdreview.txt**.
 12. Configure **rsyslogd** mediante el agregado de una regla al archivo de configuración creado recientemente **/etc/rsyslog.d/auth-errors.conf** para registrar todos los

Capítulo 16. Revisión completa

mensajes de seguridad y de autenticación que se graban en la utilidad authpriv con el alerta de prioridad, y también más alto en el archivo **/var/log/auth-errors**. Pruebe la nueva directiva de registro agregada recientemente con el comando **logger**.

13. Cree una conexión de red estática nueva con los parámetros de configuración que están en la siguiente tabla. Asegúrese de reemplazar la *X* con el número correcto para sus sistemas.
 - Configure la conexión nueva para que se inicie en forma automática.
 - Otras conexiones no deberían iniciarse automáticamente.
 - Modifique la conexión nueva para que también use la dirección 10.0.X.1/24.
 - Configure el archivo **hosts** para que 10.0.X.1 pueda denominarse como "myhost".
 - Configure el nombre del host en el servidor X.example.com.

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

14. Sincronice el árbol de directorio **/etc** en serverX con el directorio **/configbackup** en serverX.
15. Cree un archivo con el nombre **/root/configuration-backup-server.tar.gz** con el directorio **/configbackup** como contenido.
16. Para preparar el árbol de directorio archivado a fin de compararlo con los archivos de configuración actualmente usados en forma activa en serverX, extraiga el contenido del archivo **/root/configuration-backup-server.tar.gz** en el directorio **/tmp/configcompare/** en serverX.
17. Realice las siguientes tareas en la máquina serverX:
 - Use **ssh** para ejecutar el comando **hostname** en desktopX como usuario student. Envíe el resultado del comando **hostname** al archivo **/tmp/scpfile.txt** en desktopX.
 - Use **scp** para copiar el archivo **/tmp/scpfile.txt** de desktopX a **/home/student/scpfile.txt**.
18. Cree el archivo **/etc/yum.repos.d/localupdates.repo** para habilitar el repositorio "Actualizaciones" que se encuentra en la máquina content. Debería acceder al contenido que está en la siguiente URL: http://content.example.com/rhel7.0/x86_64/errata. No controle las firmas de GPG.
19. Configure serverX para que respete los requisitos de software específicos:
 - El paquete **núcleo** debe actualizarse a la versión más reciente.
 - Debe instalarse el paquete **xsane-gimp**.

-
- Debe instalarse el paquete **rht-system**.
 - Por razones de seguridad, serverX no debe tener instalado el paquete **wvdial**.
20. Genere un informe de uso del disco con el comando **du** del directorio **/usr/share/fonts** en serverX y guarde el resultado en el archivo **/home/student/dureport.txt**.
 21. Identifique y monte un sistema de archivos agregado recientemente por UUID en el directorio **/mnt/datadump** en serverX.
 22. Cree el enlace blando **/root/mydataspace**, que apunta al directorio **/mnt/datadump** en serverX.
 23. Registre el comando para encontrar todos los enlaces blandos en serverX que tengan **data** como parte de su nombre en el archivo **/home/student/find.txt**.
 24. Cuando esté listo para revisar su trabajo, ejecute **lab sa1-review grade** en **serverX**.

Capítulo 16. Revisión completa

Solución

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

Resultados:

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

Andes de comenzar

Reinic peace la máquina de serverX.

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

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

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

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

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

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

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

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

- Cree los archivos vacíos con el nombre de archivo **system_changes-machineY-month_Z.txt** en el directorio **/home/student** en la máquina serverX como usuario student. Reemplace Y con el número de máquina y reemplace Z con los meses *jan, feb* y *mar*.
 - Cree el directorio **/home/student/syschanges** con los subdirectorios **jan, feb** y **mar**.
 - Clasifique todos los archivos recién creados por mes en el subdirectorio correspondiente.
 - Elimine todos los archivos creados recientemente relacionados con las máquinas 9 y 10 porque el hardware fue reemplazado en forma permanente.
- 2.1. Cree un total de 30 archivos con nombres **system_changes-machineY-month_Z.txt**. Reemplace Y con el número de máquina y reemplace Z con los meses *jan, feb* y *mar*.

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

- 2.2. Cree el directorio **/home/student/syschanges** con los subdirectorios **jan**, **feb** y **mar**.

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

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

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

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

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

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

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

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

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

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

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

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

- Elimine la columna de propietario de archivo. No elimine ningún espacio.
- Elimine las filas **Documents** y **Pictures**.
- Guarde el archivo cuando haya finalizado la edición.

Capítulo 16. Revisión completa

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

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

- 4.2. Edite el archivo con Vim para aprovechar el *modo visual*.

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

- 4.3. Elimine la columna *propietario* del archivo.

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

- 4.4. Elimine las filas **Documents** y **Pictures**. Esta vez, ingrese el modo visual con una **V** mayúscula, que selecciona automáticamente las líneas completas.

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

- 4.5. Guarde el archivo y salga del editor.

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

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

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

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

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

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

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

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

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

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

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

Capítulo 16. Revisión completa

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

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

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

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

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

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

- 6.1. Abra una ventana de terminal e ingrese como usuario root en serverX.

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

- 6.2. Cree el directorio **/home/instructors**.

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

- 6.3. Cambie los permisos del grupo en el directorio **/home/instructors** para que pertenezca a los instructores de grupo.

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

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

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

- 6.5. Compruebe que los permisos hayan sido establecidos correctamente.

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

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

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

```
[root@serverX ~]# top
top - 12:47:46 up 2:02, 3 users, load average: 1.67, 1.25, 0.73
Tasks: 361 total, 6 running, 355 sleeping, 0 stopped, 0 zombie
%Cpu(s): 98.5 us, 1.4 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 0.1 si, 0.0 st
KiB Mem: 2043424 total, 897112 used, 1146312 free, 1740 buffers
KiB Swap: 4079612 total, 0 used, 4079612 free. 296276 cached Me

      PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  4019 root      20   0   4156     76      0 R 57.5  0.0  2:54.15 cpuhog
  2492 student   20   0 1359500 168420  37492 S 16.8  8.2  3:55.58 gnome-shell
  1938 root      20   0 189648  35972   7568 R  1.9  1.8  0:29.66 Xorg
  2761 student   20   0  620192 19688 12296 S  0.4  1.0  0:04.48 gnome-terminal+
output truncated
```

- 7.2. Salga de la pantalla de **top**.

Presione **q** para salir.

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

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

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

- 8.1. Detenga el servicio **cups**.

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

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

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

Capítulo 16. Revisión completa

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

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

9.1. Genere una clave pública de SSH en serverX como usuario student.

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

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

```
[student@serverX ~]$ ssh-copy-id desktopX
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys
student@desktopX's password: student

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'student@desktopX'"
and check to make sure that only the key(s) you wanted were added.
```

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

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

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

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

```
PermitRootLogin no
PasswordAuthentication no
```

9.5. Reinicie el servicio sshd en serverX.

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

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

```
[student@desktopX ~]$ ssh root@serverX
Password: redhat
Permission denied, please try again.
Password: redhat
```

```
Permission denied, please try again.
Password: redhat
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

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

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

10.1 Identifique la zona horaria correcta para Bahamas en serverX.

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

The following information has been given:

  Bahamas

Therefore TZ='America/Nassau' will be used.
Local time is now: Fri Mar  7 09:38:50 EST 2014.
Universal Time is now: Fri Mar  7 14:38:50 UTC 2014.
Is the above information OK?
 1) Yes
 2) No
#? 1

You can make this change permanent for yourself by appending the line
  TZ='America/Nassau'; export TZ
to the file '.profile' in your home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that you
can use the /usr/bin/tzselect command in shell scripts:
America/Nassau
```

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

Capítulo 16. Revisión completa

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

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

```
[root@serverX ~]# timedatectl
    Local time: Wed 2014-04-09 18:21:06 CEST
    Universal time: Wed 2014-04-09 16:21:06 UTC
        RTC time: Wed 2014-04-09 16:21:06
       Timezone: America/Nassau (CEST, +0200)
      NTP enabled: yes
     NTP synchronized: no
      RTC in local TZ: no
        DST active: yes
Last DST change: DST began at
                  Sun 2014-03-30 01:59:59 CET
                  Sun 2014-03-30 03:00:00 CEST
Next DST change: DST ends (the clock jumps one hour backwards) at
                  Sun 2014-10-26 02:59:59 CEST
                  Sun 2014-10-26 02:00:00 CET
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

De manera alternativa:

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

- 13.4 Configure el archivo **hosts** para que 10.0.X.1 pueda denominarse como "myhost".

Capítulo 16. Revisión completa

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

13.5 Configure el nombre del host en el servidor X.example.com.

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

14. Sincronice el árbol de directorio **/etc** en serverX con el directorio **/configbackup** en serverX.

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

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

14.2 Cree el directorio de destino para los archivos de configuración en serverX.

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

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

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

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

15.1 Guarde el directorio **/configbackup** en el archivo **/root/configuration-backup-server.tar.gz**.

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

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

16.1 Conéctese a la máquina serverX como usuario root.

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

16.2 Cree el directorio de destino **/tmp/configcompare/** donde se extraerá el contenido del archivo **/root/configuration-backup-server.tar.gz**.

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

16.3 Cambie al directorio de destino **/tmp/configcompare/** en serverX.

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

16.4 Extraiga el contenido del archivo **/root/configuration-backup-server.tar.gz** en el directorio **/tmp/configcompare/** en serverX.

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

17. Realice las siguientes tareas en la máquina serverX:

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

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

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

17.2 Use **scp** para copiar el archivo **/tmp/scpfile.txt** de desktopX a **/home/student/scpfile.txt** en la máquina serverX.

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

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

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

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

19. Configure serverX para que respete los requisitos de software específicos:

- El paquete **núcleo** debe actualizarse a la versión más reciente.
- Debe instalarse el paquete **xsane-gimp**.

Capítulo 16. Revisión completa

- Debe instalarse el paquete **rht-system**.
- Por razones de seguridad, serverX no debe tener instalado el paquete **wvdial**.

19.1 Actualice el paquete **núcleo**.

```
yum update kernel
```

19.2 Instale el paquete **xsane-gimp**.

```
yum install xsane-gimp
```

19.3 Instale el paquete **rht-system**.

```
yum install rht-system
```

19.4 Por razones de seguridad, serverX no debe tener instalado el paquete **wvdial**.

```
yum remove wvdial
```

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

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

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

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

```
[root@serverX ~]# blkid  
/dev/vda1: UUID="46f543fd-78c9-4526-a857-244811be2d88" TYPE="xfs"  
/dev/vdb1: UUID="a84f6842-ec1d-4f6d-b767-b9570f9fc0" TYPE="xfs"
```

21.2 Cree el punto de montaje **/mnt/datadump** en serverX.

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

21.3 Monte el sistema de archivos mediante UUID en el directorio **/mnt/datadump** de la máquina serverX.

```
[root@serverX ~]# mount UUID="a84f6842-ec1d-4f6d-b767-b9570f9fc0" /mnt/  
datadump
```

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

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

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

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

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

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

Resumen

Revisión integral de Red Hat System Administration I

- Revise los capítulos para validar el nivel de conocimientos.
- Revise los ejercicios de práctica para validar el nivel de habilidades.