



Capacitación integral y práctica que resuelve los problemas del mundo real

RHCSA Rapid Track

Manual del alumno (ROLE)

RHCSA RAPID TRACK

Red Hat Enterprise Linux 7 RH199

RHCSA Rapid Track

Edición 3 20170803

Autores: Wander Boessenkool, Bruce Wolfe, Scott McBrien, George Hacker,

Chen Chang, Philip Sweany, Susan Lauber, Rudolf Kastl

Editor: Scott McBrien

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, Forrest Taylor, Steve Bonneville

Revisores: Christian Linden, Mathias Homann

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

Convenciones del documento	xii
Notas y advertencias	xi
Introducción	xiii
RHCSA Rapid Track	xiii
Orientación sobre el entorno del trabajo de laboratorio en el aula	xiv
Internacionalización	xvi
1. Inicios de sesión locales y remotos	1
Acceso a la línea de comandos a través de la consola local	2
Práctica: Terminales de acceso a la consola local	5
Configuración de autenticación basada en claves SSH	8
Práctica: Uso de la autenticación mediante claves SSH	10
Obtención de ayuda de Red Hat	11
Práctica: Crear y visualizar un SoS Report	17
2. Navegación por el sistema de archivos	21
Jerarquía del sistema de archivos Linux	22
Práctica: Jerarquía de sistemas de archivos	25
Administración de archivos con las herramientas de línea de comandos	28
Práctica: Administración de archivo de línea de comandos	33
Creación de enlaces entre archivos	36
Práctica: Creación de enlaces entre archivos	38
3. Usuarios y Grupos	41
Usuarios y Grupos	42
Práctica: Conceptos de usuario y grupo	45
Obtención de acceso de superusuario	47
Práctica: Ejecución de comandos como usuario root	51
Administración de cuentas de usuarios locales	54
Práctica: Creación de usuarios usando herramientas de la línea de comandos	58
Administración de cuentas de grupos locales	60
Práctica: Administración de grupos utilizando herramientas de línea de comandos	62
Administración de contraseñas de usuarios	64
Práctica: Administración de la antigüedad de la contraseña de usuario	68
Uso de servicios de administración de identidades	70
Práctica: Conexión a un servidor LDAP y Kerberos central	78
Trabajo de laboratorio: Administración de usuarios y grupos de Linux	81
4. Permisos de archivos	89
Administración de permisos del sistema de archivos desde la línea de comandos	90
Práctica: Administrar la seguridad de los archivos desde la línea de comandos	94
Administración de permisos predeterminados y acceso a archivos	96
Práctica: Control de permisos y propiedad de archivos nuevos	101
Listas de control de acceso (ACL) POSIX	103
Práctica: interpretar ACL	109
Protección de archivos con ACL	112
Práctica: Uso de ACL para otorgar y limitar el acceso	117
5. Permisos de SELinux	123
Habilitación y supervisión de Security Enhanced Linux (SELinux)	124
Práctica: Conceptos de SELinux	128
Cambio de modos de SELinux	130

Práctica: Cambio de modos de SELinux	132
Cambio de contextos de SELinux	133
Práctica: Cambio de contextos de SELinux	136
Cambio de booleanos de SELinux	138
Práctica: Cambio de booleanos de SELinux	140
Solución de problemas de SELinux	142
Práctica: Solución de problemas de SELinux	145
Trabajo de laboratorio: Administración de seguridad de SELinux	148
6. Administración de procesos	153
Finalización de procesos	154
Práctica: Finalización de procesos	159
Supervisión de la actividad de procesos	161
Práctica: Control de la actividad de proceso	165
Uso de nice y del cambio del valor de nice para influir en la prioridad de procesos ...	167
Práctica: Detección de prioridades de procesos	170
Trabajo de laboratorio: Administración de la prioridad de los procesos de Linux	173
7. Actualización de paquetes de software	177
Asignación de suscripciones a sistemas para actualizaciones de software	178
Práctica: Administración de suscripciones de Red Hat	184
Administración de actualizaciones de software con yum	186
Práctica: Instalación y actualización de software con yum	193
Habilitación de repositorios de software yum	197
Práctica: Habilitar repositorios de software	200
Ejercicio de laboratorio: Instalación y actualización de paquetes de software	202
8. Creación y montaje de sistemas de archivos	205
Montaje y desmontaje de sistemas de archivos	206
Práctica: Montar y desmontar sistemas de archivos	209
Adición de particiones, sistemas de archivos y montajes persistentes	211
Práctica: Agregar particiones, sistemas de archivos y montajes persistentes	224
Administración de espacio swap (intercambio)	227
Práctica: Agregar y habilitar espacio swap (intercambio)	231
Trabajo de laboratorio: Adición de discos, particiones y sistemas de archivos a un sistema Linux	235
9. Administración de servicios y resolución de problemas de arranque	243
Identificación de procesos del sistema comenzados en forma automática	245
Práctica: Identificar el estado de unidades systemd	249
Control de servicios del sistema	251
Práctica: Uso de systemctl para administrar servicios	255
El proceso de arranque de Red Hat Enterprise Linux	257
Práctica: Selección de un objetivo de arranque	262
Reparación de problemas de arranque comunes	264
Práctica: restablecimiento de una contraseña root perdida	268
Reparación de problemas del sistema de archivos en el arranque	270
Práctica: Reparación de problemas en el arranque	271
Reparación de problemas del cargador de arranque	273
Práctica: Reparación de un problema del cargador de arranque	275
Ejercicio de laboratorio: Control de servicios y demonios	277
10. Configuración de red	281
Validación de la configuración de red	282

Práctica: Cómo examinar la configuración de red	285
Configuración de red con nmcli	287
Práctica: Configuración de red con nmcli	292
Edición de archivos de configuración de red	295
Práctica: Edición de archivos de configuración de red	297
Configuración de nombres de host y resolución de nombre	299
Práctica: Configuración de nombres de hosts y resolución de nombres	302
Ejercicio de laboratorio: Administración de la red de Red Hat Enterprise Linux	305
11. Registro del sistema y NTP	309
Arquitectura de registro del sistema	310
Práctica: Componentes de registro de sistema	312
Revisión de archivos Syslog	315
Práctica: Encontrar entradas de registro	319
Revisión de las entradas del journal (diario) de systemd	320
Práctica: búsqueda de eventos con journalctl	323
Preservando el journal (diario) de systemd	324
Práctica: Configuración del journal (diario) de systemd constante	326
Mantenimiento de la hora correcta	327
Práctica: Ajuste de la hora del sistema	331
Ejercicio de laboratorio: Análisis y almacenamiento de registros	334
12. Administración de volúmenes lógicos	339
Gestión de volúmenes lógicos	340
Práctica: Adición de un volumen lógico	346
Extensión de volúmenes lógicos	351
Práctica: Ampliación de un volumen lógico	356
Trabajo de laboratorio: Administración del almacenamiento de gestión de volúmenes lógicos (LVM)	359
13. Procesos programados	367
Programación de trabajos cron del sistema	368
Práctica: Programación de trabajos cron del sistema	370
Administración de archivos temporales	372
Práctica: Administración de archivos temporales	375
14. Montaje de sistemas de archivos de red	379
Montaje de almacenamiento de red con NFS	380
Práctica: Montaje y desmontaje de NFS	383
Automontaje de almacenamiento de red con NFS	387
Práctica: Automontaje de NFS	391
Acceso a almacenamiento de red con SMB	395
Práctica: Montaje de un sistema de archivos de SMB	399
Trabajo de laboratorio: Acceso a almacenamiento de red con sistema de archivos de red (NFS)	402
Trabajo de laboratorio: Acceso a almacenamiento de red con SMB	407
15. Configuración del firewall	417
Limitación de la comunicación de red	418
Práctica: Limitación de la comunicación de red	426
Trabajo de laboratorio: Limitación de la comunicación de red	428
16. Virtualización y Kickstart	433
Definición del sistema Anaconda Kickstart	434

Práctica: Sintaxis y modificación del archivo Kickstart	440
Implementación de un nuevo sistema virtual con Kickstart	444
Práctica: Instalación de un sistema usando Kickstart	448
Administración de un host de virtualización local	451
Práctica: Administración de un host de virtualización local	457

Convenciones del documento

Notas y advertencias



Nota

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



Referencias

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



Importante

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



Advertencia

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

Introducción

RHCSA Rapid Track

El curso RHCSA Rapid Track (RH199) está diseñado para estudiantes que ya tienen una experiencia significativa en la administración de Linux. El curso RHCSA Rapid Track revisa las tareas tratadas en los cursos System Administration I y II a un ritmo acelerado. El curso se desarrolla sobre la comprensión fundacional de los estudiantes respecto de la administración de Linux basada en la línea de comandos. Los estudiantes deberán poder ejecutar comandos comunes, tales como cp, grep, sort, mkdir, tar, mkfs, ssh y yum desde el prompt de comandos. Además, deben estar familiarizados con opciones de comando comunes y con el acceso a las páginas del manual para obtener ayuda. Se recomienda a los estudiantes que no posean estos conocimientos que realicen el curso Red Hat System Administration I (RH124).

Objetivos del curso

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

Destinatarios

- El curso RHCSA Rapid Track (RH199/RH200) se encuentra entre los cursos más importantes en la cartera de Linux. Está diseñado para ser un punto de entrada de currículos para profesionales de TI con significativa exposición a la administración de Linux. Este curso cubre 9 días de contenido compactado de System Administration I y II en 4 días. Para hacerlo, se requiere que los conceptos elementales no se cubran o que solo se lo haga rápidamente. Se recomienda firmemente a los estudiantes que no estén seguros si están calificados para tomar el RH199 que realicen la evaluación previa en línea.

Requisitos previos

- Los estudiantes de este curso deben tener una experiencia de entre uno y tres años a tiempo completo en la administración de sistemas Linux.

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 *root* 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 "switch de seguridad", que disminuye mientras funciona su máquina. Si el temporizador se reduce por debajo de 0, puede optar por incrementar el temporizador.

Internacionalización

Compatibilidad de idioma

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

Selección de idioma por usuario

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

Configuración de idioma

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

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

nota

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

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

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

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

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

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

Valores del método de entrada

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

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

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

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

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

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



nota

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

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

Valores de idioma predeterminado en todo el sistema

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

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

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

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

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



Importante

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

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

Paquetes de idiomas

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



Referencias

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

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

Referencia de códigos de idioma

Códigos de idioma

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



CAPÍTULO 1

INICIOS DE SESIÓN LOCALES Y REMOTOS

Descripción general	
Meta	Revisar los métodos de acceso al sistema y solicitud de soporte de Red Hat.
Objetivos	<ul style="list-style-type: none">Utilizar la sintaxis de la shell Bash para ingresar comandos en una consola Linux.Configurar ssh para permitir inicios de sesión seguros sin contraseña mediante el uso de un archivo de clave de autenticación privada.Usar el comando redhat-support-tool.
Secciones	<ul style="list-style-type: none">Acceso a la línea de comandos a través de la consola local (y práctica)Configuración de autenticación con clave de SSH (y práctica)Obtención de ayuda de Red Hat (y práctica)

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 *prompt de shell*. Cuando un usuario regular inicia una shell, el prompt 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 prompts 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 prompt 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 prompts 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 prompts 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 prompt 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. Inicios de sesión locales y remotos

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	Prompt	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.	Prompt
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

Configuración de autenticación basada en claves 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, 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.

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 |
| + + . |
| 0.E   |
| 0 0o+oo |
| .=,*'000 |
+-----+
```

- 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
```

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

Figura 1.1: 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
```

Capítulo 1. Inicios de sesión locales y remotos

```
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

Capítulo 1. Inicios de sesión locales y remotos

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 el prompt 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
-----
```

```
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 stacks (pilas) 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
```

Capítulo 1. Inicios de sesión locales y remotos

```
The checksum is: b2e78125290a4c791162e68da8534887  
Please send this file to your support representative.
```

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

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

4. 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 principal.

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

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**.

Configuración de autenticación basada en claves SSH

Con el uso de la autenticación mediante llaves SSH, la administración remota de sistemas obtiene seguridad adicional.

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 2

NAVEGACIÓN POR EL SISTEMA DE ARCHIVOS

Descripción general	
Meta	Copiar, mover, crear, eliminar, vincular y organizar archivos mientras se trabaja desde el prompt de la shell Bash.
Objetivos	<ul style="list-style-type: none">Identificar el objetivo de directorios importantes en un sistema Linux.Crear, copiar, mover y quitar archivos y directorios usando utilidades de la línea de comandos.Usar enlaces físicos y enlaces simbólicos para crear múltiples nombres.
Secciones	<ul style="list-style-type: none">Jerarquía del sistema de archivos Linux (y práctica)Administración de archivos con las herramientas de línea de comandos (y práctica)Creación de enlaces entre archivos (y práctica)

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 root del árbol está en la parte *superior* de la jerarquía y las ramas de los directorios y subdirectorios se extienden debajo de root.

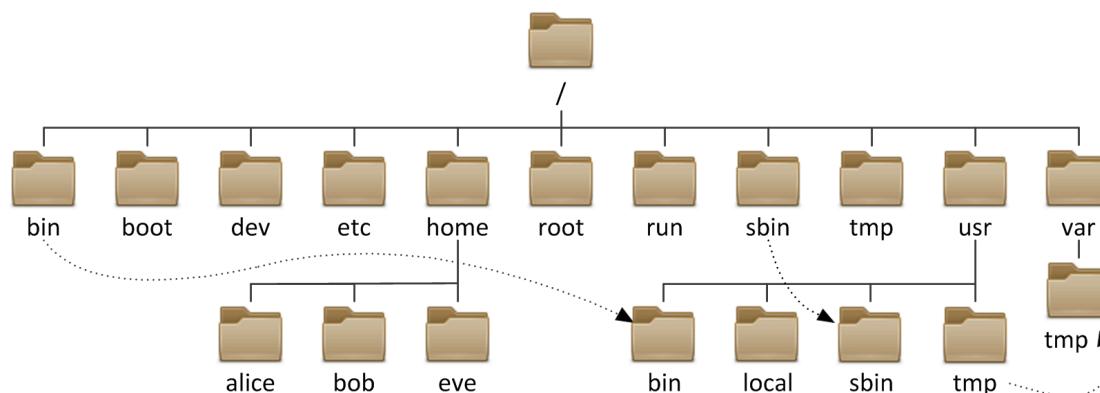


Figura 2.1: Directories del sistema de archivos importantes en Red Hat Enterprise Linux 7

El directorio `/` es el directorio root 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 root, 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.
- *persistente* 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, librerías 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	<i>Los directarios de inicio</i> 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 librerías 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 librerías y los programas de software instalados.	/usr

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:	<p>⁽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.</p>	

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. Navegación por el sistema de archivos

```
[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. Navegación por el sistema de archivos

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
```

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
```

Resumen

Jerarquía del sistema de archivos Linux

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

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.

Creación de enlaces entre archivos

El manejo de los enlaces a archivos existentes permite ahorrar espacio en el sistema de archivos.



CAPÍTULO 3

USUARIOS Y GRUPOS

Descripción general	
Meta	Administrar usuarios y grupos de Linux y administrar políticas 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 política de antigüedad de contraseña en el archivo de contraseña shadow.• Usar servicios de administración de identidades centralizados.
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)• Uso de servicios de administración de identidades (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):

① username: ② password: ③ UID: ④ GID: ⑤ GECOS: ⑥ /home/dir: ⑦ shell

- 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 prompt 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 librería 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 prompt 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 prompt 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 prompt 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 (prompt 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 prompt 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 librería 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 un prompt 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 prompt 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 3. Usuarios y Grupos

```
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 prompt 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.

id muestra la información del usuario.

- **id** mostrará la información del usuario, incluido el número UID del usuario y las membresías a grupos.

- **id username** mostrará la información del usuario para *nombre de usuario*, incluido el número UID del usuario y las membresías a grupos.

passwd establece contraseñas

- **passwd username** se puede usar para establecer la contraseña inicial o cambiar la contraseña del usuario.
- 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 prompt 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 del pool (conjunto) 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 un prompt BASH.
3. Seleccione **Applications > Utilities > Terminal**.
4. Conviértase en el usuario **root** en el prompt 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 modifica la pertenencia a grupos.**usermod**

- 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. Conviértase en el usuario **root** en el prompt 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: el algoritmo hash. El número 1 indica un hash MD5. El número 6 aparece cuando se usa un hash SHA-512.
- 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**.
- 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

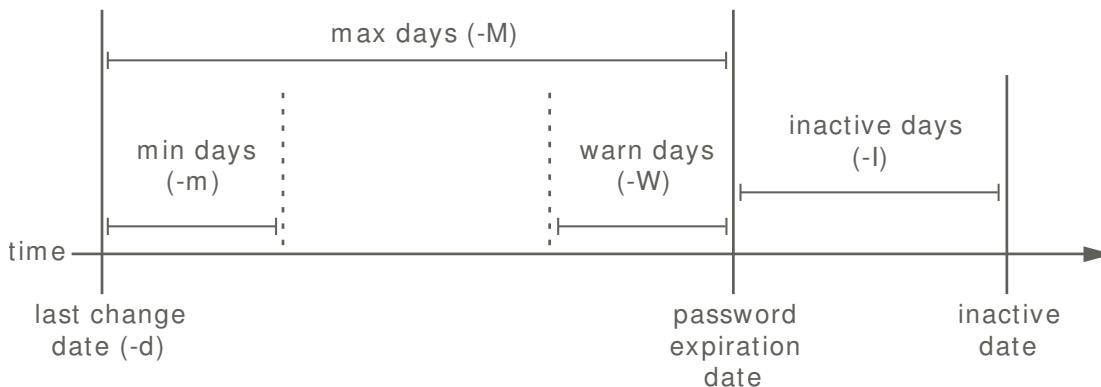
El formato de **/etc/shadow** es el siguiente (nueve campos separados por dos puntos):

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(1)**, **usermod(8)**, **shadow(5)**, **crypt(3)**

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.

Andes 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
```

Uso de servicios de administración de identidades

Objetivos

Luego de completar esta sección, los estudiantes deberían poder usar servicios de administración de identidad centralizados.

Servicios de información del usuario y de autenticación

Necesidad de administración de identidad centralizada

Las infraestructuras de computación modernas tienden a constar de muchas máquinas, con varios servicios en ejecución. Mantener las cuentas de usuarios locales de todas estas máquinas y sus servicios en sincronización es una tarea abrumadora, más aún cuando las contraseñas deben mantenerse sincronizadas.

Una solución para esto es no almacenar información de las cuentas en sistemas locales, sino recuperar esta información de un almacenamiento centralizado. Tener la información del usuario y la información de autenticación asociada centralizadas también permite lo que se denomina *Single Sign-On* (SSO). Con SSO, un usuario autentica una vez usando una contraseña (u otros medios) y luego obtiene una forma de vale o cookie que se puede usar para autenticar automáticamente a otros servicios.

Autenticación e información del usuario

Se necesitará un sistema de identidad centralizado para proporcionar al menos dos servicios:

1. *Información de la cuenta*: Esto incluye información como nombre de usuario, ubicación del directorio de inicio, UID y GID, membresías de grupos, etc. Las soluciones populares incluyen LDAP (Lightweight Directory Access Protocol), usada en varios productos como Active Directory y IPA Server, y Network Information Services (NIS).
2. *Información de autenticación*: Un medio para un sistema de validar que un usuario es quien dice que es. Esto se puede hacer al proporcionar un hash de contraseña criptográfico al sistema de cliente, o al enviar la contraseña (cifrada) al servidor, y recibir una respuesta. Un servidor LDAP puede proporcionar información de autenticación además de información de la cuenta. Kerberos solo proporciona servicios de autenticación SSO, y se usa típicamente junto con la información del usuario de LDAP. Kerberos se usa tanto en IPA Server como en Active Directory.

En un sistema Red Hat Enterprise Linux 7, **/etc/passwd** proporciona la información del usuario local, mientras que **/etc/shadow** proporciona la información de autenticación (en la forma de una contraseña con hash).

Conexión de un sistema a servidores LDAP y Kerberos centralizados

Authconfig

La configuración de un sistema Red Hat Enterprise Linux 7 para usar servicios de administración de identidad centralizados requiere la edición de varios archivos y la configuración de algunos daemons. Para conectar a servidores LDAP y Kerberos centrales, como mínimo, se deberán actualizar los siguientes archivos:

- **/etc/openldap/ldap.conf**: Para información sobre el servidor LDAP central y su configuración.
- **/etc/krb5.conf**: Para información sobre la infraestructura de Kerberos central.
- **/etc/sssd/sssd.conf**: Para configurar el *daemon de servicios de seguridad del sistema (sssd)*, el daemon responsable de la recuperación y el almacenamiento en caché de la información del usuario e información de autenticación.
- **/etc/nsswitch.conf**: Para indicarle al sistema qué servicios de autenticación e información del usuario se deben usar.
- **/etc/pam.d/***: Configuración de cómo se debe manejar la autenticación para varios servicios.
- **/etc/openldap/cacerts**: Para almacenar las *autoridades de certificación (CA) root* que pueden validar los certificados de SSL usados para identificar los servidores LDAP.

El daemon **sssd** deberá habilitarse e iniciarse para que el sistema pueda usarse.

Con esta cantidad de archivos y servicios para configurar, es fácil cometer un error. Red Hat Enterprise Linux 7 se envía con un conjunto de herramientas para automatizar estas configuraciones: **authconfig**. **authconfig** consta de tres herramientas relacionadas que pueden realizar las mismas acciones:

- **authconfig**: Una herramienta de línea de comandos. Esta herramienta se puede usar para automatizar configuraciones en varios sistemas. Los comandos usados con **authconfig** tienden a ser muy extensos, con múltiples opciones que se especifican. Esta herramienta se instala usando el paquete *authconfig*.
- **authconfig-tui**: La versión interactiva de **authconfig**. Usa una interfaz de texto guiada por un menú. Se puede usar sobre **ssh**. Esta herramienta se instala usando el paquete *authconfig*.
- **authconfig-gtk**: Esta versión inicia una interfaz gráfica. También se puede iniciar como **system-config-authentication**. Esta herramienta se instala usando el paquete *authconfig-gtk*.

Parámetros de LDAP necesarios

Para conectar a un servidor de LDAP central para obtener información del usuario, **authconfig** necesita varias configuraciones:

- El nombre del host de los servidores LDAP

Capítulo 3. Usuarios y Grupos

- El *base DN* (nombre distinguido) de la parte del árbol de LDAP donde el sistema debe buscar usuarios. Generalmente, esto se ve de forma similar a **dc=example, dc=com**, o **ou=People, o=PonyCorp**. Esta información será proporcionada por su administrador de servidores de LDAP.
- Si se usa SSL/TLS para codificar comunicaciones con el servidor LDAP, el servidor LDAP ofrece un certificado CA root que puede validar el certificado.

Importante: Un sistema también necesitará que se instalen paquetes adicionales para proporcionar funcionalidad del cliente LDAP. La instalación de *sssd* proporcionará todas las dependencias necesarias.

Parámetros de Kerberos necesarios

Para configurar un sistema para que use un sistema Kerberos centralizado para la autenticación del usuario, **authconfig** necesitará las siguientes configuraciones:

- El nombre del *dominio Kerberos* que se utilizará. Un dominio Kerberos es un dominio de máquinas que usan un conjunto común de usuarios y servidores Kerberos para la autenticación.
- Uno o más *centros de distribución de claves* (KDC). Este es el nombre de host de sus servidores Kerberos.
- El nombre de host de uno o más *admin servers (servidores de administración)*. Esta es la máquina con la que el cliente hablará cuando desee cambiar su contraseña o realizar otras modificaciones de usuario. Generalmente, esta es la misma que la del KDC primario, pero puede ser una máquina diferente.

Además, un administrador puede especificar si DNS debe usarse para buscar el dominio que se usará para un nombre de host específico y para encontrar automáticamente los servidores de administración y los KDC. Se puede instalar un paquete adicional para ayudar a resolver problemas de Kerberos y para que funcionen con vales de Kerberos de la línea de comandos: *krb5-workstation*.

Uso de authconfig-gtk

Para usar **authconfig-gtk** para configurar un sistema para LDAP + Kerberos, use los siguientes pasos:

1. Instale todos los paquetes necesarios:

```
[student@demo ~]$ sudo yum -y install authconfig-gtk sssd krb5-workstation
```

2. Inicie **authconfig-gtk**, desde la línea de comandos o desde Applications (Aplicaciones) > Sundry > Authentication (Autenticación). Ingrese la contraseña **root** cuando se la solicite.
3. En la pestaña **Identity & Authentication** (Identidad y autenticación), seleccione **LDAP** del menú desplegable **User Account Database drop-down**. Complete los campos **LDAP Search Base DN** (Nombre distinguido base de búsqueda de LDAP) y **LDAP Server** (Servidor LDAP).

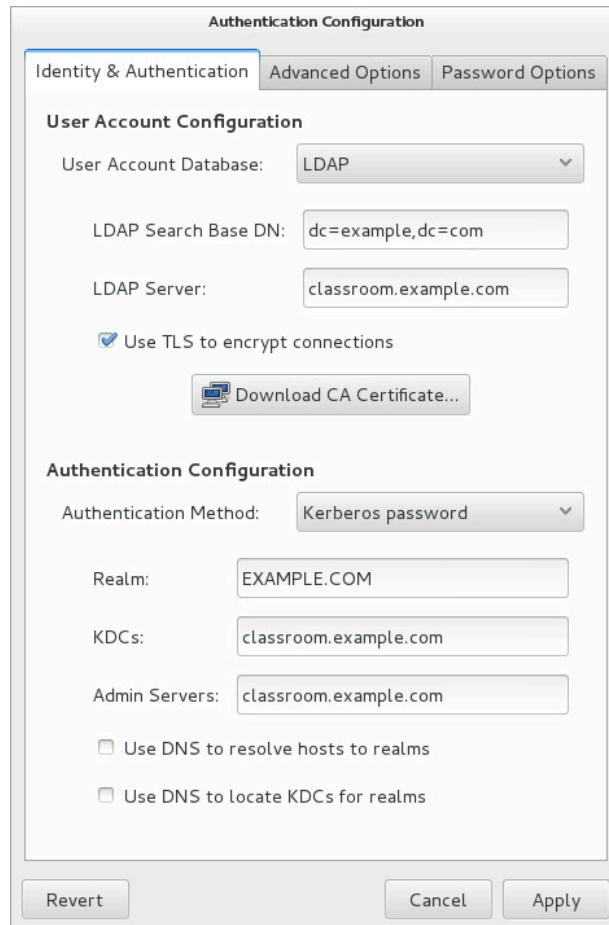


Figura 3.2: Ventana de authconfig-gtk principal

4. Si el servidor LDAP admite TLS, marque la casilla **Use TLS to encrypt connections** (Usar TLS para cifrar conexiones) y use el botón **Download CA Certificate** (Descargar certificado CA) para descargar el certificado CA.
5. En el menú desplegable **Authentication Method** (Método de autenticación), seleccione **Kerberos password** (Contraseña de Kerberos) y complete los campos **Realm** (Dominio), **KDCs** (KDC) y **Admin Servers** (Servidores de administración). Los últimos dos campos no están disponibles si la opción **Use DNS to locate KDCs for realms** (Usar DNS para localizar KDC para dominios) está marcada.
6. Si los directorios de inicio centrales no están disponibles, los usuarios pueden crear directorios en el primer inicio de sesión al marcar el cuadro **Create home directories on the first login** (Crear directorios de inicio en el primer inicio de sesión) en la pestaña **Advanced Options** (Opciones avanzadas).
7. Haga clic en el botón **Apply** (Aplicar) para guardar y activar los cambios. Esto escribirá todos los archivos de configuración relevantes y (re)iniciará el servicio **sssd**.



Advertencia

Debido a un error conocido (https://bugzilla.redhat.com/show_bug.cgi?id=1184639) en **authconfig-6.2.8-8.el7** genera un valor de krb5_realm falso como '#' en **/etc/sssd/sssd.conf**. Cuando utilice **authconfig-gtk**, se podrá evitar este problema si se elimina el valor predeterminado '#' del campo **Realm** (Dominio). Además, cuando utilice la línea de comandos de **authconfig**, asegúrese de utilizar la opción **--krb5realm=** para ingresar en un dominio cuando corresponda y verificar los archivos **/etc/krb5.conf** y **/etc/sssd/sssd.conf** en busca de valores dañados.

El soporte de producto de Red Hat proporcionó una versión de errata **authconfig-6.2.8-10.el7** que resuelve este problema para los entornos de producción. Consulte: <https://rhn.redhat.com/errata/RHBA-2015-2403.html>

Prueba de configuración

Para probar la configuración LDAP + Kerberos, un administrador puede simplemente intentar iniciar sesión en el sistema (mediante **ssh**) usando las credenciales de uno de los usuarios de red. Además, el comando **getent** se puede usar para recuperar información sobre un usuario de red, en la forma **getent passwd <USERNAME>**.

Importante: En la configuración predeterminada, **sssd** no enumerará usuarios de red cuando *no* se especifique un nombre de usuario para el comando **getent**. Esto se hace para mantener la pantalla de inicio de sesión gráfica despejada y para ahorrar tiempo y fuentes de red valiosos.

Conexión de un sistema a un servidor IPA

Red Hat proporciona una solución integrada para configurar LDAP y Kerberos: servidor IPA (Identity, Policy, and Auditing [Identidad, política y auditoría]). El servidor IPA proporciona LDAP y Kerberos, combinados con un conjunto de herramientas de administración basadas en la Web y de línea de comandos. Además de la información del usuario y de autenticación, el servidor IPA puede centralizar reglas **sudo**, claves públicas SSH, llaves de host SSH, certificados TLS, mapas de servicio de automontaje y mucho más.

Uso de ipa-client

Un sistema Red Hat Enterprise Linux 7 se puede configurar para usar un servidor IPA mediante el conjunto de herramientas **authconfig**, pero también existe una herramienta especializada: **ipa-client-install**. Este comando se puede instalar desde el paquete *ipa-client*, que extrae todas las dependencias (como *sssd*).

Uno de los beneficios de usar **ipa-client-install** es que puede recuperar casi toda la información necesaria de DNS (cuando es configurado por el servidor IPA o manualmente por un administrador), así como crear entradas de host y más en el servidor IPA. Esto permite que un administrador de servidores IPA establezca políticas de acceso, cree *directores de servicio* (p. ej., para exportaciones NFSv4) y más.

Cuando **ipa-client-install** se ejecuta sin ningún argumento, primero intentará recuperar información sobre el servidor IPA configurado para su dominio DNS de DNS. Si eso falla, se le solicitará al administrador la información necesaria, como el nombre del dominio del servidor de IPA y el dominio que se usará. Otra información que debe proporcionarse

es el nombre de usuario y la contraseña de una cuenta que tiene permitido crear nuevas entradas de la máquina en el servidor IPA. Se puede usar la cuenta del administrador del servidor IPA predeterminada (**admin**), a menos que se haya creado otra cuenta para esto.

A continuación, se muestra un ejemplo de una configuración guiada (mayormente) por DNS:

```
[student@desktop ~]$ sudo ipa-client-install
Discovery was successful!
Hostname: desktop.domain0.example.com
Realm: DOMAIN0.EXAMPLE.COM
DNS Domain: server.domain0.example.com
IPA Server: server.domain0.example.com
BaseDN: dc=server,dc=domain0,dc=example,dc=com

Continue to configure the system with these values? [no]: yes
User authorized to enroll computers: admin
Synchronizing time with KDC...
Password for admin@DOMAIN0.EXAMPLE.COM: redhat123
Successfully retrieved CA cert
  Subject: CN=Certificate Authority,O=DOMAIN0.EXAMPLE.COM
  Issuer:  CN=Certificate Authority,O=DOMAIN0.EXAMPLE.COM
  Valid From: Thu Feb 27 13:31:04 2014 UTC
  Valid Until: Mon Feb 27 13:31:04 2034 UTC

Enrolled in IPA realm DOMAIN0.EXAMPLE.COM
Created /etc/ipa/default.conf
New SSSD config will be created
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm DOMAIN0.EXAMPLE.COM
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Client configuration complete.
```

Es posible especificar toda la información necesaria como argumentos de línea de comando, permitiendo configuraciones desatendidas como parte de una configuración inicial del sistema; por ejemplo, desde un *kickstart*. Consulte la página del manual para **ipa-client-install(1)** para obtener más información.

Unión de un sistema con Active Directory

Red Hat Enterprise Linux 7 presenta varios métodos de unión de un sistema con Active Directory. Los administradores pueden elegir instalar el paquete *samba-winbind* y configurar **winbind** a través de la familia de herramientas **authconfig**, o los administradores pueden instalar los paquetes *sssd* y *realm* y usar **sssd** y el comando **realm**.



nota

El comando **realm** también se puede usar para unirse a dominios de Kerberos, o dominios de servidores IPA, pero la configuración final será ligeramente diferente; por ejemplo, los usuarios tendrán **@domain** anexado a sus nombres de usuario. **ipa-client-install** es el método preferido para unirse a dominios IPA.



nota

Debido a que no hay un servidor de Active Directory ejecutándose en el aula, no hay una posibilidad actual de practicar estos pasos.

El siguiente es un ejemplo del uso de **realmd** para unirse un dominio de Active Directory y permitir a los usuarios de Active Directory iniciar sesión en el sistema local. En este ejemplo, se supone que el dominio de Active Directory se denomina **domain.example.com**.

1. Instale los paquetes necesarios: *realmd*.

```
[student@demo ~]$ sudo yum -y install realm
```

2. Descubra la configuración para el dominio **domain.example.com**.

```
[student@demo ~]$ sudo realm discover domain.example.com
```

3. Únase al dominio de Active Directory; esto instalará todos los paquetes necesarios y configurará **sssd**, **pam**, **/etc/nsswitch.conf**, etcétera.

```
[student@demo ~]$ sudo realm join domain.example.com
```

Esto intentará unir el sistema local con Active Directory usando la cuenta **Administrator**; ingrese la contraseña para esta cuenta cuando se lo solicite. Para usar una cuenta diferente, use el argumento **--user**.

4. Las cuentas de Active Directory ahora se pueden utilizar en el sistema local, pero los inicios de sesión usando Active Directory aún están deshabilitados. Para habilitar inicios de sesión, use el siguiente comando:

```
[student@demo ~]$ sudo realm permit --realm domain.example.com --all
```

Para solo permitir a ciertos usuarios iniciar sesión, reemplace **--all** con una lista de esos usuarios. Por ejemplo:

```
[student@demo ~]$ sudo realm permit --realm domain.example.com DOMAIN\\Itchy DOMAIN\\Scratchy
```



nota

De forma predeterminada, los usuarios del dominio deben usar su nombre calificado completo para iniciar sesión; p. ej., **ipauser@ipa.example.com** para usuarios IPA o **DOMAIN\Picard** para Active Directory. Para deshabilitar esto, cambie la configuración de **use_fully_qualified_names** en el bloque del dominio correcto en **/etc/sssd/sssd.conf** a False (Falso) o elimínelo por completo; luego reinicie el servicio **sssd**.



Referencias

Páginas del manual: **authconfig(8)**, **authconfig-tui(8)**, **authconfig-gtk(8)**,
sssd(8), **sssd-ipa(8)**, **sssd . conf(5)**, **sssd-ad** y **realm(8)**

Práctica: Conexión a un servidor LDAP y Kerberos central

En este trabajo de laboratorio, conectará su sistema **desktopX** para convertirlo en un cliente del servidor LDAP que se ejecuta en **classroom.example.com**. Configurará su sistema **desktopX** para usar la infraestructura Kerberos proporcionada por **classroom.example.com** para obtener una autenticación adicional.

Recursos:	
Archivos:	http://&clrmfqdn;/pub/example-ca.crt
Máquinas:	desktopX

Resultados:

desktopX configurado para información de usuario de LDAP y autenticación de Kerberos desde **classroom.example.com**.

Andes de comenzar

- Restablezca su sistema **desktopX**.

Para simplificar la administración del usuario, su empresa ha decidido cambiar a administración de usuario centralizada. Otro equipo ya ha configurado todos los servicios de LDAP y Kerberos obligatorios. Los directorios iniciales centralizados aún no están disponibles, de modo que el sistema debe configurarse para crear directorios iniciales locales cuando un usuario inicie sesión por primera vez.

Dada la siguiente información, configure su sistema **desktopX** para que use la información de usuario del servidor LDAP y los servicios de autenticación del KDC de Kerberos. Los registros del servicio DNS para el dominio aún no se han configurado, de modo que tendrá que configurar manualmente los parámetros de Kerberos.

Nombre	Valor
Servidor LDAP	ldap://classroom.example.com
DN de base de LDAP	dc=example,dc=com
Usar TLS	Sí
CA root	http://classroom.example.com/pub/example-ca.crt
Dominio de Kerberos	EXAMPLE.COM
KDC de Kerberos	classroom.example.com
Servidor de administración de Kerberos:	classroom.example.com

- Comience por instalar los paquetes necesarios: *sssd*, *krb5-workstation* y *authconfig-gtk*.

1.1. [student@desktopx ~]\$ sudo yum -y install sssd authconfig-gtk krb5-workstation

-
2. Inicie la aplicación **Authentication Configuration** (Configuración de autenticación), luego aplique la configuración de la tabla para las opciones LDAP y Kerberos.
- 2.1. Inicie **system-config-authentication** desde la línea de comandos o inicie **Applications (Aplicaciones) > Sundry > Authentication (Autenticación)**. Ingrese la contraseña de **student (student)** cuando se le solicite.
 - 2.2. Asegúrese de que la pestaña **Identity & Authentication** (Identidad y autenticación) esté abierta.
 - 2.3. En **User Account Database** (Base de datos de la cuenta del usuario), seleccione **LDAP**.
 - 2.4. Ingrese **dc=example,dc=com** en el campo **LDAP Search Base DN** (DN de base de búsqueda de LDAP) y **classroom.example.com** en el campo **LDAP Server** (Servidor LDAP).
 - 2.5. Asegúrese de que el cuadro **Use TLS to encrypt connections** (Usar TLS para cifrar conexiones) esté marcado, y luego haga clic en el botón **Download CA Certificate...** (Descargar certificado de CA...).
 - 2.6. Ingrese **http://classroom.example.com/pub/example-ca.crt** en el campo **Certificate URL** (URL del certificado) y, luego haga clic en **OK** (Aceptar).
 - 2.7. Seleccione **Kerberos password** (Contraseña de Kerberos) en el menú desplegable **Authentication Method** (Método de autenticación) y quite la marca de los dos cuadros **Use DNS...** (Usar DNS...).
 - 2.8. Ingrese **EXAMPLE.COM** en el campo **REALM** (DOMINIO) y **classroom.example.com** en los campos **KDCs** (KDC) y **Admin Servers** (Servidores de administración).
 - 2.9. Cambie a la pestaña **Advanced Options** (Opciones avanzadas) y coloque una marca de verificación en el cuadro **Create home directories on the first login** (Crear directorios iniciales en el primer inicio de sesión).
 - 2.10 Haga clic en el botón **Apply** (Aplicar) para aplicar los cambios.
3. Use tanto **getent** como **ssh** para verificar su trabajo. Puede usar el nombre de usuario **ldapuserX** (donde **X** es el número de su estación) con la contraseña **kerberos**. Tenga en cuenta que sus usuarios aún no tienen un directorio principal montado.
- 3.1.

```
[student@desktopX ~]$ getent passwd ldapuserX
ldapuserX:*:170X:170X:LDAP Test User X:/home/guests/ldapuserX:/bin/bash
```
 - 3.2.

```
[student@desktopX ~]$ ssh ldapuserX@localhost
The authenticity of host 'localhost (::1)' can't be established.
EDCSA key fingerprint is XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (EDCSA) to the list of known hosts.
ldapuserX@localhost's password: kerberos
Creating home directory for ldapuserX.
[ldapuserX@desktopX ~]$ pwd
/home/guests/ldapuserX
[ldapuserX@desktopX ~]$ ls -a
. .bash_history .bash_profile .cache .mozilla
```

Capítulo 3. Usuarios y Grupos

```
.. .bash_logout .bashrc .config  
[ldapuserX@desktopX ~]$ logout
```

Trabajo de laboratorio: Administración de usuarios y grupos de Linux

En este trabajo de laboratorio, trabajará en **desktopX** para definir un grupo de cuentas de usuario locales y configurar la máquina para usar cuentas de usuario definidas por la red. 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 desktopX 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 vencer al final del contrato de 90 días y Betty Boop debe cambiar su contraseña cada 15 días.
- **desktopX** es un cliente para el servidor IPA que se ejecuta en serverX y puede usar las cuentas definidas en IPA para la autenticación.

Andes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX**. Observación: Este paso llevará unos 15 minutos aproximadamente.

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

- Restablezca su sistema **desktopX** mientras la configuración de **serverX** se esté ejecutando.
- Espere que su sistema serverX finalice antes de continuar.

La configuración relevante para el servidor IPA existente es la siguiente:

Nombre	Valor
Dominio	SERVERX.EXAMPLE.COM , donde X es el número de su estación.
Dominio	serverX.example.com , donde X es el número de su estación. Observe que su máquina desktopX no es parte de este dominio DNS.
Usuario administrativo	admin
Contraseña	redhat123

Ya se ha configurado a un usuario para que realice la evaluación. El nombre de usuario es **ipauser** y la contraseña es **password**. Debido a la política de contraseñas, esta contraseña deberá cambiarse en el primer inicio de sesión. Cambie esta contraseña a **redhat123**.

Capítulo 3. Usuarios y Grupos

Los directorios de inicio centrales aún no se han configurado, de modo que, por ahora, configure el sistema para que cree automáticamente un nuevo directorio de inicio local cuando un usuario inicia sesión por primera vez.

Cuando haya finalizado su trabajo, ejecute **lab combined-users grade** en su máquina **desktopX** para verificar su trabajo.

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 un GID de 900.
3. Cree tres usuarios nuevos: **sspadé**, **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. Instale el paquete *ipa-client* en su máquina **desktopX**.
8. Configure su sistema, con **ipa-client-install**, para usar la configuración del servidor IPA para el dominio DNS de **serverX.example.com**. Los directorios de inicio deben crearse automáticamente y, durante este proceso, NTP no se debe configurar.
9. Verifique que ahora pueda iniciar sesión satisfactoriamente en **desktopX** con el usuario **ipauser** mediante el uso de **ssh**. La contraseña inicial es **password**, pero se debe cambiar a **redhat123**. Debido al requisito de cambio de contraseña, tendrá que iniciar sesión dos veces.
10. Cuando finalice, ejecute el script de evaluación **lab combined-users grade** para confirmar que se hayan realizado todos los pasos de forma correcta.

Solución

En este trabajo de laboratorio, trabajará en **desktopX** para definir un grupo de cuentas de usuario locales y configurar la máquina para usar cuentas de usuario definidas por la red. 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 desktopX 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 vencer al final del contrato de 90 días y Betty Boop debe cambiar su contraseña cada 15 días.
- **desktopX** es un cliente para el servidor IPA que se ejecuta en serverX y puede usar las cuentas definidas en IPA para la autenticación.

Andes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX**. Observación: Este paso llevará unos 15 minutos aproximadamente.

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

- Restablezca su sistema **desktopX** mientras la configuración de **serverX** se esté ejecutando.
- Espere que su sistema serverX finalice antes de continuar.

La configuración relevante para el servidor IPA existente es la siguiente:

Nombre	Valor
Dominio	SERVERX.EXAMPLE.COM , donde X es el número de su estación.
Dominio	serverX.example.com , donde X es el número de su estación. Observe que su máquina desktopX no es parte de este dominio DNS.
Usuario administrativo	admin
Contraseña	redhat123

Ya se ha configurado a un usuario para que realice la evaluación. El nombre de usuario es **ipauser** y la contraseña es **password**. Debido a la política de contraseñas, esta contraseña deberá cambiarse en el primer inicio de sesión. Cambie esta contraseña a **redhat123**.

Los directorios de inicio centrales aún no se han configurado, de modo que, por ahora, configure el sistema para que cree automáticamente un nuevo directorio de inicio local cuando un usuario inicia sesión por primera vez.

Capítulo 3. Usuarios y Grupos

Cuando haya finalizado su trabajo, ejecute **lab combined-users grade** en su máquina **desktopX** para verificar su trabajo.

1. Asegúrese de que los usuarios creados recientemente tengan contraseñas que se deben cambiar cada 30 días.

```
[student@desktopX ~]$ sudo vi /etc/login.defs
[student@desktopX ~]$ 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 un GID de 900.

```
[student@desktopX ~]$ sudo groupadd -g 900 consultants
[student@desktopX ~]$ tail -5 /etc/group
stapdev:x:158:
pesign:x:989:
tcpdump:x:72:
slocate:x:21:
consultants:x:900:
```

3. Cree tres usuarios nuevos: **sspadé**, **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@desktopX ~]$ sudo useradd -G consultants spade
[student@desktopX ~]$ sudo useradd -G consultants bboop
[student@desktopX ~]$ sudo useradd -G consultants dtracy
[student@desktopX ~]$ tail -5 /etc/group
slocate:x:21:
consultants:x:900:sspadé,bboop,dtracy
sspadé:x:1001:
bboop:x:1002:
dtracy:x:1003:
[student@desktopX ~]$ sudo passwd spade
Changing password for user spade.
New password: default
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: default
passwd: all authentication tokens updated successfully.
[student@desktopX ~]$ sudo passwd bboop
[student@desktopX ~]$ 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@desktopX ~]$ sudo chage -E $(date +%Y-%m-%d -d +90days) spade
[student@desktopX ~]$ sudo chage -E $(date +%Y-%m-%d -d +90days) bboop
[student@desktopX ~]$ sudo chage -E $(date +%Y-%m-%d -d +90days) dtracy
```

5. Cambie la política de contraseña para la cuenta **bboop**, para que se le solicite una contraseña nueva cada 15 días.

```
[student@desktopX ~]$ sudo chage -M 15 bboop
[student@desktopX ~]$ 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@desktopX ~]$ sudo chage -d 0 sspade
[student@desktopX ~]$ sudo chage -d 0 bboop
[student@desktopX ~]$ sudo chage -d 0 dtracy
```

7. Instale el paquete *ipa-client* en su máquina **desktopX**.

7.1.

```
[student@desktopX ~]$ sudo yum -y install ipa-client
```

8. Configure su sistema, con **ipa-client-install**, para usar la configuración del servidor IPA para el dominio DNS de **serverX.example.com**. Los directorios de inicio deben crearse automáticamente y, durante este proceso, NTP no se debe configurar.

8.1.

```
[student@desktopX ~]$ sudo ipa-client-install --domain=serverX.example.com --no-ntp --mkhomedir
Discovery was successful!
Hostname: desktopX.example.com
Realm: SERVERX.example.com
DNS Domain: serverX.example.com
IPA Server: serverX.example.com
BaseDN: dc=serverX,dc=example.com

Continue to configure the system with these values? [no]: yes
User authorized to enroll computers: admin
Password for admin@SERVERX.EXAMPLE.COM: redhat123
...
Client configuration complete.
```

9. Verifique que ahora pueda iniciar sesión satisfactoriamente en **desktopX** con el usuario **ipauser** mediante el uso de **ssh**. La contraseña inicial es **password**, pero se debe cambiar a **redhat123**. Debido al requisito de cambio de contraseña, tendrá que iniciar sesión dos veces.

9.1.

```
[student@desktopX ~]$ ssh ipauser@desktopX.example.com
ipauser@desktopX.example.com's password: password
Password expired. Change your password now.
Creating home directory for ipauser.
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user ipauser.
Current password: password
New password: redhat123
Retype new password: redhat123
```

Capítulo 3. Usuarios y Grupos

```
passwd: all authentication tokens updated successfully.  
Connection to desktopX.example.com closed.  
[student@desktopX ~]$ ssh ipauser@desktopX.example.com  
ipauser@desktopX.example.com's password: redhat123  
Last login: Wed Feb 26 05:19:15 2014 from desktopX.example.com  
-sh-4.2$ logout
```

10. Cuando finalice, ejecute el script de evaluación **lab combined-users grade** para confirmar que se hayan realizado todos los pasos de forma correcta.

```
[student@desktopX ~]$ lab combined-users 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.

Uso de servicios de administración de identidades

- **authconfig{, -gtk, -tui}** se puede usar para configurar un sistema para usar servicios de administración de identidad centralizados.
- **sssd** se configura para recuperar, validar y almacenar en memoria caché información de autenticación y del usuario en segundo plano.



CAPÍTULO 4

PERMISOS DE ARCHIVOS

Descripción general	
Meta	Controlar el acceso a archivos y directorios mediante permisos y listas de control de accesos (ACL).
Objetivos	<ul style="list-style-type: none">Cambiar los permisos y la propiedad de los archivos con las herramientas de línea de comandos.Configurar un directorio en el que los archivos creados recientemente puedan ser escritos en forma automática por los miembros del grupo propietario del directorio, mediante permisos especiales y configuración predeterminada de desenmascarar.Describir listas de control de acceso POSIX.Administrar listas de control de acceso POSIX.
Secciones	<ul style="list-style-type: none">Administración de los permisos del sistema de archivos desde la línea de comandos (y práctica)Administración de permisos predeterminados y acceso a archivos (y práctica)Listas de control de acceso (ACL) POSIX (y práctica)Protección de archivos con ACL (y práctica)

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 un prompt BASH.
Seleccione **Applications > Utilities > Terminal**.
3. Conviértase en el usuario **root** en el prompt 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 4. Permisos de archivos

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 prompt 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 4. Permisos de archivos

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
```

Listas de control de acceso (ACL) POSIX

Objetivos

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

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

Conceptos de listas de control de acceso

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

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

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

Opción de montaje de sistema de archivos

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

Visualización e interpretación de permisos de ACL

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

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

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

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

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



Importante

Si se modifican los permisos del grupo en un archivo con ACL mediante el uso de **chmod**, no se modifican los permisos del propietario del grupo, pero sí se modifica la máscara de ACL. Use **setfac1 -m g::perms file** si lo que intenta es actualizar los permisos del propietario del grupo de archivos.

Ver ACL de archivos

Para visualizar la configuración de ACL en un archivo, use **getfac1 file**:

```
[student@serverX steamies]$ getfac1 roster.txt
# file: roster.txt
# owner: student
# group: controller
user::rwx
user:james:---
user:1005:rwx      #effective:rw-
group::rwx        #effective:rw-
group:sodor:r--
group:2210:rwx    #effective:rw-
mask::rw-
other::---
```

Dé un vistazo a cada sección del ejemplo anterior:

Abrir entradas de comentarios:

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

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

Entradas de usuarios:

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

- ① Permisos del propietario de archivos. **student** tiene **rwx**.
- ② Permisos de usuarios nombrados. Una entrada para cada usuario nombrado asociado con este archivo. **james** NO tiene permisos.

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

Entradas de grupos:

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

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

Entrada de la máscara:

```
mask::rwx
```

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

Otra entrada:

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

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

Ver ACL de directorios

Para visualizar la configuración de ACL en un directorio, use **getfac1 /directory**:

```
[student@serverX steamies]$ getfac1 .
# file: .
# owner: student
# group: controller
# flags: -s-
user::rwx
user:james:---
user:1005:rwx
group::rwx
group:sodor:r-x
group:2210:rwx
mask::rwx
other:---
default:user::rwx
default:user:james:---
default:group::rwx
default:group:sodor:r-x
default:mask::rwx
default:other:---
```

Dé un vistazo a cada sección del ejemplo anterior:

Capítulo 4. Permisos de archivos

Abrir entradas de comentarios:

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

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

Entradas de ACL estándares:

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

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

Entradas del usuario predeterminadas:

```
default:user::rwx
default:user:james:---
```

①

②

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

Entradas del grupo predeterminadas:

```
default:group::rwx
default:group:sodor:r-x
```

①

②

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

Entrada de la máscara ACL predeterminada:

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

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

Entrada de otro predeterminada:

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

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

Las entradas *predeterminadas* del ejemplo anterior no incluyen el usuario nombrado (UID **1005**) ni el grupo nombrado (GID **2210**); consecuentemente, no obtendrán entradas de ACL iniciales automáticamente agregadas para estas a ningún archivo nuevo o subdirectorio nuevo. Esto las limita de manera efectiva a archivos y subdirectorios que ya tienen ACL, o si el propietario del archivo relevante agrega la ACL más tarde utilizando **setfac1**, Aún pueden crear sus propios archivos y subdirectorios.



nota

El resultado de **getfac1** se puede usar como entrada para **setfac1**. Use **getfac1 -R /directory** para generar el resultado para el directorio y su contenido. Este resultado se puede guardar y usar para recuperar al pasar el resultado a **setfac1 --set-file=filename** para hacer una actualización masiva.

La máscara de ACL

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

La máscara se puede visualizar con **getfac1** y establecer explícitamente con **setfac1**. Se calculará y se agregará automáticamente si no se la establece de forma explícita, pero también podría heredarse de una configuración de máscara predeterminada de un directorio principal. De forma predeterminada, la máscara se calcula nuevamente siempre que se agregue, se modifique o se elimine cualquiera de las ACL afectadas.

Precedencia de permisos de ACL

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

- Si el proceso se ejecuta como el usuario que es propietario del archivo, se aplican los permisos de ACL del usuario del archivo.
- Si el proceso se ejecuta como un usuario que está detallado en una entrada de ACL del usuario, se aplican los permisos de ACL de usuario nombrado (siempre que esté permitido por la máscara).

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

Referencias

Páginas del manual: **acl(5)**, **getfac1(1)**, **ls(1)**

Práctica: interpretar ACL

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

default:m::rx /directory	
default:user:mary:rx /directory	g::rw /directory
g::rw file	getfacl /directory
group:hug:rwx /directory	user::rx file
user:mary:rx file	

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

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

Solución

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

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

Protección de archivos con ACL

Objetivos

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

- Cambiar permisos de archivos de ACL regulares usando **setfac1**.
- Controlar permisos de archivos de ACL predeterminados para archivos y directorios nuevos.

Cambio de permisos de archivos de ACL

Use **setfac1** para agregar, modificar o eliminar ACL en archivos y directorios.

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

Adición o modificación de una ACL

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



nota

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

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

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

```
[student@serverX ~]$ setfac1 -m u:name:rX file
```

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

Los permisos del *propietario del archivo* de ACL y el *propietario del archivo* estándar son equivalentes; por consiguiente, el uso de **chmod** en los permisos del *propietario del archivo* es

equivalente a usar **setfacl** en los permisos del *propietario del archivo*. **chmod** no tiene efecto sobre los usuarios nombrados.

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

```
[student@serverX ~]$ setfacl -m g:name:rw file
```

Esto sigue el mismo patrón para agregar o modificar una ACL de usuario. Si *name* se deja en blanco, se aplica al *propietario del grupo*. De lo contrario, especifique un nombre de grupo o un valor de GID para un *grupo nombrado*. Los permisos serían de lectura y escritura en este ejemplo.

chmod no tiene efecto en permisos de ningún grupo para archivos con configuraciones de ACL, pero actualiza la máscara de ACL.

Para agregar o modificar la ACL de *otro*:

```
[student@serverX ~]$ setfacl -m o:::- file
```

otro solo acepta configuración de permisos. Es común que el permiso se establezca en "*-*" (guión), que especifica que los usuarios *otro* NO tienen permiso, pero se puede especificar cualquiera de los permisos estándares.

Los permisos de *otro* de ACL y *otro* estándar son equivalentes; por consiguiente, el uso de **chmod** en los permisos de *otro* es equivalente a usar **setfacl** en los permisos de *otro*.

Agregue varias entradas a través del mismo comando y separe con coma cada una de las entradas:

```
[student@serverX ~]$ setfacl -m u::rwx,g:sodor:rX,o:::- file
```

Esto establecerá al *propietario del archivo* a leer, escribir y ejecutar, establecerá al grupo nombrado **sodor** en solo lectura y ejecución condicional y restringirá a todos los usuarios *otro* a NINGÚN permiso. El *propietario del grupo* mantendrá sus permisos de ACL o de archivo existentes y las otras entradas "nombradas" permanecerán iguales.

Uso de **getfacl** como entrada

El resultado de **getfacl** se puede usar como entrada para **setfacl**:

```
[student@serverX ~]$ getfacl file-A | setfacl --set-file=- file-B
```

--set-file acepta entrada de un archivo o *stdin*, y el "*-*" (guión) especifica el uso de *stdin*. En este caso, *file-B* tendrá la misma configuración de ACL que *file-A*.

Configuración de una máscara de ACL explícita

Una máscara de ACL se puede establecer de forma explícita en un archivo o directorio para limitar los permisos efectivos máximos para usuarios nombrados, el propietario del grupo y los grupos nombrados. Esto restringe los permisos existentes que superen la máscara, pero no afecta los permisos que son menos permisivos que la máscara.

```
[student@serverX ~]$ setfacl -m m:::r file
```

Esto agregaría un valor de la máscara que restringiría a cualquiera de los *usuarios nombrados*, el *propietario del grupo* y cualquiera de los *grupos nombrados* a permiso de solo lectura, independientemente de su configuración existente. Los usuarios *propietario del archivo* y *otro* no se ven afectados por la configuración de la máscara.

getfac1 mostrará un comentario "efectivo" además de entradas que son restringidas por una configuración de máscara.



Importante

De forma predeterminada, la máscara de ACL se vuelve a calcular cada vez que una de las configuraciones de ACL afectadas (usuarios nombrados, propietario del grupo o grupos nombrados) se modifica o elimina, y potencialmente se restablece una configuración de la máscara explícita.

Para evitar calcular nuevamente la máscara, use **-n** o incluya una configuración de la máscara (**-m m::perms**) con cualquier operación **setfac1** que modifique la configuración de ACL afectada de la máscara.

Modificaciones de ACL recursivas

Cuando se configura una ACL en un directorio, es común querer aplicar la ACL de forma recursiva a la estructura del directorio y los archivos. Use la opción **-R** para hacer esto. El permiso "X" (x mayúscula) se usa a menudo con recursión, de modo que los archivos con permiso de ejecución establecido retienen la configuración y los directorios obtienen el permiso de ejecución establecido para permitir la búsqueda de directorios. También se considera práctica recomendada usar la X mayúscula cuando se configuran ACL de manera no recursiva, dado que esto evita que un administrador agregue de forma accidental permisos de ejecución a un archivo regular.

```
[student@serverX ~]$ setfac1 -R -m u:name:rX directory
```

Esto agregaría al usuario *name* al *directorio* y todos los archivos y subdirectorios existentes, y otorgaría permiso de solo lectura y ejecución condicional.

Eliminación de una ACL

La eliminación de entradas de ACL específicas sigue el mismo formato básico que la operación de modificar, excepto que "*:perms*" no debe especificarse.

```
[student@serverX ~]$ setfac1 -x u:name,g:name file
```

Esto solo eliminaría al usuario nombrado y al grupo nombrado de la lista de ACL de archivos o directorios. El resto de las ACL existentes permanecen activas.

Es posible usar las operaciones de eliminación (**-x**) y modificación (**-m**) en la misma operación **setfac1**.

La máscara solo puede eliminarse si no hay otras ACL establecidas (excluidas las ACL *base* que no se pueden eliminar), de modo que debe eliminarse última. El archivo no tendrá ACL y **ls -l** no mostrará el símbolo "+" junto a la cadena de permisos. De forma alternativa, para eliminar TODAS las ACL de un archivo o un directorio (incluidas las ACL *predeterminadas* en los directorios), use:

```
[student@serverX ~]$ setfacl -b file
```

Control de permisos de archivos de ACL predeterminadas

Un directorio puede tener ACL *predeterminadas* establecidas que se heredan automáticamente mediante todos los archivos nuevos y subdirectorios nuevos. Puede haber permisos de ACL *predeterminadas* establecidos para cada una de las configuraciones de ACL estándares, incluida una máscara predeterminada.

Un directorio aún requiere ACL estándares para el control de acceso porque las ACL *predeterminadas* no implementan control de acceso para el directorio; solo proporcionan soporte de herencia para permisos de ACL.

Un ejemplo:

```
[student@serverX ~]$ setfacl -m d:u:name:rx directory
```

Esto agrega un usuario nombrado predeterminados (**d:u:name**) con permiso de solo lectura y ejecución en subdirectorios.

El comando **setfacl** para agregar una ACL *predeterminada* para cada uno de los tipos de ACL es exactamente el mismo que para las ACL estándares, pero incluye **d:** delante. De forma alternativa, use la opción **-d** en la línea de comandos.



Importante

Al configurar las ACL *predeterminadas* en un directorio, asegúrese de que los usuarios podrán acceder al contenido de los subdirectorios nuevos creados en este, al incluir el permiso de ejecución en la ACL *predeterminada*.

Los usuarios no recibirán automáticamente el permiso de ejecución establecido en los archivos regulares creados recientemente, ya que, a diferencia de los directorios nuevos, la máscara de ACL de un archivo regular nuevo es **rw-**.



nota

Los archivos y subdirectorios nuevos continúan obteniendo los valores de UID de su propietario y de GID del grupo primario establecidos a partir del usuario creador, excepto cuando la marca **setgid** del directorio principal está habilitada, en cuyo caso el GID del grupo primario será el mismo que el GID del directorio principal.

Eliminación de ACL predeterminadas

Eliminar una ACL *predeterminada* es también igual que eliminar una ACL estándar; nuevamente, se agrega **d:** adelante o se usa la opción **-d**.

```
[student@serverX ~]$ setfacl -x d:u:name directory
```

Esto elimina la ACL *predeterminada* que se agregó en el ejemplo anterior.

Para eliminar todas las ACL *predeterminadas* en un directorio, use **setfac1 -k /directory**.
Para eliminar TODAS las ACL en un directorio, use **setfac1 -b /directory**.



Referencias

Páginas del manual: **acl(5)**, **setfac1(1)**

Práctica: Uso de ACL para otorgar y limitar el acceso

En este laboratorio, agregará una lista de control de acceso (ACL) de grupo nombrado y una ACL de usuario nombrado a una carpeta compartida existente y su contenido. Configurará ACL *predeterminadas* para asegurar que los archivos y directorios futuros obtengan los permisos correctos.

Recursos:	
Archivos:	/shares/steamies/*, /shares/steamies/ display_engines.sh
Máquinas:	serverX

Resultados:

- Los miembros del grupo **sodor** tendrán los mismos permisos de acceso que el grupo **controller** en el directorio **steamies**, excepto **james**, quien no tiene acceso.
- Los archivos y directorios existentes se actualizarán para reflejar los nuevos permisos de ACL de **sodor** y **james**.
- Los archivos y directorios nuevos obtendrán automáticamente los permisos de ACL y de archivos correctos.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

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

- Abra una terminal.
- Cambie a **root** usando **sudo -i**.

El estudiante es un controlador para la red Sodor Island Rail. Hay un directorio compartido configurado adecuadamente y ubicado en **/shares/steamies** que aloja archivos que detallan alineación, motores a vapor, etc.

Actualmente, solo los miembros del grupo **controller** tienen acceso a este directorio, pero se ha decidido que se otorgará a los miembros del grupo **sodor** el beneficio de acceso completo a este directorio.

James, un miembro del grupo **sodor**, ha ocasionado *caos y confusión* en muchas ocasiones, de modo que se le negará el acceso al directorio, al menos hasta que muestre que es un *motor realmente útil*.

Su tarea es agregar ACL adecuadas al directorio y su contenido, de modo que los miembros del grupo **sodor** tengan acceso completo, pero negar todo tipo de acceso al usuario **james**.

Capítulo 4. Permisos de archivos

Asegúrese de que a los archivos y directorios futuros almacenados en **/shares/steamies** se le apliquen las ACL adecuadas.

Información importante:

- Grupo **controller**: **student**
- Grupo **sodor**: **thomas, james**
- Hay un subdirectorio denominado **engines** y varios archivos para evaluar las ACL. Además, hay un script ejecutable que puede evaluar.
- Thomas y James tienen sus contraseñas establecidas como **redhat**.
- Todos los cambios deben ocurrir en el directorio **steamies** y sus archivos; no ajuste el directorio **shares**.

1. Agregue las ACL nombradas al directorio **steamies** y todo su contenido.
 - 1.1. Use **setfac1** para actualizar recursivamente el directorio **steamies**, y otorgue permisos de lectura, escritura y ejecución condicional al grupo **sodor**.

```
[root@serverX ~]# setfac1 -Rm g:sodor:rwx /shares/steamies
```

-R recursivo, -m modificar/agregar, :rwx leer/escribir/ejecutar (pero solo en directorios y ejecutables existentes)

- 1.2. Use **setfac1** para actualizar recursivamente el directorio **steamies**, denegar al usuario **james** del grupo **sodor** todo tipo de acceso.

```
[root@serverX ~]# setfac1 -Rm u:james:- /shares/steamies
```

-R recursivo, -m modificar/agregar, :- sin permisos

2. Agregue las ACL nombradas como ACL *predeterminadas* para admitir futuras adiciones de archivos y directorios.

- 2.1. Use **setfac1** para agregar una regla de acceso predeterminada para el grupo **sodor**. Otorgue permisos de lectura, escritura y ejecución en el directorio **steamies**.

```
[root@serverX ~]# setfac1 -m d:g:sodor:rwx /shares/steamies
```

-m modificar/agregar, d:g grupo predeterminado, :rwx leer/escribir/ejecutar (necesario para creación y acceso adecuados a subdirectorios)

- 2.2. Use **setfac1** para agregar una regla de acceso predeterminada para el usuario **james**. Niegue todo acceso al directorio **steamies**.

```
[root@serverX ~]# setfac1 -m d:u:james:- /shares/steamies
```

-m modificar/agregar, d:u usuario predeterminado, :- sin permisos

3. Verifique sus cambios en ACL.

Thomas debe poder leer cualquier archivo, crear un directorio nuevo con un nuevo archivo en este y ejecutar el script **display_engines.sh**.

James no debe poder leer, escribir ni ejecutar ningún archivo; esto incluye no poder listar los contenidos del directorio.

Use **sudo -i -u user** para cambiar a usuarios de prueba. Use **exit** o **Ctrl+D** para salir de la shell de usuarios de prueba.

```
[root@serverX ~]# exit  
[student@serverX ~]$ sudo -i -u thomas  
[thomas@serverX ~]$ cd /shares/steamies/
```

3.1. Use **cat** para comprobar que Thomas pueda leer un archivo.

```
[thomas@serverX steamies]$ cat roster.txt  
James - Shunting at Brendam docks  
Percy - Overnight mail run  
Henry - Flying Kipper run  
Thomas - Annie and Clarabel, Knapford line
```

3.2. Use **display_engines.sh** para comprobar que Thomas pueda ejecutar un script.

```
[thomas@serverX steamies]$ ./display_engines.sh  
They're two, they're four, they're six, they're eight ...  
Edward wants to help and share  
...  
Toby, well let's say, he's square
```

3.3. Use **mkdir** para crear un directorio como Thomas.

Use **echo** para crear un archivo en el directorio nuevo como Thomas.

Cambie nuevamente a **student** cuando haya finalizado.

```
[thomas@serverX steamies]$ mkdir tidmouth  
[thomas@serverX steamies]$ echo "toot toot" > tidmouth/whistle.txt  
[thomas@serverX steamies]$ exit
```

3.4. Use **cd** para probar y cambiar dentro del directorio como James, y también pruebe **ls** para listar el directorio. Ambos comandos deben fallar con **permiso denegado**.

Puede intentar uno o más de los comandos emitidos por Thomas, excepto como James, para verificar mejor su falta de acceso. Pruebe agregar prefijos a cada archivo con la ruta completa, **/shares/steamies**, debido a que no puede usar **cd** en el directorio.

Cambie nuevamente a **student** cuando haya terminado de evaluar a **james**.

```
[student@serverX ~]$ sudo -i -u james  
[james@serverX ~]$ cd /shares/steamies/  
-bash: cd: /shares/steamies/: Permission denied  
[james@serverX ~]$ ls /shares/steamies/
```

```
ls: cannot open directory /shares/steamies: Permission denied
[james@serverX ~]$ cat /shares/steamies/roster.txt
cat: /shares/steamies/roster.txt: Permission denied
[james@serverX ~]$ exit
```

- 3.5. Use **getfacl** para ver todas las ACL en **/shares/steamies** y las ACL en **/shares/steamies/tidmouth**.



nota

Use **newgrp controller** para cambiar *student* al grupo *controller*.

El script **lab acl setup** agrega a *controller* como grupo complementario a *student*; sin embargo, a menos que haya reiniciado la shell antes de este paso, la shell actual no reconoce aún la nueva membresía y **getfacl** en **tidmouth** tendrá el **permiso denegado**.

```
[student@serverX ~]$ newgrp controller
[student@serverX ~]$ getfacl /shares/steamies
getfacl: Removing leading '/' from absolute path names
# file: shares/steamies/
# owner: root
# group: controller
# flags: -s-
user::rwx
user:james:---
group::rwx
group:sodor:rwx
mask::rwx
other::::
default:user::rwx
default:user:james:---
default:group::rwx
default:group:sodor:rwx
default:mask::rwx
default:other::::

[student@serverX ~]$ getfacl /shares/steamies/tidmouth
getfacl: Removing leading '/' from absolute path names
# file: shares/steamies/tidmouth
# owner: thomas
# group: controller
# flags: -s-
user::rwx
user:james:---
group::rwx
group:sodor:rwx
mask::rwx
other::::
default:user::rwx
default:user:james:---
default:group::rwx
default:group:sodor:rwx
default:mask::rwx
default:other::::
```

Resumen

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.

Listas de control de acceso (ACL) POSIX

- Las ACL proporcionan control de acceso detallado a archivos y directorios.
- El sistema de archivos se debe montar con soporte de ACL habilitado; XFS tiene soporte para ACL incorporado.
- ls -l** indica la presencia de la configuración de ACL con el carácter "+". Los permisos del grupo muestran la configuración de la *máscara*.
- getfacl file** muestra las ACL en un archivo o directorio; las ACL del directorio incluyen las ACL predeterminadas.
- Una máscara de ACL define los permisos máximos que los *usuarios nombrados*, el *propietario del grupo* y los *grupos nombrados* pueden obtener.
- Una precedencia de permisos de ACL es *usuario, usuarios nombrados, grupos y luego otros*.

Protección de archivos con ACL

- Cómo usar **setfacl -m acl_spec** para agregar o modificar.
- Cómo usar **setfacl -x acl_spec** para eliminar.
- Las ACL predeterminadas se pueden establecer en un directorio; delante de *acl_spec* agregue **d:**. Incluya permiso de ejecución para asegurar el acceso a nuevos subdirectorios.
- Cómo usar **-R** para recursivo, **-b** para eliminar todas las ACL, **-k** para eliminar las ACL predeterminadas.
- El *acl_spec* tiene el patrón **type:name:perms**.
 - type* puede ser **u**, **g**, **o**, o **m**.
 - name* puede ser **nombre de usuario**, **uid**, **nombre de grupo**, o **gid**. Un nombre vacío implica *propietario del archivo* o *propietario del grupo*.
 - perms* son **r**, **w**, **x**, o **X**. **"-"** significa no establecido.



CAPÍTULO 5

PERMISOS DE SELINUX

Descripción general	
Meta	Administrar el comportamiento de Security Enhanced Linux (SELinux) de un sistema para mantenerlo seguro en caso de un riesgo del servicio de red.
Objetivos	<ul style="list-style-type: none">• Explicar los conceptos básicos de los permisos de SELinux.• Cambiar modos de SELinux con setenforce.• Cambiar contextos de archivos con semanage y restorecon.• Administrar booleanos de SELinux con setsebool.• Examinar registros y usar sealert para solucionar problemas de violaciones de SELinux.
Secciones	<ul style="list-style-type: none">• Habilitación y supervisión de SELinux (y práctica)• Modificación de los modos de SELinux (y práctica)• Modificación de los contextos de SELinux (y práctica)• Modificación de los booleanos de SELinux (y práctica)• Resolución de problemas de SELinux (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">• Administración de seguridad de SELinux

Habilitación y supervisión de Security Enhanced Linux (SELinux)

Objetivos

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

- Explicar los conceptos básicos de las transiciones de contexto y los permisos de SELinux.
- Mostrar el modo actual de SELinux.
- Interpretar correctamente el contexto de SELinux de un archivo.
- Interpretar correctamente el contexto de SELinux de un proceso.
- Identificar la configuración de booleanos de SELinux actual.

Conceptos básicos de seguridad de SELinux

Security Enhanced Linux (SELinux) es una capa adicional de seguridad del sistema. Un objetivo principal de SELinux es proteger los datos del usuario de los servicios del sistema que han sido comprometidos. La mayoría de los administradores de Linux está familiarizado con el modelo de seguridad de permisos de usuario/grupo/otro. Este es un modelo basado en usuarios y grupos conocido como control de acceso discrecional. SELinux proporciona un nivel adicional de seguridad que está basado en objetos y controlado por reglas más sofisticadas, conocido como control de acceso obligatorio.

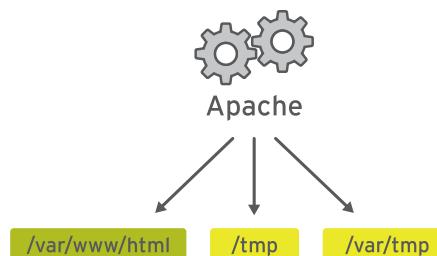


Figura 5.1: Servicio Apache sin protección de SELinux

Para permitir el acceso anónimo remoto a un servidor web, se deben abrir los puertos de firewall. Sin embargo, eso le da a la gente malintencionada la oportunidad de entrar al sistema a través de una vulnerabilidad de seguridad y, si ponen en riesgo el proceso del servidor web, obtienen sus permisos: los permisos del usuario **apache** y el grupo **apache**. Ese usuario o grupo tiene acceso de lectura a elementos como la root del documento (**/var/www/html**) y acceso de escritura a **/tmp**, **/var/tmp** y cualquier otro archivo o directorio que todos los usuarios puedan escribir.

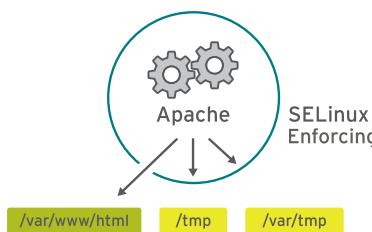


Figura 5.2: Servicio Apache con protección de SELinux

SELinux es un conjunto de reglas de seguridad que determina qué proceso puede acceder a qué archivos, directorios y puertos. Los archivos, procesos, directorios y puertos tienen etiquetas de seguridad especiales denominadas contextos de SELinux. Un contexto es simplemente un nombre que usa la política de SELinux para determinar si un proceso puede o no acceder a un archivo, directorio o puerto. De forma predeterminada, la política no permite ninguna interacción a menos que una regla explícita otorgue acceso. Si no hay ninguna regla de permiso, no se permite ningún tipo de acceso.

Las etiquetas de SELinux tienen varios contextos: usuario, rol, tipo y sensibilidad. La política de destino, que es la política predeterminada habilitada en Red Hat Enterprise Linux, basa sus reglas en el tercer contexto: el contexto de tipo. Por lo general, los nombres de contexto de tipo finalizan en `_t`. El contexto de tipo para el servidor web es `httpd_t`. El contexto de tipo para los archivos y los directorios que generalmente se encuentran en `/var/www/html` es `httpd_sys_content_t`. El contexto de tipo para los archivos y directorios que normalmente se encuentran en `/tmp` y `/var/tmp` es `tmp_t`. El contexto de tipo para los puertos del servidor web es `http_port_t`.

Hay una regla en la política que permite a Apache (el proceso de servidor web que se ejecuta como `httpd_t`) acceder a archivos y directorios con un contexto que normalmente se encuentra en `/var/www/html` y otros directorios de servidor web (`httpd_sys_content_t`). No hay una regla en la política para los archivos que normalmente se encuentran en `/tmp` y `/var/tmp`, de modo que no se permite el acceso. Con SELinux, un usuario malintencionado no podría acceder al directorio `/tmp`. SELinux tiene reglas para los sistemas de archivos remotos como NFS y CIFS, aunque todos los archivos en esos sistemas de archivos se etiquetan con el mismo contexto.

Muchos comandos que tienen que ver con archivos tienen una opción (generalmente `-Z`) para mostrar o configurar contextos de SELinux. Por ejemplo, `ps`, `ls`, `cp` y `mkdir` usan la opción `-Z` para mostrar o configurar contextos de SELinux.

```
[root@serverX ~]# ps axZ
  LABEL          PID TTY      STAT   TIME COMMAND
system_u:system_r:init_t:s0    1 ?        Ss    0:09 /usr/lib/systemd/...
system_u:system_r:kernel_t:s0   2 ?        S     0:00 [kthreadd]
system_u:system_r:kernel_t:s0   3 ?        S     0:00 [ksoftirqd/0]
[... Output omitted ...]
[root@serverX ~]# systemctl start httpd
[root@serverX ~]# ps -ZC httpd
  LABEL          PID TTY      TIME CMD
system_u:system_r:httpd_t:s0  1608 ?      00:00:05 httpd
system_u:system_r:httpd_t:s0  1609 ?      00:00:00 httpd
[... Output omitted ...]
[root@serverX ~]# ls -Z /home
```

```
drwx----- . root      root      system_u:object_r:lost_found_t:s0 lost+found
drwx----- . student   student   unconfined_u:object_r:user_home_dir_t:s0 student
drwx----- . visitor   visitor   unconfined_u:object_r:user_home_dir_t:s0 visitor
[root@serverX ~]# ls -Z /var/www
drwxr-xr-x . root      root      system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x . root      root      system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x . root      root      system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x . root      root      system_u:object_r:httpd_sys_content_t:s0 icons
```

Modos de SELinux

Con fines de solución de problemas, la protección de SELinux puede deshabilitarse temporalmente usando los modos de SELinux.

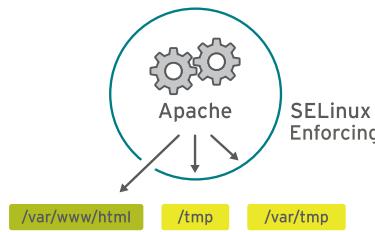


Figura 5.3: Modo de cumplimiento de SELinux

En el modo de cumplimiento, SELinux deniega de forma activa el acceso al servidor web que intente leer archivos con el contexto de tipo **tmp_t**. En el modo de cumplimiento, SELinux registra y protege.

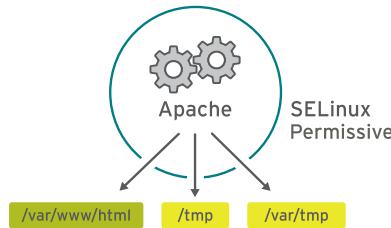


Figura 5.4: Modo permisivo de SELinux

El modo permisivo se usa generalmente para las cuestiones de solución de problemas. En el modo permisivo, SELinux permite todas las interacciones, incluso si no hay una regla explícita, y registra esas interacciones que habría denegado en el modo obligatorio. Este modo se puede usar temporalmente para permitir el acceso a contenido que SELinux está restringiendo. No se requiere reiniciar el sistema para pasar del modo de cumplimiento al modo permisivo, o viceversa.

Un tercer modo, *deshabilitado*, deshabilita SELinux por completo. Deberá reiniciar el sistema para deshabilitar SELinux por completo, o bien para pasar del modo deshabilitado al modo de cumplimiento o permisivo.



Importante

Es mejor usar el modo permisivo que apagar SELinux por completo. Esto se debe a que, incluso en el modo permisivo, el kernel mantendrá automáticamente las etiquetas del sistema de archivos de SELinux según sea necesario, con lo que se evitará la necesidad de volver a etiquetar el sistema de archivos cuando reinicie el sistema con SELinux habilitado.

Para visualizar el modo de SELinux actual en vigencia, use el comando **getenforce**.

```
[root@serverX ~]# getenforce  
Enforcing
```

Booleanos de SELinux

Los booleanos de SELinux son switches que modifican el comportamiento de la política de SELinux. Los booleanos de SELinux son reglas que pueden habilitarse o deshabilitarse. Los administradores de seguridad pueden utilizarlos para realizar ajustes selectivos en la política.

El comando **getsebool** se usa para mostrar booleanos de SELinux y su valor actual. La opción **-a** hace que este comando detalle todos los booleanos.

```
[root@serverX ~]# getsebool -a  
abrt_anon_write --> off  
allow_console_login --> on  
allow_corosync_rw_tmpfs --> off  
[... Output omitted ...]
```



nota

Muchos nombres booleanos han cambiado de Red Hat Enterprise Linux 6 a Red Hat Enterprise Linux 7.



Referencias

Páginas del manual: **selinux(8)**, **getenforce(8)**, **ls(1)**, **ps(1)** y **getsebool(8)**.

Práctica: Conceptos de SELinux

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

Booleano	Contexto	El modo permisivo
Modo de cumplimiento	Modo deshabilitado	

Término	Descripción
Las reglas de la políticas se obedecen y las violaciones se registran	
Etiqueta en procesos, archivos y puertos que determina acceso	
Se requiere un nuevo arranque para pasar a este modo	
Cambio que habilita o deshabilita un conjunto de reglas de políticas	
Las violaciones de reglas de políticas solo producen mensajes de registro	

Solución

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

Término	Descripción
Las reglas de la políticas se obedecen y las violaciones se registran	Modo de cumplimiento
Etiqueta en procesos, archivos y puertos que determina acceso	Contexto
Se requiere un nuevo arranque para pasar a este modo	Modo deshabilitado
Cambio que habilita o deshabilita un conjunto de reglas de políticas	Booleano
Las violaciones de reglas de políticas solo producen mensajes de registro	El modo permisivo

Cambio de modos de SELinux

Objetivos

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

- Modifique el modo actual de SELinux de un sistema.
- Configure el modo predeterminado de SELinux de un sistema

Con fines de solución de problemas, la protección de SELinux puede deshabilitarse temporalmente usando los modos de SELinux. En esta sección, se observará cómo cambiar los modos de SELinux de forma temporal entre el modo de cumplimiento y el modo permisivo. Solo se observará cómo configurar el modo predeterminado de SELinux que se determina en el arranque.

Cambio del modo actual de SELinux

El comando **setenforce** modifica el modo de SELinux actual:

```
[root@serverX ~]# getenforce
Enforcing
[root@serverX ~]# setenforce
usage: setenforce [ Enforcing | Permissive | 1 | 0 ]
[root@serverX ~]# setenforce 0
[root@serverX ~]# getenforce
Permissive
[root@serverX ~]# setenforce Enforcing
[root@serverX ~]# getenforce
Enforcing
```

Otra manera de configurar temporalmente el modo SELinux es pasar un parámetro al kernel en el arranque. El paso de un argumento del kernel de **enforcing=0** hace que el sistema arranque en el modo permisivo. Un valor de **1** especificaría el modo de cumplimiento. SELinux se puede deshabilitar cuando se especifica el argumento **selinux=0**. Un valor de **1** habilitaría SELinux.

Configuración del modo predeterminado de SELinux

El archivo de configuración que determina el modo de SELinux en el que se establece al momento del arranque es **/etc/selinux/config**. Observe que contiene algunos comentarios útiles:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes
#                 are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Use **/etc/selinux/config** para modificar el modo predeterminado de SELinux durante el arranque. En el ejemplo que se muestra, está configurado en el modo de cumplimiento.

Al pasar los argumentos del kernel **selinux=** o **enforcing=**, se anulan todos los valores predeterminados especificados en **/etc/selinux/config**.



Referencias

Páginas del manual: **getenforce(1)**, **setenforce(1)**, **selinux_config(5)**

Práctica: Cambio de modos de SELinux

En este trabajo de laboratorio, administrará modos de SELinux, tanto de forma temporal como de forma persistente.

Recursos	
Máquinas:	serverX

Resultados:

Obtendrá práctica al visualizar y configurar el modo actual de SELinux.

1. Inicie sesión como **root** en **serverX**. Muestre el modo actual de SELinux.

```
[root@serverX ~]# getenforce
Enforcing
```

2. Cambie el modo predeterminado de SELinux a permisivo y reinicie.

```
[root@serverX ~]# vi /etc/selinux/config
[root@serverX ~]# grep '^SELINUX' /etc/selinux/config
SELINUX=permissive
SELINUXTYPE=targeted
[root@serverX ~]# reboot
```

3. Cuando **serverX** funcione nuevamente, inicie sesión como **root** y muestre el modo actual de SELinux.

```
[root@serverX ~]# getenforce
Permissive
```

4. Modifique el modo predeterminado de SELinux al modo de cumplimiento.

```
[root@serverX ~]# vi /etc/selinux/config
[root@serverX ~]# grep '^SELINUX' /etc/selinux/config
SELINUX=enforcing
SELINUXTYPE=targeted
```

5. Configure el modo actual de SELinux al modo de cumplimiento.

```
[root@serverX ~]# setenforce 1
[root@serverX ~]# getenforce
Enforcing
```

Cambio de contextos de SELinux

Objetivos

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

- Configurar el contexto de seguridad de SELinux de los archivos en la política.
- Restaurar el contexto de seguridad de SELinux de los archivos.

Contexto inicial de SELinux

Generalmente, el contexto de SELinux del directorio principal de un archivo determina su contexto de SELinux inicial. El contexto de un directorio principal se asigna al archivo creado recientemente. Esto funciona para comandos como **vim**, **cp** y **touch**. Sin embargo, si un archivo se crea en otra parte y se conservan los permisos (como con **mv** o **cp -a**), el contexto original de SELinux no se modificará.

```
[root@serverX ~]# ls -Zd /var/www/html/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /var/www/html/
[root@serverX ~]# touch /var/www/html/index.html
[root@serverX ~]# ls -Z /var/www/html/index.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/
index.html
```

Cambio del contexto de SELinux de un archivo

Hay dos comandos que se utilizan para cambiar el contexto de SELinux de archivos: **chcon** y **restorecon**. El comando **chcon** cambia el contexto del archivo al contexto especificado como un argumento para el comando. A menudo, la opción **-t** se utiliza para especificar solo el tipo de componente del contexto.

El comando **restorecon** es el método preferido para cambiar el contexto de un archivo o directorio de SELinux. A diferencia de **chcon**, el contexto no se especifica explícitamente al usar este comando. Usa las reglas de la política de SELinux para determinar cuál debe ser el contexto del archivo.



nota

chcon no debe usarse para cambiar el contexto de archivos de SELinux. Se pueden cometer errores al especificar el contexto explícitamente. Los contextos de archivos se modificarán nuevamente a su contexto predeterminado si los sistemas de archivos del sistema se etiquetan nuevamente en el momento del arranque.

```
[root@serverX ~]# mkdir /virtual
[root@serverX ~]# ls -Zd /virtual
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /virtual
[root@serverX ~]# chcon -t httpd_sys_content_t /virtual
[root@serverX ~]# ls -Zd /virtual
drwxr-xr-x. root root unconfined_u:object_r:httpd_sys_content_t:s0 /virtual
[root@serverX ~]# restorecon -v /virtual
```

Capítulo 5. Permisos de SELinux

```
restorecon reset /virtual context unconfined_u:object_r:httpd_sys_content_t:s0->
unconfined_u:object_r:default_t:s0
[root@serverX ~]# ls -Zd /virtual
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /virtual
```

Definición de las reglas de contextos de archivos predeterminados de SELinux

Se puede usar el comando **semanage fcontext** para mostrar o modificar las reglas que usa el comando **restorecon** para configurar los contextos de archivos predeterminados. Utiliza expresiones regulares extendidas para especificar los nombres de archivo y las rutas de acceso. La expresión regular extendida más común utilizada en las reglas **fcontext** es **(/.*)?**, que significa “como opción, coincidir con un / seguido por una serie de caracteres”. Busca coincidencias con el directorio detallado antes de la expresión y todo lo que contiene ese directorio de forma recursiva.

El comando **restorecon** es parte del paquete **policycoreutil** y **semanage** es parte del paquete **policycoreutil-python**.

```
[root@serverX ~]# touch /tmp/file1 /tmp/file2
[root@serverX ~]# ls -Z /tmp/file*
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /tmp/file1
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /tmp/file2
[root@serverX ~]# mv /tmp/file1 /var/www/html/
[root@serverX ~]# cp /tmp/file2 /var/www/html/
[root@serverX ~]# ls -Z /var/www/html/file*
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /var/www/html/file1
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/
html/file2
[root@serverX ~]# semanage fcontext -l
...
/var/www(/.*)?      all files      system_u:object_r:httpd_sys_content_t:s0
...
[root@serverX ~]# restorecon -Rv /var/www/
restorecon reset /var/www/html/file1 context unconfined_u:object_r:user_tmp_t:s0
-> system_u:object_r:httpd_sys_content_t:s0
[root@serverX ~]# ls -Z /var/www/html/file*
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0
    /var/www/html/file1
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0
    /var/www/html/file2
```

En el siguiente ejemplo, se muestra cómo usar **semanage** para agregar un contexto para un directorio nuevo.

```
[root@serverX ~]# mkdir /virtual
[root@serverX ~]# touch /virtual/index.html
[root@serverX ~]# ls -Zd /virtual/
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /virtual/
[root@serverX ~]# ls -Z /virtual/
-rw-r--r--. root root unconfined_u:object_r:default_t:s0 index.html
[root@serverX ~]# semanage fcontext -a -t httpd_sys_content_t '/virtual(/.*)?'
[root@serverX ~]# restorecon -RFvv /virtual
[root@serverX ~]# ls -Zd /virtual/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /virtual/
[root@serverX ~]# ls -Z /virtual/
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0 index.html
```



Referencias

Páginas del manual: **chcon(1)**, **restorecon(8)**, **semanage(8)**

Práctica: Cambio de contextos de SELinux

En este trabajo de laboratorio, cambiará persistentemente el contexto de SELinux de un directorio y su contenido.

Recursos	
Archivos:	/etc/httpd/conf/httpd.conf
Máquinas:	serverX

Resultados:

Tendrá un servidor web que publica contenido web de una root de documento no estándar.

Andes de comenzar

Debe contar con un sistema RHEL 7 en funcionamiento con SELinux en modo de cumplimiento.

1. Inicie sesión como **root** en **serverX**. Use **yum** para instalar el servidor web Apache.

```
[root@serverX ~]# yum install -y httpd
```

2. Configure Apache para usar una root de documento en una ubicación no estándar.

- 2.1. Cree la nueva root del documento, **/custom**.

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

- 2.2. Cree el **index.html** con algo de contenido reconocible.

```
[root@serverX ~]# echo 'This is serverX.' > /custom/index.html
```

- 2.3. Configure Apache para que use la nueva ubicación. Debe reemplazar las dos apariciones de "/var/www/html" con "/custom" en el archivo de configuración de Apache, **/etc/httpd/conf/httpd.conf**.

```
[root@serverX ~]# vi /etc/httpd/conf/httpd.conf
[root@serverX ~]# grep custom /etc/httpd/conf/httpd.conf
DocumentRoot "/custom"
<Directory "/custom">
```

3. Inicie el servicio web Apache.

```
[root@serverX ~]# systemctl start httpd
```

4. Abra un navegador web en **serverX** e intente ver la siguiente URL: **http://localhost/index.html**. Recibirá un mensaje de error que dice que no tiene permiso para acceder al archivo.

-
5. Defina una regla de contextos de archivos de SELinux que establezca el tipo de contexto en **httpd_sys_content_t** para **/custom** y todos los archivos debajo de este.

```
[root@serverX ~]# semanage fcontext -a -t httpd_sys_content_t '/custom(/.*)?'
```

6. Use **restorecon** para cambiar sus contextos.

```
[root@serverX ~]# restorecon -Rv /custom
restorecon reset /custom context unconfined_u:object_r:default_t:s0-
>unconfined_u:object_r:httpd_sys_content_t:s0
restorecon reset /custom/index.html context unconfined_u:object_r:default_t:s0-
>unconfined_u:object_r:httpd_sys_content_t:s0
```

7. Intente ver **http://localhost/index.html** nuevamente. Debería ver el mensaje "This is serverX." (Esto es serverX).

Cambio de booleanos de SELinux

Objetivos

Luego de completar esta sección, los estudiantes deberían poder usar los booleanos de SELinux para hacer ajustes en el comportamiento de la política.

Booleanos de SELinux

Los booleanos de SELinux son switches que modifican el comportamiento de la política de SELinux. Los booleanos de SELinux son reglas que pueden habilitarse o deshabilitarse. Los administradores de seguridad pueden utilizarlos para realizar ajustes selectivos en la política.

El paquete **selinux-policy-devel** proporciona muchas páginas del manual, ***_selinux(8)**, que explican el propósito de los booleanos disponibles para varios servicios. Si este paquete ha sido instalado, el comando **man -k '_selinux'** puede detallar estos documentos.

El comando **getsebool** se utiliza para mostrar booleanos de SELinux y se utiliza **setsebool** para modificarlos. **setsebool -P** modifica la política de SELinux para que la modificación sea persistente. **semanage boolean -l** mostrará si un booleano es persistente o no, junto con una breve descripción del booleano.

```
[root@serverX ~]# getsebool -a
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
antivirus_use_jit --> off
...
[root@serverX ~]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> off
[root@serverX ~]# setsebool httpd_enable_homedirs on
[root@serverX ~]# semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs          (on , off) Allow httpd to enable homedirs
[root@serverX ~]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> on
[root@serverX ~]# setsebool -P httpd_enable_homedirs on
[root@serverX ~]# semanage boolean -l | grep httpd_enable_homedirs
httpd_enable_homedirs          (on , on) Allow httpd to enable homedirs
```

Para solo detallar las modificaciones locales del estado de los booleanos de SELinux (cualquier configuración que difiera de los valores predeterminados de la política), se puede usar el comando **semanage boolean -l -C**.

```
[root@serverX ~]# semanage boolean -l -C
SELinux boolean           State  Default Description
cron_can_relabel          (off , on)  Allow cron to can relabel
```



Referencias

Páginas del manual: **booleans(8)**, **getsebool(8)**, **setsebool(8)**, **semanage(8)**,
semanage-boolean(8)

Práctica: Cambio de booleanos de SELinux

Apache puede publicar contenido web alojado en los directorios de inicio de los usuarios, pero SELinux evita esto de forma predeterminada. En este ejercicio, identificará y cambiará el booleano de SELinux que permitirá a Apache acceder a los directorios de inicio de los usuarios.

Recursos	
Archivos:	/etc/httpd/conf.d/userdir.conf
Máquinas:	serverX

Resultados:

Tendrá un servidor web que publica contenido web desde los directorios de inicio de los usuarios.

Andes de comenzar

El servidor web de Apache ya debe estar instalado y ejecutándose en serverX.example.com.

1. Inicie sesión como **rroot** en **serverX**. Habilite la función Apache que permite a los usuarios publicar contenido web desde sus directorios de inicio. Edite el archivo de configuración **/etc/httpd/conf.d/userdir.conf** y cambie la línea con la directiva **UserDir** para que se lea lo siguiente:

```
#UserDir disabled
UserDir public_html
```

```
[root@serverX ~]# vi /etc/httpd/conf.d/userdir.conf
[root@serverX ~]# grep '#UserDir' /etc/httpd/conf.d/userdir.conf
#UserDir disabled
[root@serverX ~]# grep '^ *UserDir' /etc/httpd/conf.d/userdir.conf
UserDir public_html
```

2. Reinicie el servicio web Apache para que tengan efecto los cambios realizados.

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

3. Cree algo de contenido web que sea publicado desde un directorio de inicio de los usuarios.

- 3.1. Inicie sesión como **student** en otra ventana y cree un directorio **public_html**.

```
[student@serverX ~]$ mkdir ~/public_html
```

- 3.2. Cree algo de contenido en un archivo **index.html**.

```
[student@serverX ~]$ echo 'This is student content on serverX.' > ~/public_html/index.html
```

-
- 3.3. Cambie los permisos en el directorio de inicio de **student** de modo que Apache pueda acceder al subdirectorio **public_html**.

```
[student@serverX ~]$ chmod 711 ~
```

4. Abra un navegador web en **serverX** e intente ver la siguiente URL: **http://localhost/~&stu;/index.html**. Recibirá un mensaje de error que dice que no tiene permiso para acceder al archivo.
5. En su ventana **root**, use el comando **getsebool** para ver si hay booleanos que restrinjan el acceso a los directorios de inicio.

```
[root@serverX ~]# getsebool -a | grep home  
[... Output omitted ...]  
httpd_enable_homedirs --> off  
[... Output omitted ...]
```

6. Use **setsebool** para habilitar el acceso al directorio de inicio de forma persistente.

```
[root@serverX ~]# setsebool -P httpd_enable_homedirs on
```

7. Intente ver **http://localhost/~&stu;/index.html** nuevamente. Debería ver el mensaje "This is student content on serverX (Esto es contenido del estudiante en serverX)."

Solución de problemas de SELinux

Objetivos

Luego de completar esta sección, los estudiantes deberían poder usar las herramientas de análisis de registros de SELinux.

Solución de problemas de SELinux

¿Qué debe hacer cuando SELinux impide el acceso a archivos de un servidor? Hay una secuencia de pasos que debe realizarse cuando ocurre esto.

1. Antes de pensar en hacer ajustes, considere que SELinux puede estar haciendo este trabajo correctamente al prohibir el intento de acceso. Si un servidor web intenta acceder a archivos en **/home**, esto podría indicar un riesgo para el servicio si el contenido web no es publicado por usuarios. Si el acceso debería haberse otorgado, es necesario realizar pasos adicionales para resolver el problema.
2. El problema más común de SELinux es un contexto de archivos incorrecto. Esto puede ocurrir cuando un archivo se crea en una ubicación con un contexto de archivos y se traslada a una ubicación donde se espera un contexto diferente. En la mayoría de los casos, la ejecución de **restorecon** corregirá el problema. Corregir los problemas de este modo tiene poco impacto en la seguridad del resto del sistema.
3. Otra solución para un acceso demasiado restrictivo podría ser el ajuste de un booleano. Por ejemplo, el booleano **ftpd_anon_write** controla si usuarios del FTP anónimos pueden cargar archivos. Este booleano debería activarse si se desea permitir que usuarios del FTP anónimos carguen archivos en un servidor. El ajuste de booleanos requiere más cuidado porque estos pueden tener un amplio impacto en la seguridad del sistema.
4. Es posible que la política de SELinux tenga un error que evite un acceso legítimo. Debido a que SELinux se ha consolidado, es poco común que esto ocurra. Cuando está claro que se ha identificado un error en la política, comuníquese con el soporte de Red Hat para informar el error de modo que se pueda resolver.

Supervisión de las violaciones de SELinux

El paquete **setroubleshoot-server** debe estar instalado para enviar mensajes de SELinux a **/var/log/messages**. **setroubleshoot-server** escucha mensajes de auditoría en **/var/log/audit/audit.log** y envía un breve resumen a **/var/log/messages**. Este resumen incluye identificadores únicos (**UUID**) para violaciones de SELinux que se pueden usar para reunir más información. **sealert -l **UUID**** se usa para generar un informe para un incidente específico. **sealert -a /var/log/audit/audit.log** se usa para generar informes para todos los incidentes en ese archivo.

Considere el siguiente ejemplo de secuencia de comandos en un servidor web Apache estándar:

```
[root@serverX ~]# touch /root/file3
[root@serverX ~]# mv /root/file3 /var/www/html
[root@serverX ~]# systemctl start httpd
[root@serverX ~]# curl http://localhost/file3
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /file3
on this server.</p>
</body></html>
```

Si bien el contenido de **file3** es el esperado, el servidor web arroja un error de **permiso denegado**. Si se inspeccionan **/var/log/audit/audit.log** y **/var/log/messages**, se puede obtener más información sobre este error.

```
[root@serverX ~]# tail /var/log/audit/audit.log
...
type=AVC msg=audit(1392944135.482:429): avc: denied { getattr } for
pid=1609 comm="httpd" path="/var/www/html/file3" dev="vda1" ino=8980981
scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file
...
[root@serverX ~]# tail /var/log/messages
...
Feb 20 19:55:42 serverX setroubleshoot: SELinux is preventing /usr/sbin/httpd
from getattr access on the file . For complete SELinux messages. run
sealert -l 613ca624-248d-48a2-a7d9-d28f5bbe2763
```

Ambos archivos de registro indican que el motivo del error es una denegación de SELinux. El comando **sealert** detallado en **/var/log/messages** puede proporcionar más información, que incluye una posible corrección.

```
[root@serverX ~]# sealert -l 613ca624-248d-48a2-a7d9-d28f5bbe2763
SELinux is preventing /usr/sbin/httpd from getattr access on the file .

***** Plugin catchall (100. confidence) suggests *****

If you believe that httpd should be allowed getattr access on the
file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# grep httpd /var/log/audit/audit.log | audit2allow -M mypol
# semodule -i mypol.pp

Additional Information:
Source Context           system_u:system_r:httpd_t:s0
Target Context          unconfined_u:object_r:admin_home_t:s0
Target Objects          [ file ]
Source                 httpd
Source Path             /usr/sbin/httpd
Port                   <Unknown>
Host                   serverX.example.com
Source RPM Packages    httpd-2.4.6-14.el7.x86_64
Target RPM Packages   selinux-policy-3.12.1-124.el7.noarch
Policy RPM              True
Selinux Enabled         targeted
Policy Type             Enforcing
Enforcing Mode          serverX.example.com
Host Name               Linux serverX.example.com 3.10.0-84.el7.x86_64 #1
Platform
```

```
SMP Tue Feb 4 16:28:19 EST 2014 x86_64 x86_64
Alert Count          2
First Seen           2014-02-20 19:55:35 EST
Last Seen            2014-02-20 19:55:35 EST
Local ID             613ca624-248d-48a2-a7d9-d28f5bbe2763

Raw Audit Messages
type=AVC msg=audit(1392944135.482:429): avc: denied { getattr } for
pid=1609 comm="httpd" path="/var/www/html/file3" dev="vda1" ino=8980981
scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file

type=SYSCALL msg=audit(1392944135.482:429): arch=x86_64 syscall=lstat
success=no exit=EACCES a0=7f9fed0edea8 a1=7fff7bffc770 a2=7fff7bffc770
a3=0 items=0 ppid=1608 pid=1609 auid=4294967295 uid=48 gid=48 euid=48
suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295
comm=httpd exe=/usr/sbin/httpd subj=system_u:system_r:httpd_t:s0 key=(null)

Hash: httpd,httpd_t,admin_home_t,file,getattr
```



nota

La sección “Raw Audit Messages” (Mensajes de auditoría sin formato) revela el archivo de destino que presenta el problema, **/var/www/html/file3**. Además, el contexto objetivo, **tcontext**, no parece pertenecer a un servidor web. Use el comando **restorecon /var/www/html/file3** para arreglar el contexto de archivos. Si deben ajustarse otros archivos, **restorecon** puede restablecer de forma recursiva el contexto: **restorecon -R /var/www/**.



Referencias

Página del manual: (8)**sealert**

Práctica: Solución de problemas de SELinux

En este trabajo de laboratorio, aprenderá cómo solucionar problemas de denegaciones por seguridad de SELinux.

El cambio de **DocumentRoot** de un servidor web de Apache introduce denegaciones de acceso a SELinux. En este ejercicio, verá cómo ese problema podría haberse identificado y resuelto.

Recursos	
Máquinas:	serverX

Resultados:

Obtendrá algo de experiencia en el uso de herramientas de solución de problemas de SELinux.

Andes de comenzar

El servidor web de Apache ya debe estar instalado y ejecutándose en serverX.example.com.

Debe haber completado los pasos del ejercicio de práctica “Changing SELinux Contexts” (Cambio de contextos de SELinux).

1. Inicie sesión como **root** en **serverX**. Elimine la regla de contextos de archivos creada anteriormente y restaure la estructura del directorio **/custom** nuevamente a su contexto de SELinux original.
 - 1.1. Elimine la regla de contexto de archivos que agregó en el trabajo de laboratorio anterior.

```
[root@serverX ~]# semanage fcontext -d -t httpd_sys_content_t '/custom(/.*)?'
```

- 1.2. Cambie los contextos de archivos a sus valores originales.

```
[root@serverX ~]# restorecon -Rv /custom
restorecon reset /custom context unconfined_u:object_r:httpd_sys_content_t:s0
->unconfined_u:object_r:default_t:s0
restorecon reset /custom/index.html context unconfined_u:object_r:httpd_sys_
content_t:s0->unconfined_u:object_r:default_t:s0
```

2. Abra un navegador web en **serverX** e intente ver la siguiente URL: **http://localhost/index.html**. Recibirá un mensaje de error que dice que no tiene permiso para acceder al archivo.
3. Visualice los contenidos de **/var/log/messages**. Debería ver un resultado similar al siguiente:

```
[root@serverX ~]# less /var/log/messages
[... Output omitted ...]
Feb 19 12:00:35 serverX setroubleshoot: SELinux is preventing /usr/sbin/httpd
from getattr access on the file . For complete SELinux messages. run
sealert -l 82ead554-c3cb-4664-85ff-e6f256437c6c
```

```
[... Output omitted ...]
```

4. Ejecute el comando **sealert** sugerido y vea si puede identificar el problema y hallar una posible solución.

```
[root@serverX ~]# sealert -l 82ead554-c3cb-4664-85ff-e6f256437c6c
SELinux is preventing /usr/sbin/httpd from setattr access on the file .

***** Plugin catchall_labels (83.8 confidence) suggests *****
If you want to allow httpd to have setattr access on the file
Then you need to change the label on $FIX_TARGET_PATH
Do
# semanage fcontext -a -t FILE_TYPE '$FIX_TARGET_PATH'
where FILE_TYPE is one of the following: NetworkManager_log_t, ...
httpd_sys_content_t, httpd_sys_htaccess_t, httpd_sys_ra_content_t,
httpd_sys_rw_content_t, httpd_sys_script_exec_t, httpd_tmp_t, ...
Then execute:
restorecon -v '$FIX_TARGET_PATH'

***** Plugin catchall (17.1 confidence) suggests *****
If you believe that httpd should be allowed setattr access on the file by
default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# grep httpd /var/log/audit/audit.log | audit2allow -M mypol
# semodule -i mypol.pp

Additional Information:
Source Context          system_u:system_r:httpd_t:s0
Target Context          unconfined_u:object_r:default_t:s0
Target Objects          [ file ]
Source                 httpd
Source Path             /usr/sbin/httpd
Port                  <Unknown>
Host                  serverX.example.com
Source RPM Packages    httpd-2.4.6-14.el7.x86_64
Target RPM Packages   selinux-policy-3.12.1-124.el7.noarch
Policy RPM             True
Selinus Enabled         targeted
Policy Type            Enforcing
Enforcing Mode         Enforcing
Host Name              serverX.example.com
Platform               Linux serverX.example.com 3.10.0-84.el7.x86_64 #1
                                      SMP Tue Feb 4 16:28:19 EST 2014 x86_64 x86_64
Alert Count             9
First Seen              2014-02-19 10:33:06 EST
Last Seen               2014-02-19 12:00:32 EST
Local ID                82ead554-c3cb-4664-85ff-e6f256437c6c

Raw Audit Messages
type=AVC msg=audit(1392829232.3:1782): avc: denied { setattr } for
  pid=11870 comm="httpd" path="/custom/index.html" dev="vda1" ino=11520682
  scontext=system_u:system_r:httpd_t:s0
  tcontext=unconfined_u:object_r:default_t:s0 tclass=file

type=SYSCALL msg=audit(1392829232.3:1782): arch=x86_64 syscall=lstat success=no
  exit=EACCES a0=7f1854a3b068 a1=7fff493f2ff0 a2=7fff493f2ff0
  a3=ffffffffffff items=0 ppid=11866 pid=11870 auid=4294967295 uid=48
```

```
gid=48 euid=48 suid=48 egid=48 sgid=48 fsgid=48 tty=(none)
ses=4294967295 comm=httpd exe=/usr/sbin/httpd
subj=system_u:system_r:httpd_t:s0 key=(null)

Hash: httpd,httpd_t,default_t,file,getattr
```

- Lea el resultado desde el comando **sealert**. Identifique con qué archivo el servidor web Apache está teniendo problemas y busque una posible solución.

- En la parte superior del resultado, se recomienda una solución.

```
# semanage fcontext -a -t FILE_TYPE '$FIX_TARGET_PATH'
where FILE_TYPE is one of the following: NetworkManager_log_t, ...,
httpd_sys_content_t, httpd_sys_htaccess_t, httpd_sys_ra_content_t,
httpd_sys_rw_content_t, httpd_sys_script_exec_t, httpd_tmp_t, ...
Then execute:
restorecon -v '$FIX_TARGET_PATH'
```

- Observe el mensaje AVC sin formato para identificar el archivo y el proceso relevantes que están provocando la alerta.

```
Raw Audit Messages
type=AVC msg=audit(1392829232.3:1782): avc: denied { getattr } for
pid=11870 comm="httpd" path="/custom/index.html" dev="vda1" ino=11520682
scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:default_t:s0 tclass=file
```

- El proceso involucrado en la denegación por seguridad es el servidor web de Apache **httpd** y el archivo es **/custom/index.html**.

- Anteriormente, resolvimos este problema usando **semanage** y **restorecon**. Debe decidir si la violación de SELinux es una violación de seguridad o si es un acceso legítimo que requiere un ajuste de SELinux para manejar una estructura de directorios no estándar.

Trabajo de laboratorio: Administración de seguridad de SELinux

En este trabajo de laboratorio, resolverá un problema de denegación de acceso de SELinux. Los administradores de sistemas tienen problemas para obtener un nuevo servidor web para proporcionar contenido a clientes cuando SELinux está en modo de cumplimiento.

Resuelva este problema al hacer ajustes a SELinux. No deshabilite SELinux ni lo ponga en modo permisivo. No traslade el contenido web ni reconfigure Apache de ningún modo.

Recursos	
Máquinas:	serverX

Resultados:

Iniciar un servidor web en **serverX** y dirigirlo a **http://localhost/lab-content** mostrará contenido web en lugar de un mensaje de error.

Andes de comenzar

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

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

1. Inicie un navegador web en **serverX** y diríjase a **http://localhost/lab-content**. Verá un mensaje de error.
2. Investigue e identifique el problema de SELinux que evita que Apache proporcione el contenido web.
3. Resuelva el problema de SELinux que evita que Apache proporcione el contenido web.
4. Verifique que el problema de SELinux se haya resuelto y que Apache pueda proporcionar contenido web.
5. Ejecute el comando **lab selinux grade** para confirmar sus hallazgos.

Solución

En este trabajo de laboratorio, resolverá un problema de denegación de acceso de SELinux. Los administradores de sistemas tienen problemas para obtener un nuevo servidor web para proporcionar contenido a clientes cuando SELinux está en modo de cumplimiento.

Resuelva este problema al hacer ajustes a SELinux. No deshabilite SELinux ni lo ponga en modo permisivo. No traslade el contenido web ni reconfigure Apache de ningún modo.

Recursos	
Máquinas:	serverX

Resultados:

Iniciar un servidor web en **serverX** y dirigirlo a **http://localhost/lab-content** mostrará contenido web en lugar de un mensaje de error.

Andes de comenzar

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

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

1. Inicie un navegador web en **serverX** y diríjase a **http://localhost/lab-content**. Verá un mensaje de error.
2. Investigue e identifique el problema de SELinux que evita que Apache proporcione el contenido web.

Observe en **/var/log/messages** para ver mensajes de error útiles.

```
[root@serverX ~]# tail /var/log/messages
[... Output omitted ...]
Feb 20 13:55:59 serverX dbus-daemon: dbus[427]: [system] Successfully activated
    service 'org.fedoraproject.Setroubleshootd'
Feb 20 13:55:59 serverX dbus[427]: [system] Successfully activated service
    'org.fedoraproject.Setroubleshootd'
Feb 20 13:56:01 serverX setroubleshoot: Plugin Exception restorecon
Feb 20 13:56:01 serverX setroubleshoot: SELinux is preventing /usr/sbin/httpd
    from open access on the file . For complete SELinux messages. run sealert -l
    160daebd-0359-4f72-9dde-46e7fd244e27
```

Especialmente, observe los mensajes de **setroubleshootd**. Ejecute **sealert** para obtener información más detallada sobre el error de SELinux.

```
[root@serverX ~]# sealert -l 160daebd-0359-4f72-9dde-46e7fd244e27
SELinux is preventing /usr/sbin/httpd from open access on the file .

***** Plugin catchall_boolean (89.3 confidence) suggests *****

If you want to allow httpd to read user content
Then you must tell SELinux about this by enabling the 'httpd_read_user_content'
boolean.
You can read 'None' man page for more details.
Do
```

Capítulo 5. Permisos de SELinux

```
setsebool -P httpd_read_user_content 1

***** Plugin catchall (11.6 confidence) suggests *****

If you believe that httpd should be allowed open access on the file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# grep httpd /var/log/audit/audit.log | audit2allow -M mypol
# semodule -i mypol.pp

Additional Information:
Source Context          system_u:system_r:httpd_t:s0
Target Context          unconfined_u:object_r:user_tmp_t:s0
Target Objects          [ file ]
Source                 httpd
Source Path             /usr/sbin/httpd
Port                  <Unknown>
Host                  serverX.example.com
Source RPM Packages   httpd-2.4.6-14.el7.x86_64
Target RPM Packages   selinux-policy-3.12.1-124.el7.noarch
Policy RPM             True
Selinux Enabled         targeted
Policy Type            Enforcing
Enforcing Mode         serverX.example.com
Host Name              Linux serverX.example.com 3.10.0-84.el7.x86_64 #1
Platform               SMP Tue Feb 4 16:28:19 EST 2014 x86_64 x86_64
Alert Count             1
First Seen              2014-02-20 13:55:56 EST
Last Seen               2014-02-20 13:55:56 EST
Local ID                160daebd-0359-4f72-9dde-46e7fd244e27

Raw Audit Messages
type=AVC msg=audit(1392922556.862:494): avc: denied { open } for pid=24492
comm="httpd" path="/var/web-content/lab-content/index.html" dev="vda1"
ino=29062705 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:user_tmp_t:s0 tclass=file

type=SYSCALL msg=audit(1392922556.862:494): arch=x86_64 syscall=open success=no
exit=EACCES a0=7fda4c92eb40 a1=80000 a2=0 a3=0 items=0 ppid=24487 pid=24492
auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48
tty=(none) ses=4294967295 comm=httpd exe=/usr/sbin/httpd
subj=system_u:system_r:httpd_t:s0 key=(null)

Hash: httpd,httpd_t,user_tmp_t,file,open
```

Al mirar más de cerca los mensajes de auditoría sin formato, observará que Apache no puede acceder a **/var/web-content/lab-content/index.html**.

- Resuelva el problema de SELinux que evita que Apache proporcione el contenido web.

/var/web-content no es una ubicación estándar para contenido web de Apache.
Muestre el contexto de **/var/web-content** de SELinux y la root del documento estándar, **/var/www/html**.

```
[root@serverX ~]# ls -d -Z /var/web-content /var/www/html
drwxr-xr-x. root root unconfined_u:object_r:var_t:s0    /var/web-content
```

```
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /var/www/html
```

Cree una regla de contextos de archivos que establezca el tipo predeterminado en **httpd_sys_content_t** para **/var/web-content** y todos los archivos debajo de este.

```
[root@serverX ~]# semanage fcontext -a -t httpd_sys_content_t '/var/web-content(/.*)?'
```

Use el comando **restorecon** para establecer el contexto de SELinux para los archivos de **/var/web-content**.

```
[root@serverX ~]# restorecon -R /var/web-content/
```

4. Verifique que el problema de SELinux se haya resuelto y que Apache pueda proporcionar contenido web.

Use su navegador web para actualizar el enlace **http://localhost/lab-content**. Ahora debería ver algo de contenido web.

```
This is the content for the SELinux chapter test.
```

5. Ejecute el comando **lab selinux grade** para confirmar sus hallazgos.

```
[root@serverX ~]# lab selinux grade  
Confirming SELinux is in enforcing mode...PASS  
Confirming files are in expected location...PASS  
Confirming the Apache DocumentRoot is unchanged...PASS  
Confirming the web content is accessible...PASS
```

Resumen

Habilitación y supervisión de Security Enhanced Linux (SELinux)

- **getenforce** muestra el modo de SELinux actual, que determina si las reglas de SELinux se aplican.
- La opción **-Z** para **ls** y **ps** muestra las etiquetas de contexto de SELinux en archivos y procesos.
- **getsebool -a** muestra todos los booleanos de SELinux y su valor actual.

Cambio de modos de SELinux

- **setenforce** modifica el modo actual de SELinux de un sistema.
- El modo predeterminado de SELinux de un sistema se define en el archivo **/etc/selinux/config**.

Cambio de contextos de SELinux

- El comando **semanage fcontext** se usa para administrar las reglas de políticas de SELinux que determinan el contexto predeterminado para archivos y directorios.
- **restorecon** aplica el contexto definido por la política de SELinux a archivos y directorios.
- Si bien el comando **chcon** puede cambiar los archivos de contexto de SELinux, no se debe usar porque es posible que el cambio no persista.

Cambio de booleanos de SELinux

- **setsebool** activa/desactiva reglas de políticas de SELinux.
- **semanage boolean -l** muestra el valor persistente de booleanos de SELinux.
- Las páginas del manual que finalizan con **_selinux** a menudo proporcionan información útil sobre booleanos de SELinux.

Solución de problemas de SELinux

- **setroubleshootd** genera los mensajes de registro en **/var/log/messages**.
- El comando **sealert** muestra información útil que ayuda con la solución de problemas de SELinux.



CAPÍTULO 6

ADMINISTRACIÓN DE PROCESOS

Descripción general	
Meta	Evaluar y controlar los procesos que se ejecutan en un sistema Red Hat Enterprise Linux.
Objetivos	<ul style="list-style-type: none">Finalizar y controlar los procesos mediante señales.Monitorear el uso de recursos y la carga del sistema debido a la actividad del proceso.Establecer niveles de nice sobre procesos nuevos y existentes.
Secciones	<ul style="list-style-type: none">Finalización de procesos (y práctica)Supervisión de la actividad de procesos (y práctica)Uso de nice y renice para influir en la prioridad de procesos (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">Administración de la prioridad de los procesos de Linux

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 Predeterminado	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

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 **pkill**. 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 librería GNU C*)

- Sección 24: Manejo de señales

info libc processes (*Manual de referencia de la librería 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.

Andes 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
```

Capítulo 6. Administración de procesos

```
[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 adicionales.

```
[student@serverX ~]$ kill -SIGTERM %number  
[student@serverX ~]$ kill -SIGTERM %number  
[student@serverX ~]$ jobs  
[student@serverX ~]$ pkill -SIGTERM tail  
[student@serverX ~]$
```

Supervisión 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 subprocesso 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.

- 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 librerías 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.

Andes 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 prompt 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 adicionales.

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

Objetivos

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

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

Informe de niveles nice

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

Visualización de niveles nice con el comando top

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

Visualización de niveles nice con el comando ps

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

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

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



Importante

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

Inicio de procesos con un nivel nice diferente

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

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

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



Importante

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

Cambio del nivel nice de un proceso existente

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

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

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

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



Importante

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

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



Referencias

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

Práctica: Detección de prioridades de procesos

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

Recursos	
Máquinas:	desktopX

Resultados:

Un recorrido interactivo de los efectos de niveles nice.

Antes de comenzar

Ninguno

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

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

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

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



nota

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

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

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

3.1.

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

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

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

- 4.2. El porcentaje de la CPU para todos los procesos **sha1sum** es aproximadamente igual.
5. Use el comando **killall** para finalizar todos los procesos **sha1sum**.

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

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

6.1. [student@desktopX ~]\$ for I in \$(seq \$((NCORES*2-1)))
> do
> sha1sum /dev/zero &
> done
[student@desktopX ~]\$ nice -n10 sha1sum /dev/zero &

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

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

- 7.2. La instancia de **sha1sum** con el nivel nice de **10** obtiene significativamente menos CPU que otras instancias.
8. Use el comando **renice** para establecer el nivel nice de **sha1sum** con un nivel nice de **10** hasta **5**. El PID debería aún estar visible en el resultado del paso anterior.

¿Funcionó? ¿Por qué no?

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

- 8.2. Los usuarios sin privilegios no tienen permitido establecer valores nice negativos ni disminuir el valor nice de un proceso existente.
9. Mediante el uso de los comandos **sudo** y **renice**, establezca el nivel nice del proceso que identificó en el paso anterior en **-10**.

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

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

10.1 [student@desktopX ~]\$ sudo top

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

Capítulo 6. Administración de procesos

- 10.3Presione **r** para ingresar *en el modo renice* y, luego, ingrese el PID que identificó o presione **Enter** si el PID predeterminado ofrecido es el que desea.
- 10.4Ingresé **0**, luego presione **Enter**.
- 10.5Todos los comandos **sha1sum** están una vez más usando una cantidad (casi) igual de la CPU.
11. **Importante:** Limpie todo al salir de **top** y al eliminar todos sus procesos **sha1sum**.
- 11.1Presione **q** para salir de **top**.
- 11.2 [student@desktopx ~]\$ **killall sha1sum**

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

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

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

Resultados:

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

Andes de comenzar

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

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

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

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

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

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

Solución

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

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

Resultados:

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

Andes de comenzar

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

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

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

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

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

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

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

2.1.

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

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

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

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

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

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

Resumen

Finalización de procesos

Use señales para detener, iniciar y recargar procesos y configuraciones de procesos.

Supervisión de la actividad de procesos

Administrar la carga de trabajo del sistema mediante el uso de promedios de cargas y estadísticas de procesos.

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

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



CAPÍTULO 7

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.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.
Secciones	<ul style="list-style-type: none">Asignación de suscripciones a sistemas para actualizaciones de software (y práctica)Administración de actualizaciones de software con yum (y práctica)Habilitación de repositorios de software yum (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">Instalación y actualización de paquetes de software

Asignación de suscripciones a sistemas 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**.

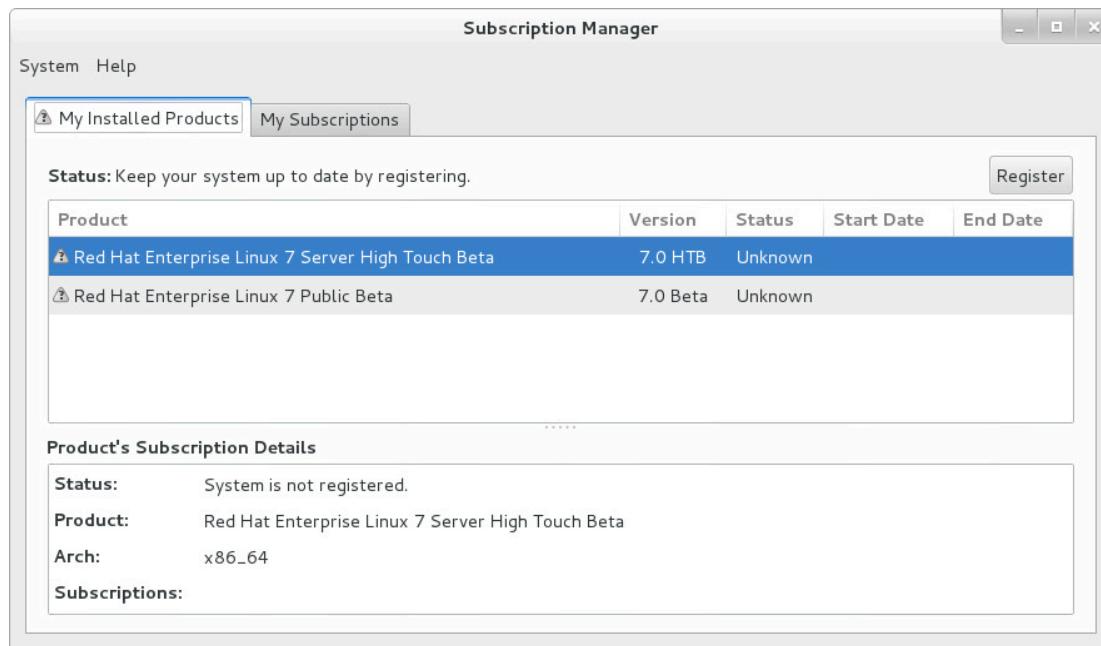
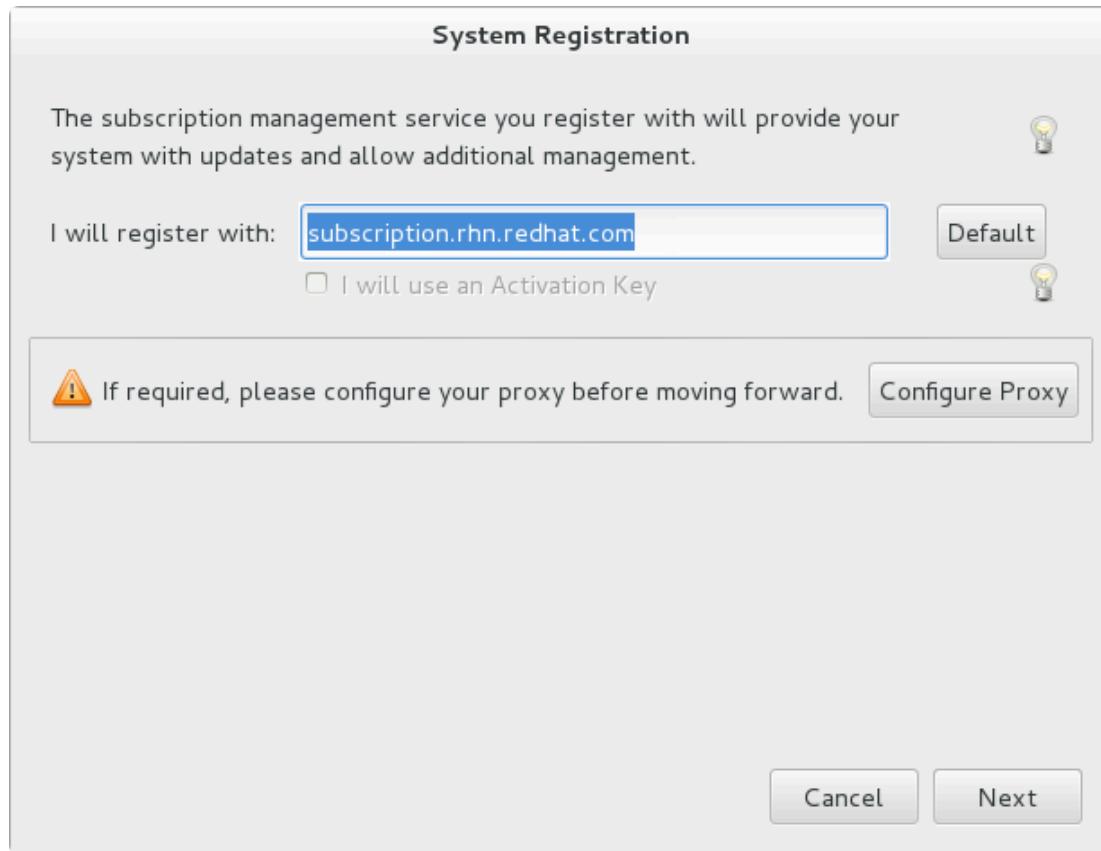


Figura 7.1: Ventana principal del administrador de suscripciones de Red Hat

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 7. Actualización de paquetes de software

Figura 7.2: 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.

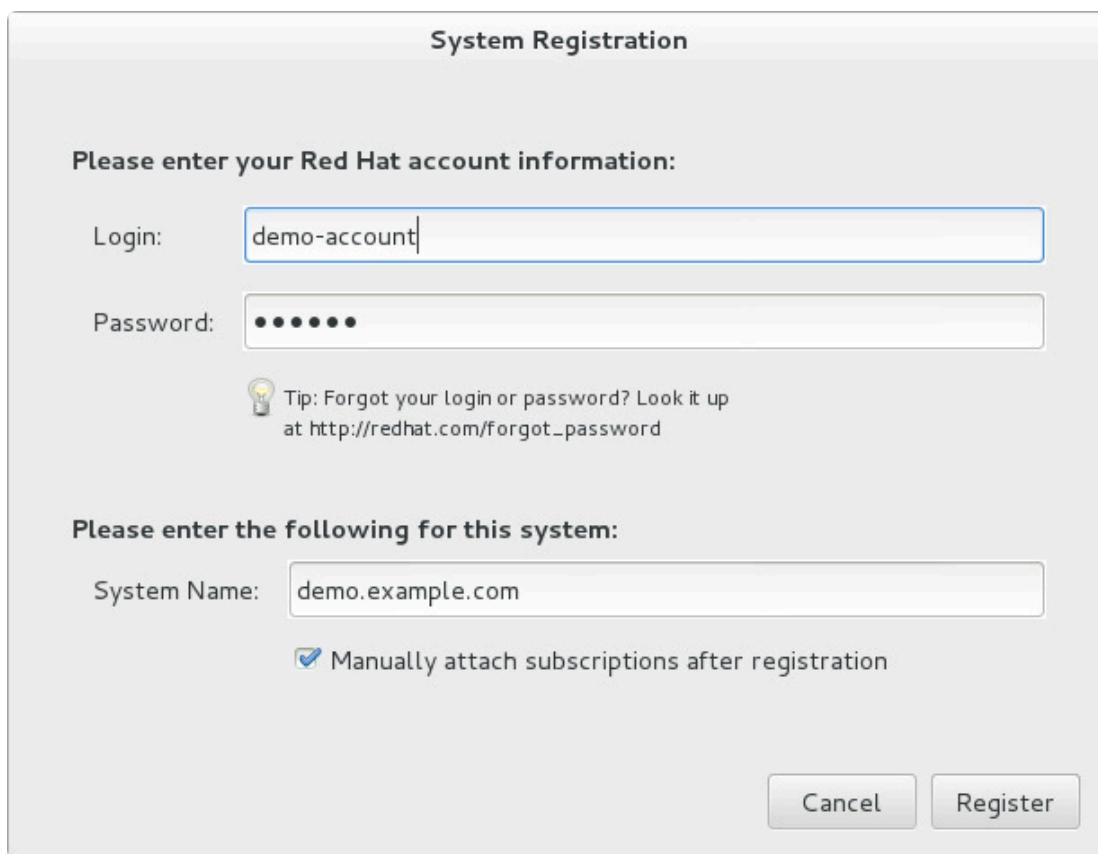


Figura 7.3: Cuadro de diálogo de información de cuenta del administrador de suscripciones de Red Hat

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.

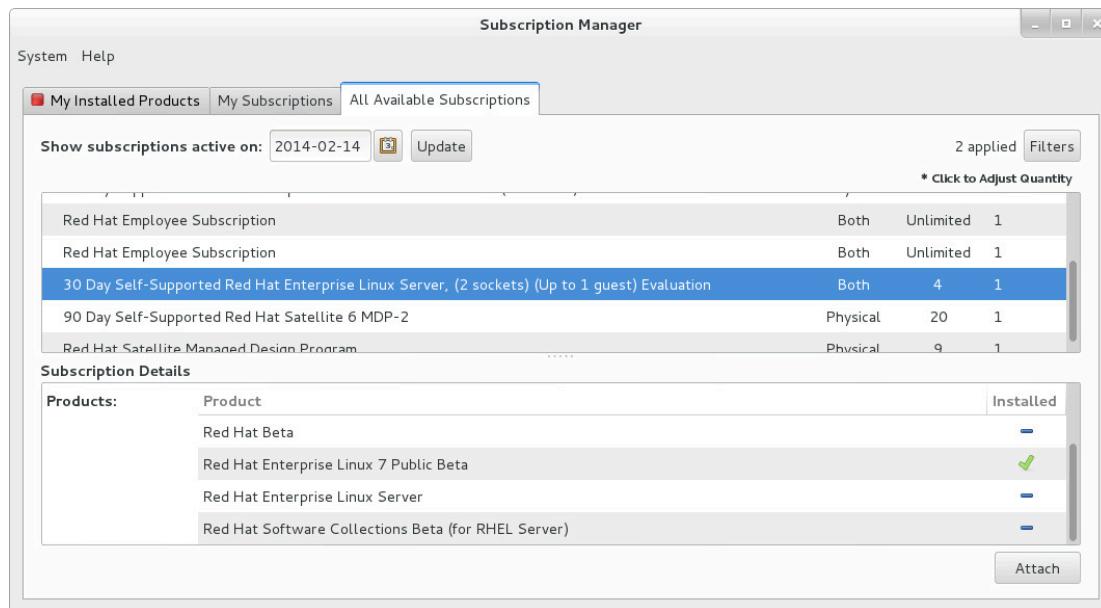


Figura 7.4: Pestaña All Available Subscriptions del administrador de suscripciones de Red Hat

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*.

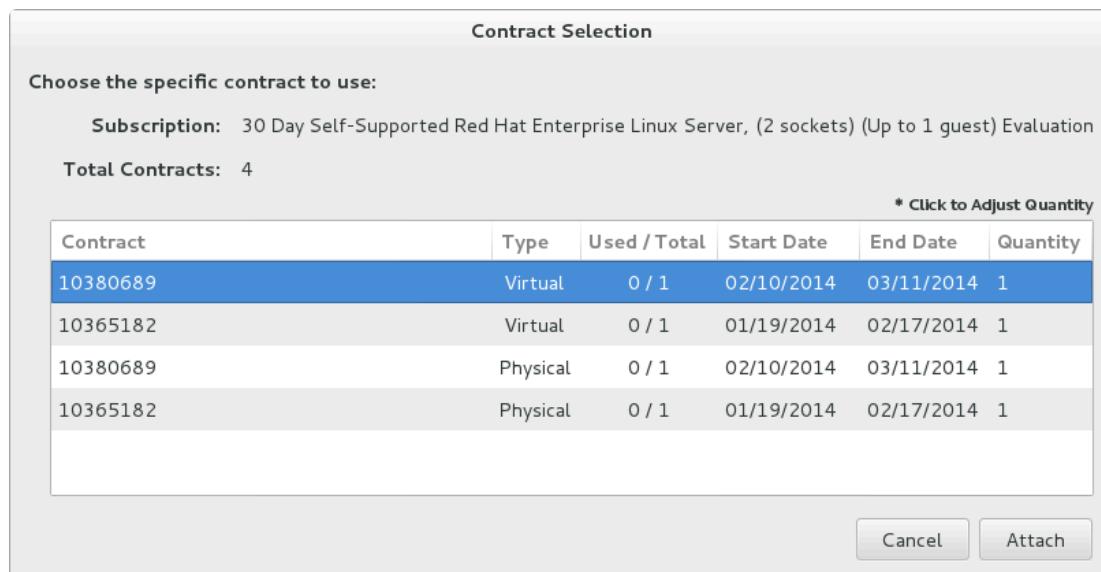


Figura 7.5: Cuadro de diálogo Contract Selection del administrador de suscripciones de Red Hat

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

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.

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
```

Capítulo 7. Actualización de paquetes de software

```
--> 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 *PACKAGENAME*** 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 *PACKAGENAME*, 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.



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-htb-
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-admin-tools
  +ipa-server
  +pkcs11-kit
Optional Packages:
  +ipa-server-trust-ad
  +nuxwdog
  +slapd-nis
```

- 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: libnfs-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**.

[root@serverX ~]# yum history				
Loaded plugins: langpacks				
ID	Login user	Date and time	Action(s)	Altered

```
-----
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
history list
```

- 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
```

Capítulo 7. Actualización de paquetes de software

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.
```

```
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 deshacer para eliminar 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 deberán 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
[rhel-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

Capítulo 7. Actualización de paquetes de software

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

- 1.1. 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
```

- 1.2. 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
```

2. 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
...
```

3. Actualice todo el software relevante proporcionado mediante el uso de **yum update**.

```
[root@serverX ~]# yum update -y
```

-
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. Muestre 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  
...
```

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.

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

Asignación de suscripciones a sistemas para actualizaciones de software

El registro de sistemas permite el acceso a actualizaciones de software para productos instalados.

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**.



CAPÍTULO 8

CREACIÓN Y MONTAJE DE SISTEMAS DE ARCHIVOS

Descripción general	
Meta	Crear y administrar discos, particiones y sistemas de archivos desde la línea de comandos.
Objetivos	<ul style="list-style-type: none">• Acceder al contenido de los sistemas de archivos.• Administrar particiones simples y sistemas de archivos.• Administrar espacio swap (intercambio).
Secciones	<ul style="list-style-type: none">• Montaje y desmontaje de sistemas de archivos (y práctica)• Adición de particiones, sistemas de archivos y montajes persistentes (y práctica)• Administración de espacio swap (intercambio) (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">• Agregar discos, particiones y sistemas de archivos a un sistema Linux

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.

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 prompt 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
```

Adición de particiones, sistemas de archivos y montajes persistentes

Objetivos

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

- Crear y eliminar particiones de disco en discos con esquema de partición MBR usando **fdisk**.
- Crear y eliminar particiones de disco en discos con esquema de partición GPT usando **gdisk**.
- Formatear dispositivos con sistemas de archivos usando **mkfs**.
- Montar sistemas de archivos en el árbol del directorio.

Partición del disco

La partición de discos permite la división de un disco duro en varias unidades de almacenamiento lógico denominadas particiones. Al separar un disco en particiones, los administradores de sistemas pueden usar diferentes particiones para realizar diferentes funciones. Algunos ejemplos de situaciones en las cuales la partición del disco es necesaria o beneficiosa son:

- Limitar espacio disponible para aplicaciones o usuarios.
- Permitir varios arranques de diferentes sistemas operativos desde el mismo disco.
- Separar archivos de programa y de sistemas operativos de archivos de usuarios.
- Crear un área separada para el swapping (intercambio) de memoria virtual del sistema operativo.
- Limitar el uso de espacio en disco para mejorar el rendimiento de herramientas de diagnóstico e imágenes de copia de seguridad.

Esquema de partición MBR

Desde 1982, el esquema de partición de *registro de arranque maestro (Master Boot Record, MBR)* ha dictado cómo los discos se deben particionar en sistemas que ejecutan firmware de BIOS. Este esquema admite un máximo de cuatro particiones principales. En sistemas Linux, con el uso de particiones extendidas y lógicas, el administrador puede crear un máximo de 15 unidades. Dado que los datos del tamaño de la partición se almacenan como valores de 32 bits, los discos particionados con el esquema MBR tienen un límite de tamaño de disco y partición máximo de 2 TiB.

Con la aparición de discos duros de cada vez más capacidad, el límite de tamaño de disco y partición de 2 TiB del esquema de partición MBR antiguo ya no es un límite teórico sino un problema del mundo real que se presenta cada vez con más frecuencia en entornos de producción. Como consecuencia, el esquema MBR heredado está en proceso de ser sustituido por el nuevo *esquema GUID Partition Table (GPT)* para la partición de disco.

Esquema de partición de GPT

Para sistemas que ejecutan *firmware Unified Extensible Firmware Interface (UEFI)*, GPT es el estándar para el diseño de tablas de partición en discos duros físicos. GPT es parte del estándar UEFI y aborda muchas de las limitaciones impuestas por el antiguo esquema basado en MBR. Según las especificaciones de UEFI, de forma predeterminada, GPT admite hasta 128 particiones. A diferencia de MBR, que usa 32 bits para almacenar información de tamaño y direcciones en bloques lógicos, GPT asigna 64 bits para direcciones en bloques lógicos. Esto asigna GPT para incluir particiones y discos de hasta 8 zebibyte (ZiB), u 8 mil millones de tebibbytes.



nota

El límite de 8 ZiB de GPT se basa en un tamaño de bloque de 512 bytes. Con proveedores de discos duros que cambian a bloques de 4096 bytes, este límite aumentará a 64 ZiB.

Además de abordar las limitaciones del esquema de partición MBR, GPT también ofrece algunas funciones y beneficios adicionales. Como lo indica su nombre, GPT usa GUID de 128 bits para identificar de forma única cada disco y partición. En contraste con MBR, que tiene un único punto de falla, GPT ofrece redundancia de la información de su tabla de particiones. El GPT principal reside en el cabezal del disco, mientras que una copia de seguridad, el GPT secundario, se aloja en el extremo del disco. Además, GPT emplea el uso de la suma de comprobación CRC para detectar errores y daños en la tabla de particiones y el encabezado de GPT.

Administración de particiones MBR con fdisk

Los editores de particiones son programas que permiten a los administradores hacer cambios en particiones de discos, como crear particiones, eliminar particiones y cambiar el tipo de partición. En el caso de discos con esquema de partición MBR, el editor de particiones **fdisk** se puede usar para realizar estas operaciones.

Creación de particiones de disco MBR

La creación de una partición de disco estilo MBR incluye ocho pasos:

1. Especifique el dispositivo de disco donde creará la partición.

Como usuario **root**, ejecute el comando **fdisk** y especifique el nombre del dispositivo de disco como un argumento. Esto iniciará el comando **fdisk** en modo interactivo, y presentará un prompt de comando.

```
[root@serverX ~]# fdisk /dev/vdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help):
```

2. Solicite una nueva partición primaria o extendida.

Ingrese **n** para solicitar una nueva partición y especifique si esta debe ser creada como una *partición primaria* o extendida. La selección predeterminada es el tipo de partición *primaria*.

```
Partition type:
  p  primary (0 primary, 0 extended, 4 free)
  e  extended
Select (default p): p
```



nota

En el caso de situaciones donde se necesitan más de cuatro particiones en un disco, este límite se puede omitir al crear tres particiones primarias y una partición extendida. Esta partición extendida sirve como contenedor dentro del cual se pueden crear varias particiones lógicas.

- Especifique un número de partición.

Este número de partición sirve como número de identificación de la nueva partición en el disco para usar en futuras operaciones de partición. El valor predeterminado es el número de partición no usado más bajo.

```
Partition number (1-4, default 1): 1
```

- Especifique el primer sector en el disco donde se iniciará la nueva partición.

El valor predeterminado es el primer sector disponible en el disco.

```
First sector (2048-20971519, default 2048): 2048
```

- Especifique el último sector en el disco donde finalizará la nueva partición.

El valor predeterminado es el último de los sectores disponibles, no asignados, contiguos al primer sector de la nueva partición.

```
Last sector, +sectors or +size{K,M,G} (6144-20971519, default 20971519): 1050623
```

Además del número de sector final, **fdisk** también puede aceptar un número que represente el tamaño deseado de la partición expresado en sectores.

```
Last sector, +sectors or +size{K,M,G} (6144-20971519, default 20971519): +52488
```

La opción de entrada final, y la más simple para el usuario, ofrecida por **fdisk** es especificar el tamaño de la nueva partición en unidades de KiB, MiB o GiB.

```
Last sector, +sectors or +size{K,M,G} (6144-20971519, default 20971519): +512M
```

Capítulo 8. Creación y montaje de sistemas de archivos

Una vez que se ingresa la delimitación final de la partición, **fdisk** mostrará una confirmación de la creación de la partición.

```
Partition 1 of type Linux and of size 512 MiB is set
```

- Defina el tipo de partición.

Si la partición recientemente creada debe tener un tipo diferente de *Linux*, ingrese el comando **t** para cambiar un tipo de partición. Ingrese el código hex para el nuevo tipo de partición. En caso de ser necesario, con el comando **L**, se puede mostrar una tabla de códigos hex para todos los tipos de partición. La configuración correcta del tipo de partición es fundamental, dado que algunas herramientas se basan en esta para funcionar adecuadamente. Por ejemplo, cuando el kernel de Linux encuentra una partición de tipo *0xfd*, Linux RAID, intentará iniciar automáticamente el volumen de RAID.

```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 82
Changed type of partition 'Linux' to 'Linux swap / Solaris'
```

- Guarde los cambios de la tabla de particiones.

Emita el comando **w** para finalizar la solicitud de creación de la partición; para ello, escriba los cambios en la tabla de particiones del disco y salga del programa **fdisk**.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource
busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

- Inicie una nueva lectura del kernel de la nueva tabla de particiones.

Ejecute el comando **partprobe** con el nombre del dispositivo del disco como argumento para forzar una nueva lectura de su tabla de particiones.

```
[root@serverX ~]# partprobe /dev/vdb
```



Importante

El programa **fdisk** pone en cola todas las ediciones de la tabla de particiones y las escribe en el disco solo cuando el administrador emite el comando **w** para escribir todos los cambios de la tabla de particiones en el disco. Si el nuevo comando **w** no se ejecuta antes de salir de la sesión de **fdisk** interactiva, todos los cambios solicitados para la tabla de particiones se descartarán y la tabla de particiones del disco permanecerá igual. Esta función es especialmente útil cuando se emiten comandos erróneos a **fdisk**. Para descartar los comandos erróneos y evitar consecuencias no deseadas, simplemente salga de **fdisk** sin guardar los cambios de la tabla de particiones.

Eliminación de particiones del disco MBR

Se deben seguir cinco pasos para eliminar una partición de un disco con un diseño de partición MBR usando **fdisk**.

1. Especifique el disco que contiene la partición que se eliminará.

Ejecute el comando **fdisk** y especifique el nombre del dispositivo de disco como un argumento.

```
[root@serverX ~]# fdisk /dev/vdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help):
```

2. Identifique el número de partición de la partición que se eliminará.

Ingrese **p** para imprimir la tabla de particiones y **fdisk** mostrará información sobre el disco y sus particiones.

```
Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xd2368130

      Device Boot      Start        End    Blocks   Id  System
  /dev/vdb1            2048     1050623     524288   82  Linux swap / Solaris
```

3. Solicite la eliminación de la partición.

Ingrese el comando **d** para iniciar la eliminación de la partición y especifique el número de partición de la partición que se eliminará.

```
Command (m for help): d
Selected partition 1
Partition 1 is deleted
```

4. Guarde los cambios de la tabla de particiones.

Emita el comando **w** para finalizar la solicitud de eliminación de la partición; para ello, escriba los cambios en la tabla de particiones del disco.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource
busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

5. Inicie una nueva lectura del kernel de la nueva tabla de particiones.

Informe al kernel que vuelva a leer la tabla de particiones con **partprobe**.

```
[root@serverX ~]# partprobe /dev/vdb
```

Administración de particiones GPT con gdisk

En el caso de discos con esquema de partición GPT, el editor de particiones **gdisk** se puede usar para administrar particiones.



Advertencia

Si bien se ha agregado el soporte GPT a **fdisk**, aún se considera experimental, de modo que se debe usar el comando **gdisk** para hacer cambios en las particiones en discos particionado con el esquema de partición GPT.

Creación de particiones de disco GPT

Son ocho los pasos que se requieren para crear una partición de estilo GPT.

1. Especifique el dispositivo de disco donde creará la partición.

Ejecute el comando **gdisk** y especifique el nombre del dispositivo de disco como un argumento. Esto iniciará el comando **gdisk** en modo interactivo, y presentará un prompt de comando.

```
[root@serverX ~]# gdisk /dev/vdb
GPT fdisk (gdisk) version 0.8.6

Partition table scan:
  MBR: not present
  BSD: not present
```

```

APM: not present
GPT: not present

Creating new GPT entries.

Command (? for help):

```

- Solicite una nueva partición.

Ingrese **n** para crear una nueva partición.

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

- Especifique el número de partición.

Este número de partición sirve como número de identificación de la partición en el disco para usar en futuras operaciones de partición. El valor predeterminado es el número de partición no usado más bajo.

```
Partition number (1-128, default 1): 1
```

- Especifique la ubicación del disco desde donde se iniciará la nueva partición.

gdisk permite dos tipos de entradas diferentes. El primer tipo de entrada es un número de sector de disco absoluto que representa el primer sector de la nueva partición.

```
First sector (34-20971486, default = 2048) or {+-}size{KMGTP}: 2048
```

El segundo tipo de entrada indica el sector de inicio de la partición por su posición relativa al primero o último sector del primer bloque contiguo de sectores libres en el disco. Al usar este formato de posición de sector relativo, la entrada se especifica en unidades de KiB, MiB, GiB, TiB o PiB.

Por ejemplo, un valor de **+512 M** significa una posición de sector que está 512 MiB **luego** del comienzo del siguiente grupo de sectores disponibles contiguos. Por otra parte, un valor de **-512 M** denota un sector posicionado 512 MiB *antes* del final de este grupo de sectores disponibles contiguos.

- Especifique el último sector en el disco donde finalizará la nueva partición.

El valor predeterminado es el último de los sectores disponibles, no asignados, contiguos al primer sector de la nueva partición.

```
Last sector (2048-20971486, default = 20971486) or {+-}size{KMGTP}: 1050623
```

Además del número de sector de finalización absoluto, **gdisk** también ofrece la opción de entrada más simple para el usuario de especificar la delimitación final de la nueva partición en unidades de KiB, MiB, GiB, TiB, o PiB desde el comienzo o el final del grupo de sectores disponibles contiguos. Un valor de **+512 M** significa una posición de partición final de 512 MiB **luego** del primer sector.

```
Last sector (2048-20971486, default = 20971486) or {+-}size{KMGTP}: +512M
```

Un valor de **-512 M** indica una posición de partición final de 512 MiB *antes* del final de sectores disponibles contiguos.

```
Last sector (2048-20971486, default = 20971486) or {+-}size{KMGTP}: -512M
```

6. Defina el tipo de partición.

Las nuevas particiones creadas por **gdisk** se establecen de forma predeterminada en el sistema de archivos de tipo *Linux*. Si se desea un tipo de partición diferente, ingrese el código hex correspondiente. En caso de ser necesario, con el comando **L**, se puede mostrar una tabla de códigos hex para todos los tipos de partición.

```
Current type is 'Linux filesystem'  
Hex code or GUID (L to show codes, Enter = 8300): 8e00  
Changed type of partition to 'Linux LVM'
```

7. Guarde los cambios de la tabla de particiones.

Emita el comando **w** para finalizar la solicitud de creación de la partición; para ello, escriba los cambios en la tabla de particiones del disco. Ingrese **y** cuando **gdisk** solicite una confirmación final.

```
Command (? for help): w  
Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING  
PARTITIONS!!  
Do you want to proceed? (Y/N): y  
OK; writing new GUID partition table (GPT) to /dev/vdb.  
The operation has completed successfully.
```

8. Inicie una nueva lectura del kernel de la nueva tabla de particiones.

Ejecute el comando **partprobe** con el nombre del dispositivo del disco como argumento para forzar una nueva lectura de su tabla de particiones.

```
[root@serverX ~]# partprobe /dev/vdb
```



Importante

El programa **gdisk** pone en cola todas las ediciones de la tabla de particiones y las escribe en el disco solo cuando el administrador emite el comando **w** para escribir todos los cambios de la tabla de particiones en el disco. Si el nuevo comando **w** no se ejecuta antes de salir de la sesión de **gdisk** interactiva, todos los cambios solicitados para la tabla de particiones se descartarán y la tabla de particiones del disco permanecerá igual. Esta función es especialmente útil cuando se emiten comandos erróneos a **gdisk**. Para descartar los comandos erróneos y evitar consecuencias no deseadas, simplemente salga de **gdisk** sin guardar los cambios de la tabla de particiones.

Eliminación de particiones del disco GPT

Son cinco los pasos necesarios para eliminar una partición de un disco con un diseño de partición GPT usando **gdisk**.

1. Especifique el disco que contiene la partición que se eliminará.

Ejecute el comando **gdisk** y especifique el nombre del dispositivo de disco como un argumento.

```
[root@serverX ~]# gdisk /dev/vdb
GPT fdisk (gdisk) version 0.8.6

Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present

Found valid GPT with protective MBR; using GPT.

Command (? for help):
```

2. Identifique el número de partición de la partición que se eliminará.

Ingrese **p** para imprimir la tabla de particiones. Anote el número en el campo *Number* (Número) de la partición que se eliminará.

```
Command (? for help): p
Disk /dev/vdb: 20971520 sectors, 10.0 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): 8B181B97-5259-4C8F-8825-1A973B8FA553
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 20971486
Partitions will be aligned on 2048-sector boundaries
Total free space is 19922877 sectors (9.5 GiB)

      Number  Start (sector)    End (sector)  Size            Code  Name
         1              2048        1050623   512.0 MiB    8E00  Linux LVM
```

3. Solicite la eliminación de la partición.

Ingrese el comando **d** para iniciar la eliminación de la partición.

```
Command (? for help): d
Using 1
```

4. Guarde los cambios de la tabla de particiones.

Emita el comando **w** para finalizar la solicitud de eliminación de la partición; para ello, escriba los cambios en la tabla de particiones del disco. Ingrese **y** cuando **gdisk** solicite una confirmación final.

```
Command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!

Do you want to proceed? (Y/N): y
OK; writing new GUID partition table (GPT) to /dev/vdb.
The operation has completed successfully.
```

5. Inicie una nueva lectura del kernel de la nueva tabla de particiones.

Informe al kernel que vuelva a leer la tabla de particiones con **partprobe**.

```
[root@serverX ~]# partprobe /dev/vdb
```

Creación de sistemas de archivos

Luego de haberse creado un dispositivo de bloque, el siguiente paso es aplicar un formato de sistema de archivos. Un sistema de archivos aplica una estructura al dispositivo de bloque de modo que se puedan almacenar y recuperar datos de este. Red Hat Enterprise Linux admite muchos tipos de sistema de archivos diferentes, pero dos tipos comunes son **xfs** y **ext4**. **xfs** se utiliza de forma predeterminada en **anaconda**, el instalador de Red Hat Enterprise Linux.

El comando **mkfs** se puede usar para aplicar un sistema de archivos a un dispositivo de bloque. Si no se especifica un tipo específico, se usará un sistema de archivos de tipo extendido dos (ext2), el cual no es deseable para muchos usos. Para especificar el tipo de sistema de archivos, se debe usar un **-t**.

```
[root@serverX ~]# mkfs -t xfs /dev/vdb1
meta-data=/dev/vdb1              isize=256    agcount=4, agsize=16384 blks
                                =          sectsz=512   attr=2, projid32bit=1
                                =          crc=0
data      =          bsize=4096   blocks=65536, imaxpct=25
                                =          sunit=0    swidth=0 blks
naming   =version 2             bsize=4096   ascii-ci=0 ftype=0
log       =internal log         bsize=4096   blocks=853, version=2
                                =          sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                  extsz=4096   blocks=0, rtextents=0
```

Montaje de sistemas de archivos

Una vez aplicado el formato de sistema de archivos, el último paso para agregar un nuevo sistema de archivos es adjuntar el sistema de archivos en la estructura de directorios. Cuando

el sistema de archivos se adjunta en una jerarquía de directorios, se puede acceder a las utilidades de espacio del usuario o escribirlas en el dispositivo.

Montaje manual de sistemas de archivos

Los administradores pueden usar el comando **mount** para adjuntar manualmente el dispositivo en una ubicación del directorio, o *punto de montaje*, al especificar el dispositivo y el punto de montaje así como cualquier opción que se pueda desear para personalizar el comportamiento del dispositivo.

```
[root@serverX ~]# mount /dev/vdb1 /mnt
```

El comando **mount** también se puede utilizar para ver los sistemas de archivos montados actualmente, los puntos de montaje y las opciones.

```
[root@serverX ~]# mount | grep vdb1
/dev/vdb1 on /mnt type xfs (rw,relatime,seclabel,attr2,inode64,noquota)
```

Montar manualmente un sistema de archivos es una manera excelente de verificar que un dispositivo formateado sea accesible o funcione de la manera deseada. No obstante, una vez que el sistema se reinicia, si bien aún existe y tiene datos intactos, no se montará en el árbol de directorios nuevamente. Si un administrador desea que el sistema de archivos se monte de forma persistente, es necesario agregar un listado para el sistema de archivos a **/etc/fstab**.

Montaje de forma persistente de sistemas de archivos

Al agregar un listado para un dispositivo en el archivo **/etc/fstab**, los administradores pueden configurar un dispositivo para montarlo en un punto de montaje en el arranque del sistema.

/etc/fstab es un archivo delimitado por espacios en blanco con seis campos por línea.

```
[root@serverX ~]# cat /etc/fstab
#
# /etc/fstab
# Created by anaconda on Thu Mar 20 14:52:46 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=7a20315d-ed8b-4e75-a5b6-24ff9e1f9838   /   xfs  defaults  1 1
```

El primer campo especifica el dispositivo que se usará. En el ejemplo anterior, el **UUID** se usa para especificar el dispositivo. De forma alternativa, se podría usar el archivo del dispositivo, por ejemplo, **/dev/vdb1**. El **UUID** se almacena en el superbloque del sistema de archivos y se crea cuando se crea el sistema de archivos.



nota

Es preferible el uso de **UUID** porque los identificadores del dispositivo de bloques pueden cambiar en determinadas situaciones, como en el caso de que un proveedor de la nube cambie la capa de almacenamiento subyacente de una máquina virtual. El archivo del dispositivo de bloques puede cambiar, pero el **UUID** permanecerá intacto en el superbloque del dispositivo.

Se puede usar el comando **blkid** para escanear los dispositivos de bloques conectados a una máquina e informar los datos como el **UUID** asignado y el formato del sistema de archivos.

```
[root@serverX ~]# blkid /dev/vdb1  
/dev/vdb1: UUID="226a7c4f-e309-4cb3-9e76-6ef972dd8600" TYPE="xfs"
```

El segundo campo es el punto de montaje donde el dispositivo debe adjuntarse en la jerarquía del directorio. El punto de montaje ya debe existir; si no, se puede crear con **mkdir**.

El tercer campo contiene el tipo de sistema de archivos que se ha aplicado al dispositivo de bloques.

El cuarto campo es la lista de opciones que debe aplicarse al dispositivo, cuando se lo monta, para personalizar el comportamiento. El campo es obligatorio, y hay un conjunto de opciones que se usan comúnmente denominadas **defaults** (valores predeterminados). Otras opciones están documentadas en la página del manual **mount**.

Los últimos dos campos son la marca dump y el orden fsck. La marca se usa con el comando **dump** para hacer una copia de seguridad del contenido del dispositivo. El campo de orden determina si el **fsck** debe ejecutarse en el momento del arranque, en el caso de que el sistema de archivos no se haya montado de forma ordenada. El valor del orden indica el orden en el que los sistemas de archivos deben ejecutar **fsck** en ellos si se requiere la revisión de múltiples sistemas.

```
UUID=226a7c4f-e309-4cb3-9e76-6ef972dd8600 /mnt xfs defaults 1 2
```



nota

Si hay una entrada incorrecta en **/etc/fstab**, es posible que la máquina no pueda volver a arrancarse. Para evitar esa situación, un administrador debe comprobar que la entrada sea válida al desmontar el sistema de archivos nuevo y usar **mount -a**, que lee **/etc/fstab**, para montar el sistema de archivos nuevamente en su lugar. Si el comando **mount -a** arroja un error, se debe corregir antes de volver a arrancar la máquina.



Referencias

Páginas del manual: **fdisk(8)**, **gdisk(8)**, **mkfs(8)**, **mount(8)**, **fstab(5)**

Práctica: Agregar particiones, sistemas de archivos y montajes persistentes

En este trabajo de laboratorio, creará una partición MBR en un disco recientemente asignado, formateará la partición con un sistema de archivos ext4 y configurará el sistema de archivos para un montaje persistente.

Recursos:	
Máquinas:	serverX

Resultados:

Sistema de archivos ext4 de 1 GiB en segundo disco montado de forma persistente en **/archive**.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en serverX.
- Cambie a **root** usando **sudo -i**.

Se le ha solicitado archivar datos en un nuevo directorio, **/archive**, en serverX. Se le ha asignado un segundo disco para este propósito. El directorio **/archive** requerirá 1 GiB de espacio. Para asegurarse de que el directorio **/archive** esté siempre disponible para usar, deberá configurar el sistema de archivos recientemente creado para montarlo de forma persistente en **/archive**, incluso luego de reiniciar el servidor.

Una vez que haya completado su trabajo, reinicie su máquina serverX y compruebe que el sistema de archivos creado recientemente se monte de forma persistente en **/archive** luego del reinicio.

1. Cree una partición MBR de 1 GiB en **/dev/vdb** de tipo **Linux**.

1.1. Use **fdisk** para modificar el segundo disco.

```
[root@serverX ~]# fdisk /dev/vdb
```

1.2. Muestre la tabla de particiones originales, y luego agregue una nueva partición que tenga un tamaño de 1 GiB.

```
Command (m for help): p
Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xfd41a9d3

Device Boot Start End Blocks Id System
Command (m for help): n
```

```
Partition type:
  p  primary (0 primary, 0 extended, 4 free)
  e  extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): Enter
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519): +1G
Partition 1 of type Linux and of size 1 GiB is set
```

1.3. Guarde los cambios de la tabla de particiones.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

1.4. Si **fdisk** emite una advertencia, ejecute el comando **partprobe** para hacer que el kernel tenga conocimiento del cambio realizado en la tabla de particiones. Esto no será necesario si el dispositivo del disco se encuentra actualmente en desuso.

```
[root@serverX ~]# partprobe
```

2. Formatee la partición recientemente creada con el sistema de archivos ext4.

```
[root@serverX ~]# mkfs -t ext4 /dev/vdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
65536 inodes, 262144 blocks
13107 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=268435456
8 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Configure el sistema de archivos recientemente creado para montarlo de forma persistente en **/archive**.

3.1. Cree el punto de montaje del directorio **/archive**.

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

3.2. Determine el UUID de la nueva partición en el segundo disco.

```
[root@serverX ~]# blkid /dev/vdb1  
/dev/vdb1: UUID="5fcb234a-cf18-4d0d-96ab-66a4d1ad08f5" TYPE="ext4"
```

3.3. Agregue una entrada a **/etc/fstab**.

```
UUID=5fcb234a-cf18-4d0d-96ab-66a4d1ad08f5 /archive ext4 defaults 0 2
```

4. Pruebe montar el sistema de archivos recientemente creado.

4.1. Ejecute el comando **mount** para montar el sistema de archivos nuevo usando la nueva entrada agregada a **/etc/fstab**.

```
[root@serverX ~]# mount -a
```

4.2. Verifique que el sistema de archivos nuevo esté montado en **/archive**.

```
[root@serverX ~]# mount | grep -w /archive  
/dev/vdb1 on /archive type ext4 (rw,relatime,seclabel,data=ordered)
```

5. Reinicie serverX. Luego de reiniciar el servidor, inicie sesión y verifique que **/dev/vdb1** se monte en **/archive**.

```
[student@serverX ~]$ mount | grep ^/  
/dev/vda1 on / type xfs (rw,relatime,seclabel,attr2,inode64,noquota)  
/dev/vdb1 on /archive type ext4 (rw,relatime,seclabel,data=ordered)
```

Administración de espacio swap (intercambio)

Objetivos

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

- Crear y formatear una partición para espacio swap (intercambio).
- Activar el espacio swap (intercambio).

Conceptos de espacio swap (intercambio)

Un *espacio swap (intercambio)* es un área del disco que se puede usar con el subsistema de administración de memoria del kernel Linux. Los espacios swap (intercambio) se utilizan para complementar la memoria RAM del sistema al contener páginas inactivas de memoria. La combinación de la memoria RAM del sistema con los espacios swap (intercambio) se denomina *memoria virtual*.

Cuando el uso de la memoria en un sistema supera un límite definido, el kernel hará un barrido de la memoria RAM en busca de páginas de memoria asignadas a los procesos, pero inactivas. El kernel escribe la página inactiva en el área swap (intercambio), y luego reasignará la página RAM que será usada por otro proceso. Si el programa requiere acceso a una página que ha sido escrita en el disco, el kernel localizará otra página de memoria inactiva, la escribirá en el disco y luego volverá a convocar la página necesaria desde el área swap (intercambio).

Dado que las áreas swap (intercambio) residen en el disco, el swap (intercambio) es increíblemente lento cuando se lo compara con la memoria RAM. Si bien se usa para aumentar la memoria RAM del sistema, el uso de espacios swap (intercambio) debe mantenerse al mínimo siempre que sea posible.

Crear un espacio swap (intercambio)

Para crear un espacio swap (intercambio), un administrador debe realizar tres acciones:

- Crear una partición.
- Establecer el tipo de partición como **82 Linux Swap**.
- Formatear una firma swap (intercambio) en el dispositivo.

Crear una partición

Use una herramienta, como **fdisk**, para crear una partición del tamaño deseado. En el siguiente ejemplo, se creará una partición de 256 MiB.

```
[root@serverX ~]# fdisk /dev/vdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0x34e4e6d7.
```

```
Command (m for help): n
Partition type:
  p  primary (0 primary, 0 extended, 4 free)
  e  extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): Enter
Using default value 2048
Last sector, +sectors or +size[K,M,G] (2048-20971519, default 20971519): +256M
Partition 1 of type Linux and of size 256 MiB is set

Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x34e4e6d7

      Device Boot      Start        End      Blocks   Id  System
/dev/vdb1            2048      526335      262144   83  Linux
```

Asignar el tipo de partición

Luego de haber creado la partición swap (intercambio), una práctica recomendada es cambiar el tipo de partición, o la id. del sistema a **82 Linux Swap**. Anteriormente, las herramientas observaban el tipo de partición para determinar si el dispositivo debía activarse; no obstante, eso ya no sucede. Si bien el tipo de partición ya no es usado por utilidades, tener el tipo establecido permite a los administradores determinar rápidamente el propósito de la partición. El siguiente ejemplo continua desde **fdisk**.

```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 82
Changed type of partition 'Linux' to 'Linux swap / Solaris'

Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x34e4e6d7

      Device Boot      Start        End      Blocks   Id  System
/dev/vdb1            2048      526335      262144   82  Linux swap / Solaris
```

Formatear el dispositivo

El comando **mkswap** aplica una *firma swap (intercambio)* al dispositivo. A diferencia de otras utilidades de formateo, **mkswap** escribe un único bloque de datos al inicio del dispositivo, dejando el resto del dispositivo sin formatear de modo que pueda utilizarse para almacenar páginas de memoria.

```
[root@serverX ~]# mkswap /dev/vdb1
Setting up swapspace version 1, size = 262140 KiB
no label, UUID=fb7fa60-b781-44a8-961b-37ac3ef572bf
```

Activar un espacio swap (intercambio)

Un administrador puede usar el comando **swapon** para activar un espacio swap (intercambio) formateado. **swapon** se puede invocar en el dispositivo, o **swapon -a** activará todos los espacios swap (intercambio) que figuran en el archivo **/etc/fstab**.

```
[root@serverX ~]# free
              total        used        free      shared      buffers      cached
Mem:       1885252      791812     1093440      17092         688      292024
-/+ buffers/cache:    499100     1386152
Swap:          0          0          0
[root@serverX ~]# swapon /dev/vdb1
[root@serverX ~]# free
              total        used        free      shared      buffers      cached
Mem:       1885252      792116     1093136      17092         692      292096
-/+ buffers/cache:    499328     1385924
Swap:      262140          0      262140
```

Activar de forma persistente un espacio swap (intercambio)

Es probable que se requiera un espacio swap (intercambio) para activar automáticamente cada vez que arranque la máquina. Para que la máquina active el espacio swap (intercambio) en cada arranque, se debe configurar en el archivo **/etc/fstab**.

En caso de ser necesario, un administrador puede desactivar un espacio swap (intercambio) usando el comando **swapoff**. Un **swapoff** solo proporcionará resultados satisfactorios si cualquier dato swapped (intercambiado) se puede escribir en otros espacios swap (intercambio) activos o nuevamente en la memoria. Si no se pueden escribir datos en otros lugares, el **swapoff** fallará, con un error, y el espacio swap (intercambio) permanecerá activo.

A continuación, se muestra una línea de ejemplo en **/etc/fstab** donde se agrega un espacio swap (intercambio) creado anteriormente.

```
UUID=fb7fa60-b781-44a8-961b-37ac3ef572bf  swap  swap  defaults  0 0
```

El ejemplo anterior usa el **UUID** como el primer campo. El **UUID** está almacenado en la firma swap (intercambio) almacenada en el dispositivo, y era parte del resultado de **mkswap**. Si el resultado de **mkswap** se ha perdido, se puede usar el comando **blkid** para escanear el sistema e informar sobre todos los dispositivos de bloques conectados. Si el administrador no desea usar el **UUID**, el nombre del dispositivo sin formato también se puede usar en el primer campo.

El segundo campo se reserva típicamente para el **punto de montaje**. Sin embargo, para dispositivos swap (intercambio), que no son accesibles a través de la estructura del directorio, este campo es el valor del marcador de posición **swap**.

El tercer campo es el tipo de sistema de archivos. El tipo de sistemas de archivos para un espacio swap (intercambio) es **swap**.

El cuarto campo es para opciones. En el ejemplo, se utiliza la opción **defaults** (valores predeterminados). **defaults** (valores predeterminados) incluye la opción de montaje **auto**, que es lo que hace que el espacio swap (intercambio) se active automáticamente en el arranque.

Los dos campos finales son la marca dump y el orden fsck. Los espacios swap (intercambio) no requieren copias de seguridad ni revisión del sistema de archivos.



nota

De forma predeterminada, los espacios swap (intercambio) se usan en serie, lo que significa que se usará el primer espacio swap (intercambio) activado hasta que esté lleno, luego el kernel empezará a usar el segundo espacio swap (intercambio). Las prioridades de los espacios swap (intercambio) se muestran con **swapon -s**, y se pueden establecer con la opción de montaje **pri=**. Si los espacios swap (intercambio) tienen la misma prioridad, el kernel los escribirá en turnos rotativos en lugar de escribir en un único espacio swap (intercambio) hasta que complete su capacidad.



Referencias

Páginas del manual: **mkswap(8)**, **swapon(8)**, **swapoff(8)**, **mount(8)**, **fdisk(8)**

Práctica: Agregar y habilitar espacio swap (intercambio)

En este trabajo de laboratorio, creará una partición swap (intercambio) y la habilitará para su uso.

Recursos:	
Máquinas:	serverX

Resultados:

Su host serverX tendrá 500 MiB de espacio swap (intercambio) ejecutándose en su segundo disco.

Andes de comenzar

- Inicie sesión en serverX.
- Cambie a **root** usando **sudo -i**.

No se creó ninguna partición de intercambio durante la instalación de serverX. Durante el uso pico, el servidor se ha ejecutado fuera de la memoria física. Ha solicitado memoria RAM adicional y está esperando ansiosamente su llegada. Mientras tanto, decide aliviar el problema al habilitar espacio swap (intercambio) en el segundo disco. Para asegurarse de que el espacio swap (intercambio) agregado recientemente esté siempre disponible para su uso, también necesitará configurarlo para que esté habilitado en el arranque.

Una vez que haya completado su trabajo, vuelva a arrancar su máquina serverX y verifique que el espacio swap (intercambio) esté disponible luego del reinicio.

1. Cree una partición de 500 MiB en **/dev/vdb** de tipo **Linux swap** (intercambio de Linux).

- 1.1. Use **fdisk** para modificar el segundo disco.

```
[root@serverX ~]# fdisk /dev/vdb
```

- 1.2. Imprima la tabla de particiones originales, y luego cree una nueva partición que tenga un tamaño de 500 GiB.

```
Command (m for help): p
Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xfd41a9d3

      Device Boot      Start        End      Blocks   Id  System
  /dev/vdb1            2048    2099199     1048576   83  Linux

Command (m for help): n
Partition type:
   p   primary (1 primary, 0 extended, 3 free)
```

```
e extended
Select (default p): p
Partition number (2-4, default 2): 2
First sector (2099200-20971519, default 2099200): Enter
Using default value 2099200
Last sector, +sectors or +size{K,M,G} (2099200-20971519, default
20971519): +500M
Partition 2 of type Linux and of size 500 MiB is set

Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xfd41a9d3

Device Boot Start End Blocks Id System
/dev/vdb1 2048 2099199 1048576 83 Linux
/dev/vdb2 2099200 3123199 512000 83 Linux
```

- 1.3. Establezca la partición creada recientemente al tipo **Linux swap** (intercambio de Linux).

```
Command (m for help): t
Partition number (1,2, default 2): 2
Hex code (type L to list all codes): L

...
1 FAT12 27 Hidden NTFS Win 82 Linux swap / So c1 DRDOS/sec (FAT-
...
Hex code (type L to list all codes): 82
Changed type of partition 'Linux' to 'Linux swap / Solaris'

Command (m for help): p

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xfd41a9d3

Device Boot Start End Blocks Id System
/dev/vdb1 2048 2099199 1048576 83 Linux
/dev/vdb2 2099200 3123199 512000 82 Linux swap / Solaris
```

- 1.4. Guarde los cambios de la tabla de particiones.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource
busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

- 1.5. Ejecute **partprobe** para hacer que el kernel tenga conocimiento del cambio en la tabla de particiones.

```
[root@serverX ~]# partprobe
```

2. Inicialice la partición creada recientemente como espacio swap (intercambio).

```
[root@serverX ~]# mkswap /dev/vdb2
Setting up swapspace version 1, size = 511996 KiB
no label, UUID=74f8f3e1-6af3-4e51-9ab5-c48e52bf4a7b
```

3. Habilite el espacio swap (intercambio) creado recientemente.

- 3.1. La creación y la inicialización del espacio swap (intercambio) no lo habilita aún para su uso como se muestra mediante los comandos **free** y **swapon -s**.

```
[root@serverX ~]# free
              total        used        free      shared  buffers   cached
Mem:       1885252      557852     1327400      17096      1080    246040
-/+ buffers/cache:     310732     1574520
Swap:          0          0          0
```

```
[root@serverX ~]# swapon -s
[root@serverX ~]#
```

- 3.2. Habilite el espacio swap (intercambio) creado recientemente.

```
[root@serverX ~]# swapon /dev/vdb2
```

- 3.3. Verifique que el espacio swap (intercambio) creado recientemente ahora esté disponible.

```
[root@serverX ~]# swapon -s
Filename  Type  Size Used Priority
/dev/vdb2                  partition 511996 0 -1
```

- 3.4. Deshabilite el espacio swap (intercambio).

```
[root@serverX ~]# swapoff /dev/vdb2
```

- 3.5. Verifique que el espacio swap (intercambio) esté deshabilitado.

```
[root@serverX ~]# swapon -s
[root@serverX ~]#
```

4. Configure el nuevo espacio swap (intercambio) de modo que esté habilitado en el arranque.

- 4.1. Determine el UUID de la nueva partición de intercambio en el segundo disco.

```
[root@serverX ~]# blkid /dev/vdb2  
/dev/vdb2: UUID="74f8f3e1-6af3-4e51-9ab5-c48e52bf4a7b" TYPE="swap"
```

- 4.2. Agregue una entrada a **/etc/fstab**.

```
UUID=74f8f3e1-6af3-4e51-9ab5-c48e52bf4a7b swap swap defaults 0 0
```

- 4.3. Evalúe la habilitación del espacio swap (intercambio) usando la nueva entrada recién agregada a **/etc/fstab**.

```
[root@serverX ~]# swapon -a
```

- 4.4. Verifique que el nuevo espacio swap (intercambio) fue habilitado.

```
[root@serverX ~]# swapon -s  
Filename           Type      Size   Used   Priority  
/dev/vdb2          partition 511996  0       -1
```

5. Reinicie serverX. Luego de reiniciar el servidor, inicie sesión y verifique que el espacio swap (intercambio) esté habilitado.

```
[student@serverX ~]# swapon -s  
Filename           Type      Size   Used   Priority  
/dev/vdb2          partition 511996  0       -1
```

Trabajo de laboratorio: Adición de discos, particiones y sistemas de archivos a un sistema Linux

En este trabajo de laboratorio, creará una partición GPT en un disco recientemente asignado, formateará la partición con un sistema de archivos XFS y configurará el sistema de archivos para un montaje persistente. También creará dos particiones swap (intercambio) de 512 MiB. Configurará una de las particiones swap (intercambio) para que tenga una prioridad 1.

Recursos:	
Máquinas:	serverX

Resultados:

- Sistema de archivos XFS de 2 GiB en una partición GPT, en el segundo disco. El sistema de archivos se monta persistentemente en **/backup**.
- Una partición swap (intercambio) de 512 MiB habilitada en el segundo disco con prioridad predeterminada.
- Otra partición swap (intercambio) de 512 MiB habilitada en el segundo disco con una prioridad 1.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en serverX.
- Cambie a **root** usando **sudo -i**.

Se le ha solicitado que copie datos importantes del disco principal en serverX a un disco separado para mantener la seguridad. Se le ha asignado un segundo disco en serverX para este propósito. Ha decidido crear una partición de GPT de 2 GiB en el segundo disco y formatearlo con el sistema de archivos XFS. Para asegurarse de que este nuevo sistema de archivos esté siempre disponible, lo configurará para montarlo de forma persistente.

Para compensar la escasez de memoria física en serverX, se recomienda crear y habilitar algo de espacio swap (intercambio) para usar. Creará dos particiones swap (intercambio) de 512 MiB en el segundo disco y establecerá la prioridad de una de las particiones en 1, de modo que sea la preferida con respecto a la otra partición swap (intercambio).

Reinic peace su máquina serverX. Verifique que el sistema de archivos XFS recientemente creado se monte de forma persistente en **/backup**. Asimismo, confirme que se activen dos espacios swap (intercambio) en el arranque y uno de los espacios swap (intercambio) tenga la prioridad -1 predeterminada y la otra tenga la prioridad 1.

Cuando haya finalizado su trabajo, ejecute **lab disk grade** en su máquina serverX para verificar su trabajo.

1. Cree una partición GPT de 2 GiB en **/dev/vdb** de tipo **Linux**.

2. Cree dos particiones de 512 MiB en **/dev/vdb** del tipo **Linux swap** (intercambio de Linux).
3. Formatee las particiones creadas recientemente. Formatee la partición de 2 GiB con un sistema de archivos XFS. Inicialice las dos particiones de 512 MiB como espacio swap (intercambio).
4. Configure el sistema de archivos recientemente creado para montarlo de forma persistente en **/backup**.
5. Configure los espacios swap (intercambio) recientemente creados para que estén habilitados en el arranque. Establezca uno de los espacios swap (intercambio) para que se prefiera sobre el otro.
6. Reinicie serverX. Luego de reiniciar el servidor, inicie sesión y verifique que **/dev/vdb1** se monte en **/backup**. También verifique que dos particiones swap (intercambio) de 512 MiB estén habilitadas y que una tenga la prioridad predeterminada y la otra tenga una prioridad 1.
7. Cuando haya completado su trabajo, ejecute **lab disk grade** en su máquina serverX para verificar su trabajo.

Solución

En este trabajo de laboratorio, creará una partición GPT en un disco recientemente asignado, formateará la partición con un sistema de archivos XFS y configurará el sistema de archivos para un montaje persistente. También creará dos particiones swap (intercambio) de 512 MiB. Configurará una de las particiones swap (intercambio) para que tenga una prioridad 1.

Recursos:	
Máquinas:	serverX

Resultados:

- Sistema de archivos XFS de 2 GiB en una partición GPT, en el segundo disco. El sistema de archivos se monta persistentemente en **/backup**.
- Una partición swap (intercambio) de 512 MiB habilitada en el segundo disco con prioridad predeterminada.
- Otra partición swap (intercambio) de 512 MiB habilitada en el segundo disco con una prioridad 1.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en serverX.
- Cambie a **root** usando **sudo -i**.

Se le ha solicitado que copie datos importantes del disco principal en serverX a un disco separado para mantener la seguridad. Se le ha asignado un segundo disco en serverX para este propósito. Ha decidido crear una partición de GPT de 2 GiB en el segundo disco y formatearlo con el sistema de archivos XFS. Para asegurarse de que este nuevo sistema de archivos esté siempre disponible, lo configurará para montarlo de forma persistente.

Para compensar la escasez de memoria física en serverX, se recomienda crear y habilitar algo de espacio swap (intercambio) para usar. Creará dos particiones swap (intercambio) de 512 MiB en el segundo disco y establecerá la prioridad de una de las particiones en 1, de modo que sea la preferida con respecto a la otra partición swap (intercambio).

Reinicie su máquina serverX. Verifique que el sistema de archivos XFS recientemente creado se monte de forma persistente en **/backup**. Asimismo, confirme que se activen dos espacios swap (intercambio) en el arranque y uno de los espacios swap (intercambio) tenga la prioridad -1 predeterminada y la otra tenga la prioridad 1.

Cuando haya finalizado su trabajo, ejecute **lsblk** en su máquina serverX para verificar su trabajo.

1. Cree una partición GPT de 2 GiB en **/dev/vdb** de tipo **Linux**.

- 1.1. Use **gdisk** para modificar el segundo disco.

```
[root@serverX ~]# gdisk /dev/vdb
```

- 1.2. Agregue una partición swap (intercambio) que tenga un tamaño de 2 GiB.

```
Command (? for help): n
Partition number (1-128, default 1): 1
First sector (34-20971486, default = 2048) or {+-}size{KMGTP}: Enter
Last sector (2048-20971486, default = 20971486) or {+-}size{KMGTP}: +2G
Current type is 'Linux filesystem'
```

1.3. Establezca la nueva partición al tipo **Linux**.

```
Hex code or GUID (L to show codes, Enter = 8300): Enter
Changed type of partition to 'Linux filesystem'
```

2. Cree dos particiones de 512 MiB en **/dev/vdb** del tipo **Linux swap** (intercambio de Linux).

2.1. Agregue una partición que sea de 512 MiB.

```
Command (? for help): n
Partition number (2-128, default 2): 2
First sector (34-20971486, default = 4196352) or {+-}size{KMGTP}: Enter
Last sector (4196352-20971486, default = 20971486) or {+-}size{KMGTP}: +512M
Current type is 'Linux filesystem'
```

2.2. Establezca la partición al tipo **Linux swap** (intercambio de Linux).

```
Hex code or GUID (L to show codes, Enter = 8300): L
...
8200 Linux swap          8300 Linux filesystem      8301 Linux reserved
...
Hex code or GUID (L to show codes, Enter = 8300): 8200
Changed type of partition to 'Linux swap'
```

2.3. Agregue otra partición que sea de 512 MiB, y configúrela con el tipo **Linux swap** (intercambio de Linux).

```
Command (? for help): n
Partition number (3-128, default 3): 3
First sector (34-20971486, default = 5244928) or {+-}size{KMGTP}: Enter
Last sector (5244928-20971486, default = 20971486) or {+-}size{KMGTP}: +512M
Current type is 'Linux filesystem'
Hex code or GUID (L to show codes, Enter = 8300): 8200
Changed type of partition to 'Linux swap'
```

2.4. Verifique las particiones.

```
Command (? for help): p
Disk /dev/vdb: 20971520 sectors, 10.0 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): 9918D507-7344-406A-9902-D2503FA028EF
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 20971486
Partitions will be aligned on 2048-sector boundaries
Total free space is 14679997 sectors (7.0 GiB)
```

Number	Start (sector)	End (sector)	Size	Code	Name
1	2048	4196351	2.0 GiB	8300	Linux filesystem
2	4196352	5244927	512.0 MiB	8200	Linux swap
3	5244928	6293503	512.0 MiB	8200	Linux swap

2.5. Guarde los cambios en la tabla de particiones.

```
Command (? for help): w
Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!

Do you want to proceed? (Y/N): y
OK; writing new GUID partition table (GPT) to /dev/vdb.
The operation has completed successfully.
```

2.6. Ejecute **partprobe** para hacer que el kernel tenga conocimiento del cambio en la tabla de particiones.

```
[root@serverX ~]# partprobe
```

3. Formatee las particiones creadas recientemente. Formatee la partición de 2 GiB con un sistema de archivos XFS. Inicialice las dos particiones de 512 MiB como espacio swap (intercambio).

3.1. Formatee la partición recientemente creada con el sistema de archivos XFS.

```
[root@serverX ~]# mkfs -t xfs /dev/vdb1
meta-data=/dev/vdb1              isize=256    agcount=4, agsize=131072 blks
                                =          sectsz=512   attr=2, projid32bit=1
                                =          crc=0
data     =              bsize=4096   blocks=524288, imaxpct=25
        =          sunit=0      swidth=0 blks
naming   =version 2             bsize=4096   ascii-ci=0 ftype=0
log      =internal log          bsize=4096   blocks=2560, version=2
        =          sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                  extsz=4096   blocks=0, rtextents=0
```

3.2. Inicialice las dos particiones como espacio swap (intercambio).

```
[root@serverX ~]# mkswap /dev/vdb2
Setting up swapspace version 1, size = 524284 KiB
no label, UUID=d00554b7-dfac-4034-bdd1-37b896023f2c
```

```
[root@serverX ~]# mkswap /dev/vdb3
Setting up swapspace version 1, size = 524284 KiB
no label, UUID=af30ccb0-3866-466a-825a-58889a49ef33
```

4. Configure el sistema de archivos recientemente creado para montarlo de forma persistente en **/backup**.

4.1. Cree el punto de montaje del directorio **/backup**.

Capítulo 8. Creación y montaje de sistemas de archivos

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

- 4.2. Determine el UUID de la primera partición en el segundo disco.

```
[root@serverX ~]# blkid /dev/vdb1
/dev/vdb1: UUID="748ca35a-1668-4a2f-bfba-51ebe550f6f0" TYPE="xfs"
          PARTLABEL="Linux filesystem" PARTUUID="83b18afb-9c12-48bf-a620-7f8a612df5a8"
```

- 4.3. Agregue una entrada a **/etc/fstab**.

```
UUID=748ca35a-1668-4a2f-bfba-51ebe550f6f0 /backup xfs defaults 0 2
```

5. Configure los espacios swap (intercambio) recientemente creados para que estén habilitados en el arranque. Establezca uno de los espacios swap (intercambio) para que se prefiera sobre el otro.

- 5.1. Agregue entradas a **/etc/fstab** usando los UUID generados en los pasos de **mkswap** anteriores. Establezca la prioridad en uno de los espacios swap (intercambio) en 1.

```
UUID=d00554b7-dfac-4034-bdd1-37b896023f2c swap swap defaults 0 0
UUID=af30cbb0-3866-466a-825a-58889a49ef33 swap swap pri=1 0 0
```

6. Reinicie serverX. Luego de reiniciar el servidor, inicie sesión y verifique que **/dev/vdb1** se monte en **/backup**. También verifique que dos particiones swap (intercambio) de 512 MiB estén habilitadas y que una tenga la prioridad predeterminada y la otra tenga una prioridad 1.

```
[student@serverX ~]$ mount | grep ^
/dev/vda1 on / type xfs (rw,relatime,seclabel,attr2,inode64,noquota)
/dev/vdb1 on /backup type xfs (rw,relatime,seclabel,attr2,inode64,noquota)
```

```
[student@serverX ~]$ free
              total        used        free      shared  buffers   cached
Mem:       1885252      563528     1321724        17096       696    245224
 -/+ buffers/cache:     317608     1567644
Swap:        1048568           0     1048568
```

```
[student@serverX ~]$ swapon -s
Filename            Type      Size  Used  Priority
/dev/vdb2          partition 524284  0    -1
/dev/vdb3          partition 524284  0     1
```

7. Cuando haya completado su trabajo, ejecute **lab disk grade** en su máquina serverX para verificar su trabajo.

```
[student@serverX ~]$ lab disk grade
```

Resumen

Montaje y desmontaje de sistemas de archivos

El acceso al contenido de sistemas de archivos en dispositivos de almacenamiento interno y externo es importante.

Adición de particiones, sistemas de archivos y montajes persistentes

- **fdisk** se puede usar para agregar, modificar y eliminar particiones en discos con esquemas de partición MBR.
- **gdisk** se puede usar para agregar, modificar y eliminar particiones en discos con esquemas de partición GPT.
- Los sistemas de archivos se crean en particiones de discos usando **mkfs**.
- Para que los montajes de sistemas de archivos sean persistentes, se deben agregar a **/etc/fstab**.

Administración de espacio swap (intercambio)

- Cree y active un espacio swap (intercambio).



CAPÍTULO 9

ADMINISTRACIÓN DE SERVICIOS Y RESOLUCIÓN DE PROBLEMAS DE ARRANQUE

Descripción general	
Meta	Controlar y supervisar los daemons del sistema, y resolver problemas del proceso de arranque de Red Hat Enterprise Linux.
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 daemons del sistema y los servicios de red con <code>systemctl</code>.• Describir el proceso de arranque de Red Hat Enterprise Linux.• Reparar problemas de arranque comunes.• Reparar problemas de archivos en el arranque.• Reparar problemas del cargador de arranque.
Secciones	<ul style="list-style-type: none">• Identificación de procesos del sistema comenzados en forma automática (y práctica)• Control de servicios del sistema (y práctica)• El proceso de arranque de Red Hat Enterprise Linux (y práctica)• Reparación de problemas de arranque comunes (y práctica)• Reparación de problemas de sistemas de archivos en el arranque (y práctica)

Descripción general	
	<ul style="list-style-type: none">• Reparación de problemas del cargador de arranque (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">• Control de servicios y daemons

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 *init 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
```

```
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...y
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 ~]$ sudo systemctl list-units --type=service
```

2. Enumere todas las unidades de socket, activas e inactivas, en el sistema.

```
[student@serverX ~]$ sudo 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 ~]$ sudo systemctl status chrony
```

- 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 ~]$ sudo systemctl is-enabled sshd
```

- 4.2. Determine si el servicio **sshd** está activo sin mostrar toda la información de estado.

```
[student@serverX ~]$ sudo systemctl is-active sshd
```

- 4.3. Muestre el estado del servicio **sshd**.

```
[student@serverX ~]$ sudo systemctl status sshd
```

5. Enumere los estados habilitados y deshabilitados de todas las unidades de servicio.

```
[student@serverX ~]$ sudo 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 *enmascarar*. 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 evitara 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**.

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.	systemctl status <i>UNIT</i>
Detener un servicio en un sistema en funcionamiento.	systemctl stop <i>UNIT</i>
Iniciar un servicio en un sistema en funcionamiento.	systemctl start <i>UNIT</i>
Reiniciar un servicio en un sistema en funcionamiento.	systemctl restart <i>UNIT</i>
Volver a cargar el archivo de configuración de un servicio en ejecución.	systemctl reload <i>UNIT</i>
Deshabilitar completamente el inicio (tanto manual como durante el proceso de arranque) de un servicio.	systemctl mask <i>UNIT</i>
Poner un servicio enmascarado a disposición.	systemctl unmask <i>UNIT</i>
Configurar un servicio para que se inicie durante el proceso de arranque.	systemctl enable <i>UNIT</i>
Deshabilitar el inicio de un servicio durante el proceso de arranque.	systemctl disable <i>UNIT</i>
Enumerar unidades necesarias y deseadas por la unidad especificada.	systemctl list-dependencies <i>UNIT</i>



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 **chrony** y ya no se ejecuta en el sistema.

Andes de comenzar

Restablezca su sistema serverX.

1. Observe los resultados de `systemctl restart` y los comandos `systemctl reload`.

- 1.1. Muestre el estado del servicio **sshd**. Tenga en cuenta la ID de proceso de demonio.

```
[student@serverX ~]$ sudo systemctl status sshd
```

- 1.2. Reinicie el servicio **sshd** y visualice el estado. Cambió la ID de proceso del demonio.

```
[student@serverX ~]$ sudo systemctl restart sshd  
[student@serverX ~]$ sudo systemctl status sshd
```

- 1.3. 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 ~]$ sudo systemctl status sshd
```

2. Verifique que el servicio **chrony** se esté ejecutando.

```
[student@serverX ~]$ sudo systemctl status chronyd
```

3. Detenga el servicio **sshd** y visualice el estado.

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

4. Determine si el servicio **chrony** está habilitado para comenzar en el arranque del sistema.

```
[student@serverX ~]$ sudo systemctl is-enabled chronyd
```

5. Reinicie el sistema y, a continuación, visualice el estado del servicio **chrony**.

```
[student@serverX ~]$ sudo systemctl status chronyd
```

Capítulo 9. Administración de servicios y resolución de problemas de arranque

6. Inhabilite el servicio **chrony** 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 ~]$ sudo systemctl status chronyd
```

7. Reinicie el sistema y, a continuación, visualice el estado del servicio **chrony**.

```
[student@serverX ~]$ sudo systemctl status chronyd
```

El proceso de arranque de Red Hat Enterprise Linux

Objetivos

Luego de completar esta sección, los estudiantes deberían poder describir e influenciar el proceso de arranque de Red Hat Enterprise Linux.

El proceso de arranque de Red Hat Enterprise Linux

7

Los sistemas de computación modernos son combinaciones complejas de hardware y software. Desde un estado de apagado no definido hasta un sistema de ejecución con un prompt de inicio de sesión (gráfico), se requiere una gran cantidad de piezas de hardware y software que funcionen en conjunto. La siguiente lista proporciona una descripción general de alto nivel de las tareas de arranque de un sistema físico **x86_64** a Red Hat Enterprise Linux 7. La lista de máquinas virtuales **x86_64** es prácticamente la misma, pero algunos de los pasos específicos del hardware son manejados por el hipervisor en el software.

1. La máquina se enciende. El firmware del sistema (UEFI moderno o BIOS más antiguo) ejecuta una *prueba automática de encendido* (*Power On Self Test, POST*), y comienza a inicializar parte del hardware.

Configurado mediante lo siguiente: Las pantallas de configuración de BIOS/UEFI del sistema, a las cuales se llega típicamente al presionar una determinada combinación de teclas (p. ej., **F2**) al principio del proceso de arranque.

2. El firmware del sistema busca un dispositivo de arranque, ya sea configurado en el firmware de arranque UEFI o al buscar un *registro de arranque maestro* (*Master Boot Record, MBR*) en todos los discos, en el orden configurado en el BIOS.

Configurado mediante lo siguiente: Las pantallas de configuración de BIOS/UEFI del sistema, a las cuales se llega típicamente al presionar una determinada combinación de teclas (p. ej., **F2**) al principio del proceso de arranque.

3. El firmware del sistema lee un *cargador de arranque* desde el disco, luego pasa el control del sistema al cargador de arranque. En un sistema Red Hat Enterprise Linux 7, este será típicamente **grub2**.

Configurado mediante lo siguiente: **grub2-install**

4. El cargador de arranque carga su configuración desde el disco, y presenta al usuario un menú de posibles configuraciones para arrancar.

Configurado mediante lo siguiente: **/etc/grub.d/**, **/etc/default/grub** y (no manualmente) **/boot/grub2/grub.cfg**.

5. Luego de que el usuario haya hecho una elección (o se haya agotado el tiempo de espera automático), el cargador de arranque carga el kernel y el *initramfs configurados* desde el disco y los coloca en la memoria. Un **initramfs** es un archivo **gzip-ed cpio** que contiene módulos del kernel para todo el hardware necesario en el arranque,

scripts de inicio y más. En Red Hat Enterprise Linux 7, **initramfs** contiene un sistema totalmente utilizable por sí solo.

Configurado mediante lo siguiente: **/etc/dracut.conf**

6. El cargador de arranque pasa el control del sistema al kernel, y detalla todas las opciones especificadas en la línea de comandos del kernel en el cargador de arranque, y la ubicación del **initramfs** en la memoria.

Configurado mediante lo siguiente: **/etc/grub.d/**, **/etc/default/grub** y (no manualmente) **/boot/grub2/grub.cfg**.

7. El kernel inicializa todo el hardware para el cual puede encontrar un controlador en el **initramfs**, y luego ejecuta **/sbin/init** desde **initramfs** como **PID 1**. En Red Hat Enterprise Linux 7, **initramfs** contiene una copia de trabajo de **systemd** como **/sbin/init**, al igual que un daemon de **udev**.

Configurado mediante lo siguiente: parámetro de línea de comandos **init=**.

8. La instancia **systemd** desde **initramfs** ejecuta todas las unidades para el objetivo **initrd.target**. Esto incluye el montaje del sistema de archivos root real en **/sysroot**.

Configurado mediante lo siguiente: **/etc/fstab**

9. El sistema de archivos root del kernel se cambia (articula) desde el sistema de archivos root de **initramfs** al sistema de archivos root del sistema que se montó anteriormente en **/sysroot**. Luego, vuelve a ejecutarse **systemd** usando la copia de **systemd** instalado en el sistema.

10. **systemd** busca un objetivo predeterminado, ya sea especificado desde la línea de comandos del kernel o configurado en el sistema, luego inicia (y detiene) unidades para cumplir con la configuración para ese objetivo, y resuelve dependencias entre unidades automáticamente. En su esencia, un objetivo **systemd** es un conjunto de unidades que debe activarse para alcanzar un estado de sistema deseado. Estos objetivos incluirán típicamente al menos una pantalla de inicio de sesión basado en texto o inicio de sesión gráfico que se generará.

Configurado mediante lo siguiente: **/etc/systemd/system/default.target**, **/etc/systemd/system/**

Arrancar, reiniciar y apagar

Para apagar o reiniciar un sistema en ejecución desde la línea de comandos, los administradores pueden usar el comando **systemctl**.

systemctl poweroff detendrá todos los servicios en ejecución, desmontará todos los sistemas de archivos (o volverá a montarlos como solo lectura cuando no se puedan desmontar) y luego apagará el sistema.

systemctl reboot detendrá todos los servicios en ejecución, desmontará todos los sistemas de archivos y luego reiniciará el sistema.

Para facilitar la compatibilidad con sistemas anteriores, los comandos **poweroff** y **reboot** aún existen, pero en Red Hat Enterprise Linux 7 son enlaces simbólicos a la herramienta **systemctl**.



Importante

systemctl halt y **halt** también están disponibles para detener el sistema, pero a diferencia de sus equivalentes de **poweroff**, estos comandos *no* apagan el sistema, sino que lo llevan hasta un punto donde es seguro apagarlo manualmente.

Selección de un objetivo de systemd

Un objetivo de **systemd** es un conjunto de unidades de **systemd** que deben iniciarse para alcanzar un estado deseado. Los más importantes de estos objetivos están detallados en la siguiente tabla.

Objetivo	Propósito
graphical.target	El sistema admite varios usuarios, e inicios de sesión gráficos y basados en texto.
multi-user.target	El sistema admite varios usuarios y solo inicios de sesión basados en texto.
rescue.target	Prompt sulogin , inicialización del sistema básico finalizada.
emergency.target	Prompt sulogin , cambio de initramfs completo y root del sistema montado en / solo lectura.

Es posible que un objetivo sea parte de otro objetivo; por ejemplo, **graphical.target** incluye **multi-user.target**, que a su vez depende de **basic.target** y otros. Estas dependencias se pueden visualizar desde la línea de comandos con el siguiente comando:

```
[root@serverX ~]# systemctl list-dependencies graphical.target | grep target
```

Una descripción general de todos los objetivos disponibles se puede visualizar con:

```
[root@serverX ~]# systemctl list-units --type=target --all
```

Una descripción general de todos los objetivos instalados en el disco se puede visualizar con:

```
[root@serverX ~]# systemctl list-unit-files --type=target --all
```

Selección de un objetivo en el tiempo de ejecución

En un sistema en ejecución, los administradores pueden elegir cambiar a un objetivo diferente usando el comando **systemctl isolate**; por ejemplo:

```
[root@serverX ~]# systemctl isolate multi-user.target
```

Aislar un objetivo detendrá todos los servicios no requeridos por ese objetivo (y sus dependencias), e iniciará todos los servicios requeridos que aún no se hayan iniciado.



nota

No todos los objetivos se pueden aislar. Solo los objetivos que tienen establecido **AllowIsolate=yes** en sus archivos de unidad se pueden aislar; por ejemplo, el objetivo **graphical.target** se puede aislar, pero el objetivo **cryptsetup.target** no.

Configuración de un objetivo predeterminado

Cuando el sistema se inicia, y el control se pasa a **systemd** desde **initramfs**, **systemd** intentará activar el objetivo **default.target**. Normalmente, el objetivo **default.target** será un enlace simbólico (en **/etc/systemd/system/**) a **graphical.target** o **multi-user.target**.

En lugar de editar este enlace simbólico manualmente, la herramienta **systemctl** viene con dos comandos para administrar este enlace: **get-default** y **set-default**.

```
[root@serverX ~]# systemctl get-default
multi-user.target
[root@serverX ~]# systemctl set-default graphical.target
rm '/etc/systemd/system/default.target'
ln -s '/usr/lib/systemd/system/graphical.target' '/etc/systemd/system/default.target'
[root@serverX ~]# systemctl get-default
graphical.target
```

Selección de un objetivo diferente en el momento del arranque

Para seleccionar un objetivo diferente al momento del arranque, se puede agregar una opción especial a la línea de comandos del kernel desde el cargador de arranque: **systemd.unit=**.

Por ejemplo, para arrancar el sistema en una shell de rescate donde se pueden hacer cambios de configuración (casi) sin ningún servicio en ejecución, se puede agregar lo siguiente desde el menú del cargador de arranque interactivo antes del inicio:

```
systemd.unit=rescue.target
```

Este cambio de configuración solo afectará a un único arranque, lo que hace que sea una herramienta útil para la solución de problemas en el proceso de arranque.

Para usar este método de selección de un objetivo diferente, use el siguiente procedimiento para sistemas Red Hat Enterprise Linux 7:

1. (Re)inicie el sistema.
2. Interrumpa la cuenta regresiva del menú del cargador de arranque presionando cualquier tecla.
3. Mueva el cursor hasta la entrada que debe iniciarse.
4. Presione **e** para editar la entrada actual.
5. Mueva el cursor hasta la línea que comienza con **linux16**. Esta es la línea de comandos del kernel.

6. Agregue **systemd.unit=desired.target**.
7. Presione **Ctrl+x** para realizar el arranque con estos cambios.



Referencias

Páginas del manual: **bootup(7)**, **dracut.bootup(7)**, **systemd.target(5)**, **systemd.special(7)**, **sulogin(8)** y **systemctl(1)**.

info grub2 (*Manual GNU GRUB*)

Práctica: Selección de un objetivo de arranque

En este trabajo de laboratorio, configurará su sistema **serverX** para arrancar en diferentes objetivos.

Recursos:	
Máquinas:	serverX

Resultados:

Un sistema arrancado en diferentes destinos.

Antes de comenzar

- Restablezca su sistema **serverX**.

- En su sistema **serverX**, cambie al objetivo **multi-user** manualmente sin reiniciar.

1.1. [student@serverX ~]\$ **sudo systemctl isolate multi-user.target**

- Inicie sesión en una consola basada en texto como **root**.

- Configure su **serverX** para que arranque automáticamente en el objetivo **multi-user** después de un nuevo arranque; luego reinicie su sistema **serverX** para verificar.

3.1. [root@serverX ~]# **systemctl set-default multi-user.target**
rm '/etc/systemd/system/default.target'
ln -s '/usr/lib/systemd/system/multi-user.target' '/etc/systemd/system/default.target'

3.2. [root@serverX ~]# **systemctl reboot**

- Reinic peace su sistema **serverX**, luego, desde el menú del cargador de arranque, arranque en el objetivo **rescue**.

- 4.1. Reinicie su máquina **serverX**.

[root@serverX ~]# **systemctl reboot**

- 4.2. Presione cualquier tecla para interrumpir el cargador de arranque cuando aparezca el menú.

- 4.3. Mueva la selección a la entrada predeterminada (la primera) usando las teclas de dirección.

- 4.4. Presione **e** para editar la entrada actual.

- 4.5. Mueva el cursor hasta la línea que comienza con **linux16**.

-
- 4.6. Mueva el cursor hasta el final de la línea (usando la tecla **End** (Fin)), y agregue el siguiente texto:

```
systemd.unit=rescue.target
```

- 4.7. Presione **Ctrl+x** para realizar el arranque con la configuración modificada.
- 4.8. Cuando se le solicite la contraseña **root**, ingrese **redhat**.
5. Configure el objetivo **systemd** predeterminado nuevamente al objetivo gráfico.

```
[root@serverX ~]# systemctl set-default graphical.target
```

6. Presione **Ctrl+d** para continuar arrancando en el destino predeterminado (nuevo).

Reparación de problemas de arranque comunes

Objetivos

Luego de completar esta sección, los estudiantes deberían poder reparar problemas de arranque comunes.

Recuperación de la contraseña root

Una tarea que todos los administradores de sistemas deben poder realizar es recuperar una contraseña **root** perdida. Si el administrador aún tiene la sesión iniciada, ya sea como usuario sin privilegios, pero con acceso **sudo** completo, o como **root**, esta tarea es sencilla. Cuando el administrador no ha iniciado sesión, esta tarea es un poco más complicada.

Existen varios métodos para establecer una nueva contraseña **root**. Un administrador de sistemas podría, por ejemplo, arrancar el sistema usando un CD Live, montar el sistema de archivos root desde allí y editar **/etc/shadow**. En esta sección, exploraremos un método que no requiere el uso de medios externos.



nota

En Red Hat Enterprise Linux 6 y versiones anteriores, un administrador podía arrancar el sistema en *nivel de ejecución 1*, y se le presentaba un prompt de root. Los análogos más cercanos al nivel de ejecución 1 en una máquina Red Hat Enterprise Linux 7 son los objetivos **rescue.target** y **emergency.target**, ambos requieren la contraseña **root** para iniciar sesión.

En Red Hat Enterprise Linux 7, es posible tener scripts que se ejecuten desde la pausa de **initramfs** en ciertos puntos, proporcionar una **root** shell y luego continuar cuando esa shell se cierre. Si bien esto se realiza principalmente para depuraciones, también se puede usar para recuperar una contraseña de root perdida:

1. Reinicie el sistema.
2. Interrumpa la cuenta regresiva del cargador de arranque presionando cualquier tecla.
3. Mueva el cursor a la entrada que debe arrancarse.
4. Presione **e** para editar la entrada seleccionada.
5. Mueva el cursor hasta la línea de comandos del kernel (la línea que empieza con **linux16**).
6. Agregue **rd.break** (esto hará que se produzca un quiebre antes de que el control se entregue de **initramfs** al sistema real).



nota

La solicitud de **initramfs** se mostrará en todas las consolas que se especifiquen *últimas* en la línea de comandos del kernel.

- Presione **Ctrl+x** para realizar el arranque con los cambios.



nota

Es posible que las imágenes creadas previamente coloquen múltiples argumentos de consola en el kernel para respaldar una amplia variedad de situaciones de implementación. La advertencia con rd.break es que mientras muchos de los mensajes del kernel se enviarán a todas las consolas, el prompt usará en última instancia la última consola. Si no recibe el prompt, se recomienda que vuelva a ordenar temporalmente los argumentos de la consola=.

En este punto, se presentará una **root** shell, con el sistema de archivos root para el sistema real montado para solo lectura en **/sysroot**.



Importante

SELinux aún no está habilitado en este punto, de modo que cualquier archivo nuevo que se cree no tendrá un contexto de SELinux asignado. Tenga en cuenta que algunas herramientas (como **passwd**) primero crean un archivo nuevo, y luego lo trasladan al lugar del archivo que intentan editar; y se crea así de manera efectiva un nuevo archivo sin un contexto SELinux.

Para recuperar la contraseña **root** desde este punto, realice el siguiente procedimiento:

- Vuelva a montar **/sysroot** como lectura-escritura.

```
switch_root:/# mount -o remount,rw /sysroot
```

- Cambie a jail **chroot**, donde **/sysroot** se trata como la root de un árbol de sistemas de archivos.

```
switch_root:/# chroot /sysroot
```

- Establezca una nueva contraseña root:

```
sh-4.2# passwd root
```

- Asegúrese de que todos los archivos no etiquetados (incluido **/etc/shadow** en este punto) obtengan una nueva etiqueta durante el arranque.

```
sh-4.2# touch /.autorelabel
```

5. Ingrese **exit** dos veces. El primero saldrá del jail de **chroot** y el segundo saldrá de la shell de depuración de **initramfs**.

En este punto, el sistema continuará con el arranque, realizará un nuevo etiquetado de SELinux completo, y luego realizará el arranque nuevamente.

Uso de journalctl

Puede ser útil mirar los registros de arranques anteriores (que fallaron). Si el registro de **journald** se ha hecho persistente, esto se puede hacer con la herramienta **journalctl**.

Primero asegúrese de tener habilitado el registro de **journald** persistente:

```
[root@serverX ~]# mkdir -p -m2755 /var/log/journal  
[root@serverX ~]# chown :systemd-journal /var/log/journal  
[root@serverX ~]# killall -USR1 systemd-journal
```

Para inspeccionar los archivos de registro para un arranque anterior, use la opción **-b** para **journalctl**. Sin argumentos, la opción **-b** filtrará el resultado solo con mensajes que pertenecen a este arranque, pero con un número negativo como argumento, filtrará arranques anteriores. Por ejemplo:

```
[root@serverX ~]# journalctl -b-1 -p err
```

Este comando mostrará todos los mensajes calificados como error o peor del arranque anterior.

Diagnosticar y reparar problemas de arranque de systemd

Si hay problemas durante el inicio de servicios, existe un par de herramientas disponibles para los administradores de sistemas que pueden ayudar con la depuración o la resolución de problemas:

Shell de depuración temprana

Al ejecutar **systemctl enable debug-shell.service**, una **root** shell se iniciará en **TTY9 (Ctrl+Alt+F9)** al principio de la secuencia de arranque. Este shell inicia sesión automáticamente como root, de modo que un administrador puede usar alguna de las otras herramientas de depuración mientras el sistema aún está arrancando.

Advertencia

No olvide deshabilitar el servicio **debug-shell.service** cuando haya finalizado la depuración, dado que deja una shell root no autenticada abierta a cualquier usuario con acceso a la consola local.

Objetivos de emergencia y recuperación

Al agregar **systemd.unit=rescue.target** o **systemd.unit=emergency.target** delante de la línea de comandos del kernel desde el cargador de arranque, el sistema iniciará una shell de emergencia o recuperación especial en lugar de iniciarse normalmente. Estas dos shells requieren la contraseña **root**. El objetivo de **emergencia** mantiene el sistema de archivos root montado con solo lectura; mientras que **rescue.target** espera que **sysinit.target** se complete primero para que una mayor parte del sistema se inicie (p. ej., registros, sistemas de archivos, etc.).

Estas shells se pueden usar para arreglar problemas que impiden que el sistema arranque normalmente; por ejemplo, un bucle de dependencia entre servicios o una entrada incorrecta en **/etc/fstab**. Cuando se sale de estas shells, continúa el proceso de arranque regular.

Trabajos atascados

Durante el inicio, **systemd** inicia varios trabajos. Si alguno de estos trabajos no se puede completar, impedirán que otros trabajos se ejecuten. Para inspeccionar la lista de trabajos actual, un administrador puede usar el comando **systemctl list-jobs**. Todos los trabajos detallados como **en ejecución** deben completarse para que los trabajos detallados como **en espera** puedan continuar.



Referencias

Páginas del manual: **dracut cmdline(7)**, **systemd-journald(8)**, **journalctl(1)**, **sushell(8)** y **systemctl(1)**

/usr/lib/systemd/system/debug-shell.service

Práctica: restablecimiento de una contraseña root perdida

En este trabajo de laboratorio, recuperará una contraseña root perdida.

Recursos:		
Máquinas:	serverX	

Resultados:

Contraseña root recuperada.

Antes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo:

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

El script **lab rootpw setup** acaba de restablecer su contraseña root a una secuencia de comandos aleatoria y reinició el sistema. Sin usar **sudo**, entre en su propio sistema y restablezca la contraseña **root** nuevamente a **redhat**.

- Vuelva a arrancar su sistema e interrumpa la cuenta regresiva en el menú del cargador de arranque.
 - Envíe **Ctrl+Alt+Del** a su sistema usando la entrada del menú o el botón relevantes.
 - Cuando el menú del cargador de arranque aparece, presione cualquier tecla para interrumpir la cuenta regresiva.
- Edite la entrada del cargador de arranque predeterminada (en la memoria) para anular el proceso de arranque luego de que todos los sistemas de archivos hayan sido montados, pero antes de que el control se entregue a **systemd**, luego arranque.
 - Use las teclas de dirección para destacar la entrada del cargador de arranque predeterminada.
 - Presione **e** para editar la entrada actual.
 - Con las teclas de dirección, navegue hacia la línea que comienza con **linux16**.
 - Presione **End** (Fin) para mover el cursor hasta el final de la línea.
 - Agregue **rd.break** en el final de la línea.
 - Presione **Ctrl+x** para realizar el arranque con la configuración modificada.
- En el prompt **switch_root**, vuelva a montar la lectura-escritura de **systemd** del archivo **/sysroot** y, luego, use **chroot** para ir a un jail **chroot** en **/sysroot**.
 - ```
switch_root:/# mount -o remount,rw /sysroot
```

```
switch_root:/# chroot /sysroot
```

4. Cambie la contraseña **root** nuevamente a **redhat**.

- 4.1. sh-4.2# echo redhat | passwd --stdin root

5. Configure el sistema para que realice automáticamente un etiquetado nuevo de SELinux completo luego del arranque. Esto es necesario dado que la herramienta **passwd** recreó el archivo **/etc/shadow** sin un contexto SELinux.

- 5.1. sh-4.2# touch /.autorelabel

6. Escriba **exit** dos veces para continuar arrancando su sistema de forma normal. El sistema ejecutará un nuevo etiquetado SELinux, luego volverá a arrancar nuevamente por sí solo.

7. Verifique su trabajo al ejecutar el siguiente comando:

```
[student@serverX ~]$ lab rootpw grade
```

# Reparación de problemas del sistema de archivos en el arranque

## Objetivos

Luego de completar esta sección, los estudiantes deberían poder reparar problemas de sistemas de archivos durante el arranque.

Los errores en sistemas de archivos dañados y en **/etc/fstab** pueden impedir que un sistema arranque. En la mayoría de los casos, **systemd** continuará con el arranque luego de un tiempo de espera, o caerá en una shell de reparación de emergencia que requiere la contraseña **root**.

En la siguiente tabla, se detallan algunos errores comunes y sus resultados.

| Problema                                                       | Resultado                                                                                                                                                                                               |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sistema de archivos dañado                                     | <b>systemd</b> intentará un <b>fsck</b> . Si el problema es demasiado grave para un arreglo automático, se le solicitará al usuario que ejecute <b>fsck</b> manualmente desde una shell de emergencia.  |
| Dispositivo no existente/UUID mencionado en <b>/etc/fstab</b>  | <b>systemd</b> esperará un tiempo establecido a que el dispositivo esté disponible. Si el dispositivo no aparece como disponible, el usuario cae en una shell de emergencia luego del tiempo de espera. |
| Punto de montaje no existente en <b>/etc/fstab</b>             | <b>systemd</b> crea el punto de montaje si es posible; de lo contrario, cae en una shell de emergencia.                                                                                                 |
| Opción de montaje incorrecta especificada en <b>/etc/fstab</b> | El usuario cae en una shell de emergencia.                                                                                                                                                              |

En todos los casos, un administrador también puede utilizar el objetivo **emergency.target** para diagnosticar y arreglar el problema, dado que ningún sistema de archivos se montará antes de que se muestre la shell de emergencia.

### nota

Al usar la shell de recuperación automática durante problemas de sistemas de archivos, no olvide emitir un **systemctl daemon-reload** luego de editar **/etc/fstab**. Sin esta recarga, **systemd** continuará usando la versión anterior.

### Referencias

Páginas del manual: **systemd-fsck(8)**, **systemd-fstab-generator(3)**, **systemd.mount(5)**

# Práctica: Reparación de problemas en el arranque

En este trabajo de laboratorio, recuperará el sistema de un error en **/etc/fstab**.

| Recursos: |         |
|-----------|---------|
| Máquinas: | serverX |

## Resultados:

Luego de completar este ejercicio, su máquina debería arrancar nuevamente de forma normal, sin intervención del usuario.

## Andes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo:

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

Usted *tenía* un nuevo administrador en su equipo, pero se decidió que sería mejor para todos si ese administrador buscara otra profesión.

Ahora que el problema de su personal ha sido resuelto, hay un par de problemas restantes. Uno de ellos es una máquina que ha sido “arreglada” por este administrador.

1. Mire bien la consola de su máquina **serverX**. Parece que se atascó antes.

Tómese un minuto para especular sobre una posible causa de este comportamiento, luego vuelva a arrancar la máquina e interrumpa la cuenta regresiva del menú del cargador de arranque. (Si espera el tiempo suficiente, el sistema finalmente iniciará una shell de rescate por sí solo, pero eso puede tardar un tiempo).

- 1.1. Generalmente, enviaría **Ctrl+Alt+Del** a su sistema para que se reinicie. Este problema de arranque particular hace que esa secuencia de teclas reintente la secuencia de arranque nuevamente sin reiniciarse. En este caso, espere a que la tarea termine o use el switch de encendido para forzar un reinicio.
- 1.2. Cuando el menú del cargador de arranque aparezca luego de la prueba automática del BIOS, presione cualquier tecla para interrumpir la cuenta regresiva.
2. Si observa el error que tuvo durante el arranque anterior, parece que al menos ciertas partes del sistema aún están funcionando. Dado que sabe la contraseña **root (redhat)**, intente un arranque de **emergencia**.
  - 2.1. Use las teclas de dirección para destacar la entrada del cargador de arranque predeterminada.
  - 2.2. Presione **e** para editar la entrada actual.
  - 2.3. Con las teclas de dirección, navegue hacia la línea que comienza con **linux16**.

- 2.4. Presione **End** (Fin) para mover el cursor hasta el final de la línea.
- 2.5. Agregue **systemd.unit=emergency.target** en el final de la línea.
- 2.6. Presione **Ctrl+x** para realizar el arranque con la configuración modificada.
3. Inicie sesión en el modo de emergencia. Preste atención a los errores que pueda recibir.
  - 3.1. En el prompt **Give root password for maintenance** (Proporcione la contraseña root para mantenimiento), ingrese **redhat**.
4. Inspeccione qué sistemas de archivos se montan actualmente.
  - 4.1. 

```
[root@localhost ~]# mount
...
/dev/vda1 on / type xfs (ro,relatime,seclabel,attr2,inode64,noquota)
```
5. Parece que el sistema de archivos root está montado como solo lectura; móntelo como lectura-escritura.
  - 5.1. 

```
[root@localhost ~]# mount -o remount,rw /
```
6. Intente montar todos los demás sistemas de archivos:
  - 6.1. 

```
[root@localhost ~]# mount -a
mount: mount point /RemoveMe does not exist
```
7. Abra **/etc/fstab** en un editor y arregle el problema.
  - 7.1. 

```
[root@localhost ~]# vi /etc/fstab
```
  - 7.2. Elimine la línea no válida (la que tiene **RemoveMe**).
  - 7.3. Guarde los cambios, luego salga del editor.
8. Intente montar todas las entradas para verificar que su **/etc/fstab** ahora sea correcto.
  - 8.1. 

```
[root@localhost ~]# mount -a
```
9. Salga de su shell de **emergencia** y reinicie el sistema; para ello, escriba **reboot**. Ahora su sistema debería arrancar normalmente.

# Reparación de problemas del cargador de arranque

## Objetivos

Luego de completar esta sección, los estudiantes deberían poder reparar problemas del cargador de arranque.

El cargador de arranque utilizado de forma predeterminada en Red Hat Enterprise Linux 7 es **grub2**, la segunda versión importante del *Gran gestor de arranque unificado*.

**grub2** se puede usar para arrancar tanto en sistemas BIOS como UEFI, y admite el arranque de casi cualquier sistema de operaciones que se ejecute en hardware moderno.

El archivo de configuración principal de **grub2** es **/boot/grub2/grub.cfg**, pero se supone que los administradores no editan este archivo directamente. En cambio, se utiliza una herramienta denominada **grub2-mkconfig** para generar esa configuración usando un conjunto de archivos de configuración diferente, y la lista de kernels instalados.

**grub2-mkconfig** observará a **/etc/default/grub** en busca de opciones, como el tiempo de espera del menú predeterminado y la línea de comandos del kernel que se usará, y luego usa un conjunto de scripts en **/etc/grub.d/** para generar un archivo de configuración.

Para hacer cambios permanentes en la configuración del cargador de arranque, un administrador debe editar los archivos de configuración detallados anteriormente, y luego ejecutar el siguiente comando:

```
[root@serverX ~]# grub2-mkconfig > /boot/grub2/grub.cfg
```

En aquellos casos en los que se hayan hecho cambios importantes, se recomienda que el administrador ejecute ese comando sin la redirección, de modo que los resultados se puedan inspeccionar primero.

### Directivas importantes

Para resolver una configuración de **grub2** rota, un administrador primero deberá comprender la sintaxis de **/boot/grub2/grub.cfg**. Las entradas reales que se pueden utilizar para el arranque están codificadas dentro de bloques de **menuentry**. En estos bloques, las líneas **linux16** y **initrd16** apuntan al kernel que se cargará desde el disco (junto con la línea de comandos del kernel) y a las **initramfs** que se cargarán. Durante la edición interactiva en el arranque, la finalización de la **pestaña** está disponible para encontrar estos archivos.

Las líneas de **set root** dentro de esos bloques no apuntan al sistema de archivos root para el sistema Red Hat Enterprise Linux 7; en cambio, apuntan al sistema de archivos desde el cual **grub2** debería cargar los archivos de initramfs y el kernel. La sintaxis es **harddrive**, **partition**, donde **hd0** es el primer disco duro en el sistema, **hd1** es el segundo, etc. Las particiones se indican como **msdos1** para la primera partición de MBR, o **gpt1** para la primera partición de GPT en esa unidad.

### Reinstalación del cargador de arranque

En aquellos casos donde el mismo cargador de arranque se ha dañado, se puede volver a instalar usando el comando **grub2-install**. En sistemas BIOS, el disco donde **grub2** debe

instalarse en el MBR debe proporcionarse como un argumento. En sistemas UEFI, no es necesario ningún argumento cuando la partición del sistema EFI se monta en **/boot/efi**.



### Referencias

**info grub2** (*Manual GNU GRUB*)

**info grub2-install** (*Manual GNU GRUB*)

- Capítulo 28: "Cómo invocar **grub2-install**"

# Práctica: Reparación de un problema del cargador de arranque

En este trabajo de laboratorio, reparará un problema con la configuración del cargador de arranque en una de sus máquinas.

## Recursos:

|                  |         |
|------------------|---------|
| <b>Máquinas:</b> | serverX |
|------------------|---------|

## Resultados:

Una máquina que arranca normalmente sin la intervención del usuario.

### Antes de comenzar

- Restablezca su sistema **serverX**.
- Inicie sesión en su sistema **serverX** y configúrelo:

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

Uno de sus *anteriores* compañeros de trabajo estaba experimentando con la aceleración del proceso de arranque en una de sus máquinas. Luego de varios intentos fallidos, se le ha asignado a usted la tarea de reparar el daño provocado.

- Observe la consola de su máquina **serverX**, luego reiníciela e interrumpa el reloj de la cuenta regresiva del cargador de arranque.
  - Envíe **Ctrl+Alt+Del** a su sistema usando la entrada del menú o el botón relevantes.
  - Cuando el menú del cargador de arranque aparezca, presione cualquier tecla para interrumpir la cuenta regresiva.
- Mueva el cursor hasta la entrada de arranque predeterminada, luego presione **e** para editar esa entrada. Inspeccione la configuración detenidamente, en busca de cualquier cosa que parezca fuera de lo común.
- Encuentre la línea que bloquea el proceso de arranque, modifíquela, y luego arranque con esos cambios.
  - os16** no es una directiva **grub** válida. Cámbiela a **linux16**.
  - Presione **Ctrl+x** para arrancar el sistema con la configuración modificada.
- Espere a que el sistema arranque, inicie sesión como **student**, eleve sus privilegios a **root**, y luego genere una nueva configuración de **grub2**. No sobrescriba inmediatamente la configuración existente; inspeccione la nueva configuración primero.
  - ```
[student@serverX ~]$ sudo -i
[root@serverX ~]# grub2-mkconfig
```
 - Desplácese por el resultado para ver si parece una configuración de **grub2** válida.

- 4.3. Grabe la configuración a disco.

```
[root@serverX ~]# grub2-mkconfig > /boot/grub2/grub.cfg
```

5. Reinicie la máquina y compruebe si arranca normalmente de nuevo sin la intervención del usuario.

- 5.1.

```
[root@serverX ~]# systemctl reboot
```

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.

Andes 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**.

El proceso de arranque de Red Hat Enterprise Linux

- El proceso de arranque de Red Hat Enterprise Linux 7 se puede dividir en cuatro pasos:
 1. Hardware (BIOS/UEFI)
 2. Cargador de arranque (**grub2**)
 3. **kernel** e **initramfs**
 4. **systemd**
- **systemctl reboot** y **systemctl poweroff** reinician y apagan el sistema, respectivamente.
- **systemctl isolate desired.target** cambia a un nuevo objetivo en tiempo de ejecución.
- **systemctl get-default** y **systemctl set-default** se pueden usar para consultar y establecer el objetivo predeterminado.
- **systemd.unit=** en la línea de comandos del kernel selecciona un objetivo diferente en el arranque.

Reparación de problemas de arranque comunes

- Use **rd.break** en la línea de comandos del kernel para interrumpir el proceso de arranque antes de que se entregue el control desde el **initramfs**. El sistema se montará (solo lectura) bajo **/sysroot**.
- Se puede usar **journalctl** para filtrar para arranques específicos con la opción **-b**.
- El servicio **debug-shell.service** se puede utilizar para obtener una **root** shell automática durante el arranque.

Reparación de problemas del sistema de archivos en el arranque

- **systemd** mostrará una shell de emergencia en la mayoría de los casos en que lidie con problemas de sistemas de archivo.
- El objetivo **emergency.target** también puede utilizarse para diagnosticar y arreglar problemas de sistemas de archivos.

Reparación de problemas del cargador de arranque

- Use **e** y **Ctrl+x** para editar las entradas del cargador de arranque en la memoria, y luego realice el arranque.

- Use **grub2-mkconfig > /boot/grub2/grub.cfg** para volver a generar la configuración del cargador de arranque.
- **grub2-install** se utiliza para reinstalar el cargador de arranque.



CAPÍTULO 10

CONFIGURACIÓN DE RED

Descripción general	
Meta	Configurar la red IPv4 básica en los sistemas Red Hat Enterprise Linux.
Objetivos	<ul style="list-style-type: none">Probar 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">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
Trabajo de laboratorio	<ul style="list-style-type: none">Administración de la red de Red Hat Enterprise Linux

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 difusión (broadcast) 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

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.

- 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 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
```

- 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      0
        TX: bytes packets errors dropped carrier collsns
        360733      1730      0      0      0      0
```

- 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
```

- 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:               --
```

Capítulo 10. Configuración de red

```
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:ff: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 iface 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" iface 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"
```

4. 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 DEVICENAME**.

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
...
```

Capítulo 10. Configuración de red

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
<code>nmcli net off</code>	Deshabilitar todas las interfaces administradas.
<code>nmcli con add ...</code>	Añadir una conexión nueva.
<code>nmcli con mod "<ID>" ...</code>	Modificar una conexión.
<code>nmcli con del "<ID>"</code>	Eliminar una conexión.



nota

El comando **nmcli** también tiene un modo de edición interactivo. 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.

Andes 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
```

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. Asigne el nombre *static-eth0* a la conexión nueva.

```
[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.11/24 brd 172.25.X.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

<i>Estática</i>	<i>Dinámica</i>	<i>Cualquiera de las opciones</i>
BOOTPROTO=none		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 root, 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 root, 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
```

Capítulo 10. Configuración de red

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
```

Capítulo 10. Configuración de red

```
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.

Andes 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
```

```
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.

Andes 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.10/24
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.10/24
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
```

- Reinic peace el sistema y, luego, ejecute **lab network grade** para verificar la configuración.

```
[root@desktopX ~]# lab network grade
```

Resumen

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 11

REGISTRO DEL SISTEMA Y NTP

Descripción 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 (diario) de systemd para solucionar problemas o revisar el estado del sistema.• Configurar systemd-journald para almacenar el journal (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 (diario) de systemd (y práctica)• Conservación del journal (diario) de systemd (y práctica)• Mantenimiento del 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 journal (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.

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 prioridades 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 la depuración de gravedad en el archivo de registro creado recientemente **/var/log/messages-debug** mediante la adición del **rsyslog** archivo de configuración de **/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
...
Feb 13 10:37:44 localhost root: Debug Message Test
```

Revisión de las entradas del journal (diario) de systemd

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder encontrar e interpretar las entradas de registro en el journal (diario) de systemd para solucionar problemas o revisar el estado del sistema.

Cómo encontrar eventos con `journalctl`

El journal (diario) 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 journal (diario) de systemd se almacena en `/run/log` de manera predeterminada, y sus contenidos se borran después del reinicio. El administrador del sistema puede modificar esta configuración y esta se analiza en otra parte de la siguiente sección.

El comando `journalctl` muestra el journal (diario) 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 (diario) para la solución de problemas y auditorías es limitar las búsquedas en el journal (diario) para mostrar solo el resultado relevante. En los siguientes párrafos, se presentarán varias estrategias diferentes para restringir el resultado de consultas del journal (diario).

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 (diario) por prioridad de las entradas del journal (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 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 (diario) y continúa proporcionando las entradas del journal (diario) nuevas a medida que se escriben en el journal (diario).

```
[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 rango 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 (diario) que se registraron hoy:

```
[root@serverX ~]# journalctl --since today
```

Proporciona las entradas del journal (diario) 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 (diario), 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 (diario), pueden usarse todos los campos adicionales que se muestran. Esto es útil para restringir el resultado de búsquedas complejas para determinados eventos del journal (diario).

```
[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]
_PRIORITY=6
_UID=0
_GID=0
_BOOT_ID=1ea26e84667848af9a4a2904a76ff9a5
_MACHINE_ID=4513ad59a3b442ffa4b7ea88343fa55f
_CAP_EFFECTIVE=0000001ffffffffffff
_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 (diario) 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 (diario), 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 (diario) de systemd según criterios específicos.

Resultados:

Los estudiantes practicarán visualizar la salida del journal (diario) de **systemd** de manera que coincida con diferentes criterios.

1. Obtener la salida de solo los mensajes del journal (diario) **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 (diario) **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 (diario) 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 (diario) de systemd

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder configurar **systemd-journald** para que almacene el journal (diario) en el disco y no en la memoria.

Almacenar el journal (diario) del sistema de manera permanente.

De manera predeterminada, el journal (diario) de systemd se conserva en **/run/log/journal**, lo que significa que se borra cuando se reinicia el sistema. El journal (diario) es un mecanismo nuevo en Red Hat Enterprise Linux 7, y para la mayoría de las instalaciones, basta con un journal (diario) detallado que comienza con el último inicio.

Si el directorio **/var/log/journal** existe, el journal (diario) 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 (diario) sea persistente, no todos los datos se conservarán para siempre. El journal (diario) tiene un mecanismo de rotación de registro incorporado que se activará mensualmente. Además, de manera predeterminada, el journal (diario) 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 (diario) 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 (diario) de systemd puede hacerse persistente si se crea el directorio **/var/log/journal** como usuario root:

```
[root@serverX ~]# mkdir /var/log/journal
```

Asegúrese de que el directorio **/var/log/journal** sea propiedad del usuario root 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 (diario) 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 (diario) constante, generalmente es necesario limitar la cola del journal (diario) 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 (diario) de systemd constante

En este ejercicio de laboratorio, los estudiantes usarán el journal (diario) de systemd constante.

Resultados:

El journal (diario) de **systemd** se escribe en el disco.

- Configure el journal (diario) 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 (diario) de systemd sea constante, busque un directorio nuevo con los archivos de registro del journal (diario) 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".

Capítulo 11. Registro del sistema y NTP

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**.

De manera predeterminada, **chronyd** 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 **chronyd** 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 **chronyd** 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 **chronyd**. 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 en 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.
```

Capítulo 11. Registro del sistema y NTP

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 **chrony** 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 **chrony** 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  
=====
```

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 (diario) 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.
2. Muestre todas las entradas del journal (diario) **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 (diario) 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.

- 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 (diario) **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 (diario) de systemd

El journal (diario) de systemd ofrece capacidades avanzadas para consultar eventos.

Preservando el journal (diario) de systemd

Configuración de **systemd-journald** para el almacenamiento permanente del journal (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 12

ADMINISTRACIÓN DE VOLÚMENES LÓGICOS

Descripción general	
Meta	Crear y gestionar volúmenes lógicos desde la línea de comandos.
Objetivos	<ul style="list-style-type: none">• Administrar volúmenes lógicos.• Extender volúmenes lógicos.
Secciones	<ul style="list-style-type: none">• Gestión de volúmenes lógicos (y práctica)• Extensión de volúmenes lógicos (y práctica)
Trabajo de laboratorio	<ul style="list-style-type: none">• Administración del almacenamiento de gestión de volúmenes lógicos (LVM)

Gestión de volúmenes lógicos

Objetivos

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

- Implementar almacenamiento del LVM.
- Visualizar información de componentes del LVM.

Implementación de almacenamiento del LVM

LVM viene con un conjunto integral de herramientas de línea de comandos para implementar y administrar almacenamiento del LVM. Estas herramientas de línea de comandos se pueden usar en scripts, lo que las hace más adecuadas para la automatización.



Importante

Los siguientes ejemplos usan el dispositivo **vda** y sus particiones para ilustrar comandos de LVM. En la práctica, estos ejemplos deberían usar los dispositivos correctos para el disco y las particiones del disco utilizados por el sistema.

Creación de un volumen lógico

Son cinco los pasos necesarios para crear un volumen lógico utilizable:

1. **Prepare el dispositivo físico.**

Use **fdisk**, **gdisk** o **parted** para crear una nueva partición para usar con LVM. Siempre configure el tipo de partición en **Linux LVM** (LVM Linux) en las particiones de LVM; use **0x8e** para particiones estilo MBR. Si es necesario, use **partprobe** para registrar la nueva partición con el kernel.

De forma alternativa, use un disco entero, un arreglo RAID o un disco SAN.

Solo se necesita preparar un dispositivo físico si no hay ninguno ya preparado, y se requiere un volumen físico nuevo para crear o ampliar un grupo de volúmenes.

```
[root@serverX ~]# fdisk /dev/vda
```

Use **m** para obtener ayuda, **p** para imprimir la tabla de particiones existentes, **n** para crear una partición nueva, **t** para cambiar el tipo de partición, **w** para escribir los cambios y **q** para salir.

2. **Cree un volumen físico.**

pvccreate se usa para etiquetar la partición (u otro dispositivo físico) para su uso con el LVM como volumen físico. Se escribe un encabezado para almacenar los datos de configuración del LVM directamente en el PV. Un PV se divide en extensiones físicas (PE) de un tamaño fijo; por ejemplo, bloques de 4 MiB. Etiquete varios dispositivos al mismo tiempo con nombres de dispositivos delimitados por espacios como argumentos para **pvccreate**.

```
[root@serverX ~]# pvcreate /dev/vda2 /dev/vdb1
```

Esto etiquetará dispositivos **/dev/vda2** y **/dev/vdb1** como PV, listos para la asignación en un grupo de volúmenes.

Un PV solo debe crearse si no hay PV libres para crear o ampliar un VG.

3. Cree un grupo de volúmenes.

vgcreate se usa para crear un pool (conjunto) de uno o más volúmenes físicos, a los que se denomina grupo de volúmenes. El tamaño del VG se determina mediante la cantidad total de extensiones físicas en el pool (conjunto). Un VG es responsable de alojar uno o más volúmenes lógicos al asignar PE libres a un LV; por lo tanto, debe tener suficientes PE libres disponibles en el momento en que se crea el LV.

Como argumentos para **vgcreate**, defina un nombre de VG y detalle uno o más PV para asignar al VG.

```
[root@serverX ~]# vgcreate vg-alpha /dev/vda2 /dev/vdb1
```

Esto creará un VG denominado **vg-alpha** que tiene el tamaño combinado, en unidades de PE, de los dos PV: **/dev/vda2** y **/dev/vdb1**.

Un VG solo debe crearse cuando no haya ninguno en existencia. Se pueden crear más VG por motivos administrativos para administrar el uso de PV y LV. O bien, los VG existentes se pueden ampliar para alojar nuevos LV cuando sea necesario.

4. Cree un volumen lógico.

lvcreate crea un nuevo volumen lógico desde las extensiones físicas disponibles en un grupo de volúmenes. Use estos argumentos para **lvcreate** como mínimo: use la opción **-n** para configurar el nombre del LV, la opción **-L** para configurar el tamaño del LV en bytes, e identifique el nombre del VG donde se creará el LV.

```
[root@serverX ~]# lvcreate -n hercules -L 2G vg-alpha
```

Esto creará un LV denominado **hercules**, con un tamaño de **2 GiB**, en el VG **vg-alpha**. Debe haber suficientes extensiones físicas libres para distribuir 2 GiB, y si es necesario, se redondeará a un factor del tamaño de unidades de PE.

Hay varias maneras de especificar el tamaño: **-L** anticipa el tamaño en bytes, o valores nombrados más grandes, como mebibbytes (megabytes binarios, 1048576 bytes) y gibibbytes (gigabytes binarios). La opción **-l** anticipa tamaños medidos como una cantidad de extensiones físicas.

Algunos ejemplos:

- **lvcreate -L 128M**: Cambia el tamaño del volumen lógico a exactamente 128 MiB.
- **lvcreate -l 128** : Cambia el tamaño del volumen lógico a exactamente 128 extensiones. El número total de bytes depende del tamaño del bloque de extensiones físicas en el volumen físico subyacente.



Importante

Diferentes herramientas mostrarán el nombre del volumen lógico, ya sea usando el nombre tradicional `/dev/vgname/lvname` o el nombre del asignador de dispositivos del kernel `/dev/mapper/vgname-lvname`.

5. Agregue el sistema de archivos.

Use `mkfs` para crear un sistema de archivos `xfs` en el nuevo volumen lógico. De forma alternativa, cree un sistema de archivos basado en su sistema de archivos preferido; por ejemplo, `ext4`.

```
[root@serverX ~]# mkfs -t xfs /dev/vg-alpha/hercules
```

Para hacer que el sistema de archivos esté disponible luego de los reinicios:

- Use `mkdir` para crear un directorio de punto de montaje.

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

- Agregue una entrada al archivo `/etc/fstab`:

```
/dev/vg-alpha/hercules /mnt/hercules xfs defaults 1 2
```

- Ejecute `mount -a` para montar todos los sistemas de archivos en `/etc/fstab`, incluida la entrada que agregó recientemente.

```
[root@serverX ~]# mount -a
```

Eliminación de un volumen lógico

Son cuatro los pasos necesarios para eliminar *todos* los componentes de un volumen lógico:

1. Prepare el sistema de archivos.

Traslade todos los datos que se deben conservar a otro sistema de archivos, y luego use `umount` para desmontar el sistema de archivos. No olvide eliminar todas las entradas `/etc/fstab` asociadas con este sistema de archivos.

```
[root@serverX ~]# umount /mnt/hercules
```



Advertencia

Al eliminar un volumen lógico se destruirán todos los datos almacenados en este. Realice una copia de seguridad de los datos o trasládelos *ANTES* de eliminar el volumen lógico.

2. Elimine el volumen lógico.

lvremove se usa para eliminar un volumen lógico que ya no es necesario. Use el nombre del dispositivo como el argumento.

```
[root@serverX ~]# lvremove /dev/vg-alpha/hercules
```

Antes de ejecutar este comando, se debe desmontar el sistema de archivos del LV. Se le solicitará una confirmación antes de eliminar el LV.

Las extensiones físicas del LV se liberarán y estarán disponibles para ser asignadas a LV existentes o nuevos en el grupo de volúmenes.

3. Elimine el grupo de volúmenes.

vgremove se usa para eliminar un grupo de volúmenes que ya no es necesario. Use el nombre del VG como el argumento.

```
[root@serverX ~]# vgremove vg-alpha
```

Los volúmenes físicos del VG se liberarán y estarán disponibles para ser asignados a VG existentes o nuevos en el sistema.

4. Elimine los volúmenes físicos.

pvremove se usa para eliminar volúmenes físicos que ya no son necesarios. Use una lista delimitada por espacios de dispositivos del PV para eliminar más de uno a la vez. Los metadatos del PV se borran de la partición (o disco). Ahora, la partición está libre para una nueva asignación o para ser formateada.

```
[root@serverX ~]# pvremove /dev/vda2 /dev/vdb1
```

Revisión de la información de estado de LVM

Volúmenes físicos

Use **pvdisplay** para visualizar información sobre volúmenes físicos (VP). Si no se especifica ningún argumento con el comando, este detallará información sobre todos los PV del sistema. Si el argumento es el nombre de un dispositivo específico, la información que se mostrará se limitará a este PV específico.

```
[root@serverX ~]# pvdisplay /dev/vda2
--- Physical volume ---
PV Name      /dev/vda2
VG Name      vg-alpha
PV Size      256.00 MiB / not usable 4.00 MiB
Allocatable   yes
PE Size      4.00 MiB
Total PE    63
Free PE     26
Allocated PE 37
```

Capítulo 12. Administración de volúmenes lógicos

PV UUID	JWzDpn-LG3e-n2oi-9EtD-VT2H-PMem-1ZXwP1
---------	--

- ① **PV Name** (Nombre de PV) corresponde al nombre del dispositivo.
- ② **VG Name** (Nombre de VG) muestra el grupo de volúmenes donde se encuentra el PV.
- ③ **PV Size** (Tamaño de PV) muestra el tamaño físico del PV, incluido todo el espacio no utilizable.
- ④ **PE Size** (Tamaño de PE) es el tamaño de la extensión física, que es el tamaño más pequeño a donde puede ser asignado un volumen lógico.

Es también el factor de multiplicación que se utiliza en el cálculo del tamaño de cualquier valor informado en las unidades de PE, como *Free PE* (PE libre); por ejemplo: 26 PE x 4 MiB (el *PE Size* [Tamaño de PE]) da 104 MiB de espacio libre. El tamaño de un volumen lógico se redondeará a un factor de unidades de PE.

- LVM establece el tamaño de la PE automáticamente, aunque es posible especificarlo.
- ⑤ **Free PE** (PE libre) muestra cuántas unidades de PE están disponibles para la asignación para nuevos volúmenes lógicos.

Grupos de volúmenes

Use **vgdisplay** para visualizar información sobre grupos de volúmenes (GV). Si no se especifica ningún argumento para el comando, mostrará información sobre todos los VG. Si se usa el nombre del VG como un argumento, la información que se muestra se limitará a ese VG específico.

```
[root@serverX ~]# vgdisplay vg-alpha
--- Volume group ---
VG Name          vg-alpha      ①
System ID        lvm2
Format           lvm2
Metadata Areas   3
Metadata Sequence No 4
VG Access        read/write
VG Status        resizable
MAX LV           0
Cur LV           1
Open LV          1
Max PV           0
Cur PV           3
Act PV           3
VG Size          1012.00 MiB    ②
PE Size          4.00 MiB
Total PE         253          ③
Alloc PE / Size  175 / 700.00 MiB
Free  PE / Size  78 / 312.00 MiB ④
VG UUID          3snNw3-CF71-CcYG-Llk1-p6EY-rHEv-xfUSez
```

- ① **VG Name** (Nombre de VG) es el nombre del grupo de volúmenes.
- ② **VG Size** (Tamaño de VG) es el tamaño total del pool (conjunto) de almacenamiento disponible para la asignación de volúmenes lógicos.
- ③ **Total PE** (PE total) es el tamaño total expresado en unidades de PE.
- ④ **Free PE / Size** (PE libre/tamaño) muestra cuánto espacio libre hay en el VG para distribuir para nuevos LV o para ampliar los LV existentes.

Volúmenes lógicos

Use **lvdisplay** para visualizar información sobre volúmenes lógicos (LV). Una vez más, ningún argumento con el comando mostrará información sobre todos los LV, y el uso del nombre del dispositivo del LV como un argumento mostrará información sobre ese dispositivo específico.

```
[root@serverX ~]# lvdisplay /dev/vg-alpha/hercules
--- Logical volume ---
LV Path          /dev/vg-alpha/hercules 1
LV Name          hercules
VG Name          vg-alpha 2
LV UUID          5IyRea-W8Zw-xLhk-3h2a-IuVN-YaeZ-i3IRrN
LV Write Access  read/write
LV Creation host, time server1.example.com 2014-02-19 00:26:48 -0500
LV Status        available
# open           1
LV Size          700 MiB 3
Current LE      175 4
Segments         3
Allocation       inherit
Read ahead sectors auto
- current set to 8192
Block device    252:0
```

- 1** **LV Path** (Ruta de LV) muestra el nombre del dispositivo de este volumen lógico.

Es posible que algunas herramientas informen el nombre del dispositivo como **/dev/mapper/vgname-lvname**; ambos representan el mismo LV.

- 2** **VG Name** (Nombre de VG) muestra el grupo de volúmenes donde se encuentra el PV.
- 3** **LV Size** (Tamaño de LV) muestra el tamaño total del LV. Use herramientas del sistema de archivos para comprobar el espacio libre y el espacio usado para el almacenamiento de datos.
- 4** **Current LE** (LE actual) muestra la cantidad de extensiones lógicas usadas por este LV. Una LE generalmente se asigna a una extensión física del VG y, por lo tanto, al volumen físico.



Referencias

Páginas del manual: **lvm(8)**, **pvcreate(8)**, **vgcreate(8)**, **lvcreate(8)**, **pvremove(8)**, **vgremove(8)**, **lvremove(8)**, **pvdisplay(8)**, **vgdisplay(8)**, **lvdisplay(8)**, **fdisk(8)**, **gdisk(8)**, **parted(8)**, **partprobe(8)** y **mkfs(8)**

Práctica: Adición de un volumen lógico

En este trabajo de laboratorio, agregará un volumen físico, un grupo de volúmenes, un volumen lógico y un sistema de archivos XFS. Montará de forma persistente el sistema de archivos de volúmenes lógicos.

Recursos:		
Máquinas:	serverX	

Resultados:

Un volumen lógico de 400 MiB denominado **storage** en el grupo de volúmenes **shazam**, montado en **/storage**. El grupo de volúmenes consta de dos volúmenes físicos, cada uno de 256 MiB.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en serverX.
- Abra una terminal.
- Cambie a root (**sudo -i**).

1. Crear los recursos físicos

- 1.1. Use **fdisk** para crear dos particiones de 256 MiB cada una y configúrelas con el tipo Linux LVM.

```
[root@serverX ~]# fdisk /dev/vdb
```

Nota: Los siguientes pasos omiten algunos resultados.

- 1.2. Agregue una nueva partición primaria de 256 MiB.

```
Command (m for help): n
Partition type:
  p  primary (0 primary, 0 extended, 4 free)
  e  extended
Select (default p): Enter
Using default response p
Partition number (1-4, default 1): Enter
First sector (2048-20971519, default 2048): Enter
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519): +256M
```

- 1.3. Cambie el tipo de partición a *Linux LVM* - *0x8e*.

```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'
```

1.4. Repita los dos pasos anteriores para agregar una segunda partición primaria del mismo tamaño en el siguiente espacio disponible para particiones.

1.5. Escriba los cambios en la tabla de particiones y salga.

```
Command (m for help): w  
The partition table has been altered!
```

1.6. Use **partprobe** para registrar las nuevas particiones con el kernel.

```
[root@serverX ~]# partprobe
```

2. Crear los volúmenes físicos

Use **pvcreate** para agregar las dos nuevas particiones como PV.

```
[root@serverX ~]# pvcreate /dev/vdb1 /dev/vdb2  
Physical volume "/dev/vdb1" successfully created  
Physical volume "/dev/vdb2" successfully created
```

3. Crear el grupo de volúmenes

Use **vgcreate** para crear un nuevo VG denominado **shazam** creado a partir de los dos PV.

```
[root@serverX ~]# vgcreate shazam /dev/vdb1 /dev/vdb2  
Volume group "shazam" successfully created
```

4. Crear el volumen lógico

Use **lvcreate** para crear un LV de 400 MiB denominado **storage** desde el VG **shazam**.

```
[root@serverX ~]# lvcreate -n storage -L 400M shazam  
Logical volume "storage" created
```

Esto creará un dispositivo denominado **/dev/shazam/storage**, actualmente sin un sistema de archivos.

5. Agregar un sistema de archivos persistente

5.1. Use **mkfs** para colocar un sistema de archivos **xfs** en el LV **storage**; use el nombre del dispositivo del LV.

```
[root@serverX ~]# mkfs -t xfs /dev/shazam/storage  
meta-data=/dev/shazam/storage      isize=256      agcount=4, agsize=25600 blks  
...
```

5.2. Use **mkdir** para crear un punto de montaje en **/storage**.

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

5.3. Use **vim** para agregar la siguiente línea en la parte inferior de **/etc/fstab** en serverX:

```
/dev/shazam/storage    /storage    xfs defaults 1 2
```

- 5.4. Use **mount** para verificar la entrada **/etc/fstab** y monte el nuevo dispositivo del LV **storage**.

```
[root@serverX ~]# mount -a
```

6. Evaluar y revisar su trabajo

- 6.1. Como prueba final, copie algunos archivos en **/storage** y verifique cuántos se copiaron.

```
[root@serverX ~]# cp -a /etc/*.conf /storage  
[root@serverX ~]# ls /storage | wc -l  
47
```

Comprobaremos que aún tengamos la misma cantidad de archivos en el siguiente ejercicio de práctica.

- 6.2. **fdisk -l /dev/vdb** le mostrará las particiones que existen en **/dev/vdb**.

```
[root@serverX ~]# fdisk -l /dev/vdb
```

Compruebe las entradas **/dev/vdb1** y **/dev/vdb2**, y observe las columnas **Id** (Id.) y **System** (Sistema) que muestran **8e** y **Linux LVM**, respectivamente.

- 6.3. **pvdisplay** le mostrará información sobre cada uno de los volúmenes físicos. De forma opcional, incluya el nombre del dispositivo para limitar detalles a un PV específico.

```
[root@serverX ~]# pvdisplay /dev/vdb2  
--- Physical volume ---  
PV Name          /dev/vdb2  
VG Name          shazam  
PV Size          256.00 MiB / not usable 4.00 MiB  
Allocatable      yes  
PE Size          4.00 MiB  
Total PE         63  
Free PE          26  
Allocated PE     37  
PV UUID          N64t6x-URdJ-fVU3-FQ67-zU6g-So7w-hvXMcM
```

Esto muestra que nuestro PV está asignado al VG **shazam**, tiene un tamaño de 256 MiB (aunque 4 MiB no se pueden utilizar) y el tamaño de nuestra extensión física (**PE Size** [Tamaño de PE]) es de 4 MiB (el tamaño de un LV assignable más pequeño).

Hay 63 PE, de las cuales 26 PE están libres para la asignación para LV en el futuro y 37 PE están asignadas actualmente a LV. Esto se traduce a los siguientes valores de MiB:

- Un total de 252 MiB (63 PE x 4 MiB); recuerde, 4 MiB no se pueden utilizar.
- 104 MiB libres (26 PE x 4 MiB)

- 148 MiB asignados (37 PE x 4 MiB)

6.4. **vgdisplay vgname** mostrará información sobre el grupo de volúmenes denominado **vgname**.

```
[root@serverX ~]# vgdisplay shazam
```

Compruebe lo siguiente:

- El valor de **VG Size** (Tamaño de VG) es **504,00 MiB**.
- El valor de **Total PE** (PE total) es **126**.
- El valor de **Alloc PE / Size** (PE asign. / Tamaño) es **100 / 400,00 MiB**.
- El valor de **Free PE / Size** (PE libre / Tamaño) es **26 / 104,00 MiB**.

6.5. **lvdisplay /dev/vgname/lvname** mostrará información sobre el volumen lógico denominado **lvname**.

```
[root@serverX ~]# lvdisplay /dev/shazam/storage
```

Observe los valores de **LV Path** (Ruta de LV), **LV Name** (Nombre de LV), **VG Name** (Nombre de VG), **LV Status** (Estado de LV), **LV Size** (Tamaño de LV) y **Current LE** (LE actual) (extensiones lógicas, que se asignan a extensiones físicas).

6.6. **mount** mostrará todos los dispositivos que están montados y todas las opciones de montaje. Debe incluir **/dev/shazam/storage**.



nota

Recordatorio: Muchas herramientas informarán en cambio el nombre del asignador de dispositivos, **/dev/mapper/shazam-storage**; es el mismo volumen lógico.

```
[root@serverX ~]# mount
```

Debe observar (probablemente, en la última línea) **/dev/mapper/shazam-storage** montado en **/storage** y la información de montaje asociada.

6.7. **df -h** mostrará espacio libre legible para el ser humano. De forma opcional, incluya el punto de montaje para limitar detalles a ese sistema de archivos.

```
[root@serverX ~]# df -h /storage
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/shazam-storage  397M   21M  377M   6% /storage
```

Capítulo 12. Administración de volúmenes lógicos

Estos valores, permitidos para metadatos del sistema de archivos, son lo que esperaríamos.

Extensión de volúmenes lógicos

Objetivos

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

- Extender y reducir un grupo de volúmenes.
- Extender un LV con un sistema de archivos XFS.
- Extender un LV con un sistema de archivos ext4.

Extensión y reducción de un grupo de volúmenes

Se puede agregar más espacio en disco a un grupo de volúmenes mediante la adición de más volúmenes físicos. Esto se denomina extensión del grupo de volúmenes. Las nuevas extensiones físicas proporcionadas mediante los volúmenes físicos adicionales luego se pueden reasignar a volúmenes lógicos.

Los volúmenes físicos no usados se pueden eliminar de un grupo de volúmenes. Esto se denomina reducción del grupo de volúmenes. Se puede utilizar una herramienta denominada `pvmove` para trasladar datos desde extensiones de un volumen físico a extensiones de otros volúmenes físicos en el grupo de volúmenes. De esta manera, se puede agregar un nuevo disco a un grupo de volúmenes existentes, se pueden trasladar los datos desde un disco más antiguo o más lento hacia el disco nuevo y se puede eliminar el disco viejo del grupo de volúmenes. Esto se puede hacer mientras los volúmenes lógicos del grupo de volúmenes están en uso.



Importante

En los siguientes ejemplos, se usa el dispositivo **vdb** y sus particiones para ilustrar comandos LVM. En la práctica, estos ejemplos deberían usar los dispositivos correctos para el disco y las particiones del disco utilizados por el sistema.

Ampliación de un grupo de volúmenes

Potencialmente, son cuatro los pasos necesarios para ampliar un grupo de volúmenes:

1. **Prepare el dispositivo físico.**

Al igual que en la creación de un nuevo grupo de volúmenes, se debe crear y preparar una nueva partición para usar como volumen físico de LVM.

Use **fdisk**, **gdisk** o **parted** para crear una nueva partición para usar con LVM. Siempre configure el tipo de partición en **Linux LVM** (LVM Linux) en las particiones de LVM; use **0x8e** para particiones estilo MBR. Si es necesario, use **partprobe** para registrar la nueva partición con el kernel.

De forma alternativa, use un disco entero, un arreglo RAID o un disco SAN.

Solo se necesita preparar un dispositivo físico si no hay ninguno ya preparado, y se requiere un volumen físico nuevo para ampliar el grupo de volúmenes.

```
[root@serverX ~]# fdisk /dev/vdb
```

Use **m** para obtener ayuda, **p** para imprimir la tabla de particiones existentes, **n** para crear una partición nueva, **t** para cambiar el tipo de partición, **w** para escribir los cambios y **q** para salir.

2. Cree el volumen físico.

pvccreate se usa para etiquetar la partición (u otro dispositivo físico) para su uso con el LVM como volumen físico. Se escribe un encabezado para almacenar los datos de configuración del LVM directamente en el PV. Un PV se divide en extensiones físicas de un tamaño fijo; por ejemplo, bloques de 4 MiB. Use el nombre del dispositivo como el argumento para **pvccreate**.

```
[root@serverX ~]# pvccreate /dev/vdb2
```

Esto etiquetará el dispositivo **/dev/vdb2** como un PV, listo para la asignación en el grupo de volúmenes.

Un PV solo debe crearse si no hay PV libres para extender el VG.

3. Amplíe un grupo de volúmenes.

vgextend se usa para agregar un nuevo volumen físico al grupo de volúmenes existente. Use el nombre del VG y el nombre del dispositivo del PV como argumentos para **vgextend**.

```
[root@serverX ~]# vgextend vg-alpha /dev/vdb2
```

Esto ampliará el VG **vg-alpha** al tamaño del PV **/dev/vdb2**.

4. Verifique que el nuevo espacio esté disponible.

Use **vgdisplay** para confirmar que las extensiones físicas adicionales estén disponibles. Compruebe el **Free PE / Size** (PE libre/tamaño) en el resultado. No debe ser cero.

```
[root@serverX ~]# vgdisplay vg-alpha
--- Volume group ---
  VG Name           vg-alpha
...
  Free  PE / Size    178 / 712.00 MiB
...
```

Reducción de un grupo de volúmenes

Son solo dos los pasos necesarios para ampliar un grupo de volúmenes:

1. Traslade las extensiones físicas.

pvmove se utiliza para reubicar todas las extensiones físicas usadas en el volumen físico para otros PV del VG. Esto solo es posible si hay suficientes extensiones libres en el VG y si todas corresponden a otros PV. Use el nombre del dispositivo del PV para el cual las PE se trasladarán como el argumento para el comando.

```
[root@serverX ~]# pvmove /dev/vdb2
```

Esto trasladará las PE desde **/dev/vdb2** a otros PV con PE libres en el mismo VG.



Advertencia

Antes de usar **pvmove**, se recomienda efectuar una copia de seguridad de los datos en los volúmenes lógicos del grupo de volúmenes. Una pérdida de energía imprevista durante la operación puede hacer que el grupo de volúmenes quede en un estado incoherente. Esto provocaría la pérdida de datos en volúmenes lógicos en el grupo de volúmenes.

2. Reduzca el grupo de volúmenes.

vgreduce se usa para eliminar el volumen físico del grupo de volúmenes. Use el nombre del VG y el nombre del dispositivo del PV como argumentos para el comando.

```
[root@serverX ~]# vgreduce vg-alpha /dev/vdb2
```

El PV **/dev/vdb2** ahora se elimina del VG **vg-alpha** y se puede agregar a otro VG. De forma alternativa, se puede usar **pvremove** para dejar de usar el dispositivo como un PV de forma permanente.

Ampliar un volumen lógico y su sistema de archivos XFS

Uno de los beneficios de los volúmenes lógicos es la capacidad para aumentar su tamaño sin experimentar tiempo de inactividad. Las extensiones físicas libres en un grupo de volúmenes se pueden agregar a un volumen lógico para extender su capacidad, que luego se puede usar para extender el sistema de archivos que contiene.

Ampliación de un volumen lógico

Son tres los pasos necesarios para ampliar un volumen lógico:

1. Verifique que el grupo de volúmenes tenga espacio disponible.

vgdisplay se usa para verificar que haya suficientes extensiones físicas disponibles para su uso.

```
[root@serverX ~]# vgdisplay vg-alpha
  --- Volume group ---
  VG Name              vg-alpha
  ...
  Free   PE / Size     178 / 712.00 MiB
  ...
```

Compruebe el **Free PE / Size** (PE libre/tamaño) en el resultado. Debe informar un valor igual o mayor que el espacio adicional requerido. Si no hay suficiente espacio

disponible, amplíe el grupo de volúmenes en al menos el espacio requerido. Consulte "Ampliación y reducción de un grupo de volúmenes".

2. Amplíe el volumen lógico.

lvextend amplía el volumen lógico a un nuevo tamaño. Agregue el nombre del dispositivo del LV como el último argumento para el comando.

```
[root@serverX ~]# lvextend -L +300M /dev/vg-alpha/hercules
```

Esto aumentará el tamaño del volumen lógico **hercules** en 300 MiB. Observe el signo "+" delante del tamaño: significa agregar este valor al tamaño existente; de lo contrario, el valor define el tamaño final exacto del LV.

Al igual que **lvcreate**, hay varias maneras de especificar el tamaño: **-L** generalmente espera valores de extensiones físicas, mientras que **-L** espera tamaños en bytes o valores nombrados más grandes, como mebibytes y gibibytes.

Algunos ejemplos:

- **lvextend -L 128**: Cambia el tamaño del volumen lógico a *exactamente* 128 extensiones.
- **lvextend -L +128**: Agrega 128 extensiones al tamaño actual del volumen.
- **lvextend -L 128M**: Cambia el tamaño del volumen lógico a *exactamente* 128 MiB.
- **lvextend -L +128M**: Agrega 128 MiB al tamaño actual del volumen lógico.
- **lvextend -L +50%FREE**: Agrega el 50 % del espacio libre actual en el VG al LV.

3. Amplíe el sistema de archivos.

xfs_growfs /mountpoint amplía el sistema de archivos para que ocupe el LV ampliado. **xfs_growfs** requiere que el sistema de archivos se monte mientras se está ejecutando; puede continuar usándose durante la operación de modificación del tamaño.

```
[root@serverX ~]# xfs_growfs /mnt/hercules
```



nota

Un error común es ejecutar **lvextend** y olvidarse de ejecutar **xfs_growfs**. Una alternativa a ejecutar estos pasos de forma consecutiva es incluir **-r** como una opción con el comando **lvextend**. Esto modifica el tamaño del sistema de archivos luego de que el VL se extienda, usando **fsadm(8)**. Funciona con varios sistemas de archivos diferentes.

- Es una buena idea verificar el nuevo tamaño del sistema de archivos montado:
df -h /mountpoint.

Ampliar un volumen lógico y su sistema de archivos ext4

Ampliación de un volumen lógico

Los pasos para ampliar un volumen lógico basado en **ext4** son básicamente los mismos que para un LV basado en **xfs**, excepto por el paso para modificar el tamaño del sistema de archivos. Consulte "Ampliar un volumen lógico y su sistema de archivos XFS" para obtener más detalles.

- Verifique que el grupo de volúmenes tenga espacio disponible.**

vgdisplay vgname se usa para verificar que haya suficientes extensiones físicas disponibles para su uso.

- Amplíe el volumen lógico.**

lvextend -l +extents /dev/vgname/lvname amplía el volumen lógico */dev/vgname/lvname* en el valor de las *extenciones*.

- Amplíe el sistema de archivos.**

resize2fs /dev/vgname/lvname amplía el sistema de archivos para ocupar el nuevo LV ampliado. Al igual que **xfs_growfs**, el sistema de archivos se puede montar y estar en uso mientras se encuentra en ejecución. Como alternativa, incluya la opción **-p** para ver el progreso de la operación de modificación del tamaño.

```
[root@serverX ~]# resize2fs /dev/vg-alpha/hercules
```



nota

La principal diferencia entre **xfs_growfs** y **resize2fs** es el argumento que se pasó para identificar el sistema de archivos. **xfs_growfs** toma el punto de montaje y **resize2fs** toma el nombre del volumen lógico.



Referencias

Páginas del manual: **lvm(8)**, **pvcREATE(8)**, **pvmOVE(8)**, **vgDISPLAY(8)**, **vgEXTEND(8)**, **vgREDUCE(8)**, **vgDISPLAY(8)**, **vgEXTEND(8)**, **vgREDUCE(8)**, **lvEXTEND(8)**, **fdisk(8)**, **gdisk(8)**, **parted(8)**, **partprobe(8)**, **xfs_growfs(8)** y **resize2fs(8)**

Práctica: Ampliación de un volumen lógico

En este trabajo de laboratorio, ampliará el volumen lógico agregado en el ejercicio de práctica anterior.

Recursos:		
Máquinas:	serverX	

Resultados:

Un volumen lógico con el tamaño modificado, 700 MiB en total, denominado **storage** (almacenamiento) en el grupo de volúmenes **shazam**, montado en **/storage**. Modificación del tamaño llevada a cabo mientras el sistema de archivos aún está montado y en uso. Grupo de volúmenes ampliado para incluir un volumen físico adicional de 512 MiB, con un tamaño del VG total de 1 GiB.

Antes de comenzar

Completar Práctica: Adición de un volumen lógico

1. Comprobar el espacio en el grupo de volúmenes

Use **vgdisplay** para comprobar si el VG tiene suficiente espacio libre para ampliar el LV hasta un tamaño total de 700 MiB.

```
[root@serverX ~]# vgdisplay shazam
  --- Volume group ---
  VG Name          shazam
  System ID
  Format          lvm2
  ...
  VG Size         504.00 MiB
  PE Size         4.00 MiB
  Total PE        126
  Alloc PE / Size 100 / 400.00 MiB
  Free  PE / Size 26 / 104.00 MiB
  VG UUID        0BBAtU-2nBS-4SW1-khmF-yJzi-z7bD-DpCrAV
```

Solo hay 104 MiB disponibles (26 PE x extensiones de 4 MiB) y necesitamos al menos 300 MiB para tener un total de 700 MiB. Necesitamos ampliar el VG.

Para una posterior comparación, use **df** para comprobar el espacio libre en el disco actual:

```
[root@serverX ~]# df -h /storage
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/shazam-storage 397M   21M  377M   6% /storage
```

2. Crear los recursos físicos

Use **fdisk** para crear una partición adicional de 512 MiB y configúrela con el tipo Linux LVM.

2.1. [root@serverX ~]# fdisk /dev/vdb

Nota: Los siguientes pasos omiten algunos resultados.

2.2. Agregue una nueva partición primaria de 512 MiB.

```
Command (m for help): n
Partition type:
  p  primary (2 primary, 0 extended, 2 free)
  e  extended
Select (default p): Enter
Using default response p
Partition number (3,4, default 3): Enter
First sector (1050624-20971519, default 1050624): Enter
Using default value 1050624
Last sector, +sectors or +size{K,M,G} (1050624-20971519, default
20971519): +512M
Partition 3 of type Linux and of size 512 MiB is set
```

2.3. Cambie el tipo de partición a *Linux LVM* - 0x8e.

```
Command (m for help): t
Partition number (1-3, default 3): Enter
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'
```

2.4. Escriba los cambios en la tabla de particiones y salga.

```
Command (m for help): w
The partition table has been altered!
```

2.5. Use **partprobe** para registrar las nuevas particiones con el kernel.

```
[root@serverX ~]# partprobe
```

3. **Crear el volumen físico**

Use **pvcreate** para agregar la nueva partición como un PV.

```
[root@serverX ~]# pvcreate /dev/vdb3
Physical volume "/dev/vdb3" successfully created
```

4. **Ampliar el grupo de volúmenes**

4.1. Use **vgextend** para ampliar el VG denominado **shazam**, mediante el nuevo PV / **dev/vdb3**.

```
[root@serverX ~]# vgextend shazam /dev/vdb3
Volume group "shazam" successfully extended
```

4.2. Use **vgdisplay** para comprobar nuevamente el espacio libre del VG **shazam**. Ahora, debe haber suficiente espacio libre.

```
[root@serverX ~]# vgdisplay shazam
--- Volume group ---
```

```
VG Name          shazam
System ID       lvm2
Format          lvm2
...
VG Size         1012.00 MiB
PE Size         4.00 MiB
Total PE        253
Alloc PE / Size 100 / 400.00 MiB
Free PE / Size 153 / 612.00 MiB
VG UUID        0BBATU-2nBS-4SW1-khmF-yJzi-z7bD-DpCrAV
```

Ahora hay 612 MiB disponibles (153 PE x extensiones de 4MiB); perfecto.

5. Ampliar el volumen lógico

Use **lvextend** para ampliar el LV existente a 700 MiB.

```
[root@serverX ~]# lvextend -L 700M /dev/shazam/storage
Extending logical volume storage to 700.00 MiB
Logical volume storage successfully resized
```



nota

En nuestro ejemplo, especificamos el tamaño exacto para hacer el LV final, pero también podríamos haber usado:

- **-L +300M** para agregar el nuevo espacio usando el tamaño en MiB.
- **-l 175** para especificar el número total de extensiones (175 PE x 4 MiB).
- **-l +75** para agregar las extensiones adicionales necesarias.

6. Modificar el tamaño del sistema de archivos

Use **xfs_growfs** para ampliar el sistema de archivos XFS hasta el resto del espacio libre del LV.

```
[root@serverX ~]# xfs_growfs /storage
meta-data=/dev/mapper/shazamstorage  isize=256    agcount=4, agsize=25600 blks
...
```

7. Verificar la disponibilidad del contenido y el nuevo tamaño del sistema de archivos

Use **df** y **ls | wc** para revisar el nuevo tamaño del sistema de archivos y verifique que los archivos existentes aún estén presentes.

```
[root@serverX ~]# df -h /storage
Filesystem           Size   Used  Avail Use% Mounted on
/dev/mapper/shazam-storage 684M   21M  663M   3% /storage
[root@serverX ~]# ls /storage | wc -l
47
```

Los archivos aún están allí y el sistema de archivos tiene el tamaño esperado.

Trabajo de laboratorio: Administración del almacenamiento de gestión de volúmenes lógicos (LVM)

En este trabajo de laboratorio, modificará el tamaño de un volumen lógico existente, agregará recursos de LVM según sea necesario, y luego agregará un nuevo volumen lógico con un sistema de archivos XFS montado de manera persistente en este.

Recursos:		
Máquinas:	serverX	

Resultados:

- Volumen lógico **loans** con tamaño modificado a 768 MiB y montado de forma persistente en **/finance/loans**.
- Un nuevo volumen lógico de 128 MiB denominado **risk** con un sistema de archivos XFS, montado de forma persistente en **/finance/risk**.

Antes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

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

- Abra una terminal.
- Cambie a **root** usando **sudo -i**.

El departamento de finanzas de su empresa tiene un volumen lógico denominado **loans** que está empezando a ejecutarse sin espacio en el disco, y se le ha solicitado a usted que amplíe el espacio a un tamaño de 768 MiB.

También se le ha solicitado crear un nuevo sistema de archivos para alojar documentos para el equipo de administración de riesgos, que es parte del departamento de finanzas; se ha acordado un volumen lógico de 128 MiB denominado **risk** y debe montarse en **/finance/risk**. El sistema de archivos estándar de su empresa es XFS.

Hay un grupo de volúmenes denominado **finance** usado para alojar volúmenes lógicos del departamento, pero desafortunadamente no tiene espacio suficiente para ampliar el volumen lógico existente y agregar uno nuevo, de modo que a usted se le han asignado 512 MiB más desde el disco duro actual. Se debe crear la partición.

Cuando haya finalizado, reinicie su máquina **serverX**, y luego ejecute el comando **lab lvm grade** desde su máquina **serverX** para verificar su trabajo.

- Cree una partición de 512 MiB en **/dev/vdb**; inicialícela como un volumen físico y amplíe el grupo de volúmenes **finance** con esta.

Capítulo 12. Administración de volúmenes lógicos

2. Amplíe el volumen lógico **loans** a 768 MiB, que incluye el sistema de archivos.
3. En el grupo de volúmenes existente, cree un nuevo volumen lógico denominado **risk** de un tamaño de 128 MiB. Agregue un sistema de archivos XFS y móntelo de forma persistente en **/finance/risk**.
4. Cuando haya finalizado, reinicie su máquina **serverX**, y luego ejecute el comando **labc lvm grade** desde su máquina **serverX** para verificar su trabajo.

Solución

En este trabajo de laboratorio, modificará el tamaño de un volumen lógico existente, agregará recursos de LVM según sea necesario, y luego agregará un nuevo volumen lógico con un sistema de archivos XFS montado de manera persistente en este.

Recursos:	
Máquinas:	serverX

Resultados:

- Volumen lógico **loans** con tamaño modificado a 768 MiB y montado de forma persistente en **/finance/loans**.
- Un nuevo volumen lógico de 128 MiB denominado **risk** con un sistema de archivos XFS, montado de forma persistente en **/finance/risk**.

Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

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

- Abra una terminal.
- Cambie a **root** usando **sudo -i**.

El departamento de finanzas de su empresa tiene un volumen lógico denominado **loans** que está empezando a ejecutarse sin espacio en el disco, y se le ha solicitado a usted que amplíe el espacio a un tamaño de 768 MiB.

También se le ha solicitado crear un nuevo sistema de archivos para alojar documentos para el equipo de administración de riesgos, que es parte del departamento de finanzas; se ha acordado un volumen lógico de 128 MiB denominado **risk** y debe montarse en **/finance/risk**. El sistema de archivos estándar de su empresa es XFS.

Hay un grupo de volúmenes denominado **finance** usado para alojar volúmenes lógicos del departamento, pero desafortunadamente no tiene espacio suficiente para ampliar el volumen lógico existente y agregar uno nuevo, de modo que a usted se le han asignado 512 MiB más desde el disco duro actual. Se debe crear la partición.

Cuando haya finalizado, reinicie su máquina **serverX**, y luego ejecute el comando **lab lvm grade** desde su máquina **serverX** para verificar su trabajo.

- Cree una partición de 512 MiB en **/dev/vdb**; inicialícela como un volumen físico y amplíe el grupo de volúmenes **finance** con esta.
 - Use **fdisk** para crear una partición de 512 MiB y configúrela con el tipo Linux LVM.

```
[root@serverX ~]# fdisk /dev/vdb
```

Nota: Los siguientes pasos omiten algunos resultados.

Capítulo 12. Administración de volúmenes lógicos

- 1.2. Agregue una nueva partición primaria de 512 MiB.

```
Command (m for help): n
Partition type:
  p  primary (1 primary, 0 extended, 3 free)
  e  extended
Select (default p): Enter
Partition number (2-4, default 2): Enter
First sector (1050624-20971519, default 1050624): Enter
Last sector, +sectors or +size{K,M,G} (1050624-20971519, default
20971519): +512M
```

- 1.3. Cambie el tipo de partición a *Linux LVM* - 0x8e.

```
Command (m for help): t
Partition number (1,2, default 2): Enter
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'
```

- 1.4. Escriba los cambios en la tabla de particiones y salga.

```
Command (m for help): w
The partition table has been altered!
```

- 1.5. Use **partprobe** para registrar la nueva partición con el kernel.

```
[root@serverX ~]# partprobe
```

- 1.6. Use **pvcreate** para agregar la partición como un PV.

```
[root@serverX ~]# pvcreate /dev/vdb2
Physical volume "/dev/vdb2" successfully created
```

- 1.7. Use **vgextend** para ampliar el VG denominado **finance**, usando el nuevo PV **/dev/vdb2**.

```
[root@serverX ~]# vgextend finance /dev/vdb2
Volume group "finance" successfully extended
```

2. Amplíe el volumen lógico **loans** a 768 MiB, que incluye el sistema de archivos.

- 2.1. Use **lvextend** para ampliar el LV **loans** a 768 MiB.

```
[root@serverX ~]# lvextend -L 768M /dev/finance/loans
Extending logical volume loans to 768.00 MiB
Logical volume loans successfully resized
```



nota

De forma alternativa, podría haber usado **-L +512M** para modificar el tamaño del LV.

- 2.2. Use **xfs_growfs** para ampliar el sistema de archivos XFS hasta el resto del espacio libre del LV.

```
[root@serverX ~]# xfs_growfs /finance/loans
meta-data=/dev/mapper/finance-loans isize=256    agcount=4, agsize=16384 blks
...
```



nota

En este ejemplo, se muestra el paso **xfs_growfs** para ampliar el sistema de archivos. Una alternativa hubiese sido agregar la opción "**-r**" al comando **lvextend**.

3. En el grupo de volúmenes existente, cree un nuevo volumen lógico denominado **risk** de un tamaño de 128 MiB. Agregue un sistema de archivos XFS y móntelo de forma persistente en **/finance/risk**.
- 3.1. Use **lvcreate** para crear un LV de 128 MiB denominado **risk** desde el VG **finance**.

```
[root@serverX ~]# lvcreate -n risk -L 128M finance
Logical volume "risk" created
```

- 3.2. Use **mkfs** para colocar un sistema de archivos **xfs** en el LV **risk**; use el nombre del dispositivo del LV.

```
[root@serverX ~]# mkfs -t xfs /dev/finance/risk
meta-data=/dev/finance/risk      isize=256    agcount=4, agsize=8192 blks
...
```

- 3.3. Use **mkdir** para crear un punto de montaje en **/finance/risk**.
 - 3.4. Use **vim** para agregar la siguiente línea en la parte inferior de **/etc/fstab** en serverX:
- ```
/dev/finance/risk /finance/risk xfs defaults 1 2
```
- 3.5. Use **mount** para verificar la entrada **/etc/fstab** y monte el nuevo dispositivo del LV **risk**.

```
[root@serverX ~]# mount -a
```

4. Cuando haya finalizado, reinicie su máquina **serverX**, y luego ejecute el comando **lab lvm grade** desde su máquina **serverX** para verificar su trabajo.

- 4.1. [root@serverX ~]\$ systemctl reboot

- 4.2. [student@serverX ~]\$ lab lvm grade

# Resumen

## Gestión de volúmenes lógicos

- **pvcREATE, pVREMOVE y pVDISPLAY** crean, eliminan y detallan volúmenes físicos (PV).
- **VGCREATE, VGREMOVE y VGDISPLAY** crean, eliminan y detallan grupos de volúmenes (VG).
- **lVCREATE, LVREMOVE y LVDISPLAY** crean, eliminan y detallan volúmenes lógicos (LV).
- La adición de volúmenes lógicos se realiza en el orden PV, VG y LV.
- La eliminación de volúmenes lógicos se realiza en el orden LV, VG y PV.

## Extensión de volúmenes lógicos

- Ampliar un grupo de volúmenes (VG) usando **pvcREATE** y **VGEXTEND**; usar **VGDISPLAY** para comprobar los resultados.
- Reducir un VG usando **PVMOVE** y **VGREDUCE**.
- Ampliar un volumen lógico (LV) usando **LVEXTEND**.
- Usar **XFS\_GROWFS** para cambiar el tamaño de sistemas de archivos **XFS**.
- Usar **RESIZE2FS** para cambiar el tamaño de sistemas de archivos **EXT4**.





## CAPÍTULO 13

# PROCESOS PROGRAMADOS

| Descripción general |                                                                                                                                                                           |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Meta</b>         | Programar tareas para que se ejecuten automáticamente en el futuro.                                                                                                       |
| <b>Objetivos</b>    | <ul style="list-style-type: none"><li>• Programar trabajos recurrentes con cron.</li><li>• Administrar archivos temporales.</li></ul>                                     |
| <b>Secciones</b>    | <ul style="list-style-type: none"><li>• Programación de trabajos recurrentes con cron (y práctica)</li><li>• Administración de archivos temporales (y práctica)</li></ul> |

# Programación de trabajos cron del sistema

## Objetivos

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

- Programar tareas de sistemas recurrentes.

## Trabajos cron del sistema

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

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

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

```
For details see man 4 crontabs

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

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

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



### Importante

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

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

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

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

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

Una vez cada cuántos días debe ejecutarse este trabajo.

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

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

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

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

- **Command (Comando)**

El comando que se ejecutará.

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



## Referencias

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

# Práctica: Programación de trabajos cron del sistema

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

| Recursos         |                                                                                                                                                                                       |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Archivos:</b> | <ul style="list-style-type: none"> <li>• <code>/etc/crontab</code></li> <li>• <code>/etc/cron.d/*</code></li> <li>• <code>/etc/cron.{hourly,daily,weekly,monthly}/*</code></li> </ul> |
| <b>Máquinas:</b> | <code>desktopX</code>                                                                                                                                                                 |

## Resultados

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

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

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

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

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

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

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

Inserte lo siguiente en su editor:

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

- 2.3. Haga el script ejecutable:

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

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

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

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

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

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

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

**/etc/cron.d/sysstat** parece prometedor.

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

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

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

3.5. Guarde sus cambios y salga.

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

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

# Administración de archivos temporales

## Objetivos

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

## Administración de archivos temporales con **systemd-tmpfiles**

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

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

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

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

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

### Limpieza regular

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

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

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

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

```
OnUnitActiveSec=1d
```

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

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



## Importante

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

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

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

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

## Archivos de configuración systemd-tmpfiles

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

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

Algunos ejemplos con explicaciones:

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

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

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

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

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

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

### Precedencia de archivos de configuración

Los archivos de configuración pueden estar en tres lugares:

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

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

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

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



### nota

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



### Referencias

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

# Práctica: Administración de archivos temporales

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

| Recursos         |                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Archivos:</b> | <ul style="list-style-type: none"> <li>• <b>/etc/tmpfiles.d/</b></li> <li>• <b>/usr/lib/tmpfiles.d/tmp.conf</b></li> </ul> |
| <b>Máquinas:</b> | <b>serverX</b>                                                                                                             |

## Resultados:

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

### Antes de comenzar

Restablezca su sistema **serverX**.

En producción, se han presentado varios problemas:

- **/tmp** se queda sin espacio en disco. Parece que permitir que los archivos estén 10 días en desuso antes de eliminarlos no es adecuado para su sitio. Ha determinado que eliminar archivos luego de cinco días de desuso es aceptable.

- Su daemon de búsqueda de desplazamiento del tiempo **gallifrey** necesita un directorio temporal por separado denominado **/run/gallifrey**. Los archivos en este directorio deben purgarse automáticamente luego de haber estado en desuso durante más de 30 segundos. Solo **root** debe tener acceso de lectura y escritura a **/run/gallifrey**.

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

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

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

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

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

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

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

## Capítulo 13. Procesos programados

---

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

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

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

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

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

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

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

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

- 6.2. Espere al menos 30 segundos.

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

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

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

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

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

# Resumen

## Programación de trabajos cron del sistema

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

## Administración de archivos temporales

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





## CAPÍTULO 14

# MONTAJE DE SISTEMAS DE ARCHIVOS DE RED

| Descripción general           |                                                                                                                                                                                                                                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Meta</b>                   | Usar <code>autofs</code> y la línea de comandos para montar y desmontar el almacenamiento de red con NFS y SMB.                                                                                                                           |
| <b>Objetivos</b>              | <ul style="list-style-type: none"><li>Montar, acceder y desmontar almacenamiento de red con NFS.</li><li>Automontaje y acceso a almacenamiento de red con NFS.</li><li>Montar, automontar y desmontar sistemas de archivos SMB.</li></ul> |
| <b>Secciones</b>              | <ul style="list-style-type: none"><li>Montaje de almacenamiento de red con NFS (y práctica)</li><li>Automontaje de almacenamiento de red con NFS (y práctica)</li><li>Acceso a almacenamiento de red con SMB (y práctica)</li></ul>       |
| <b>Trabajo de laboratorio</b> | <ul style="list-style-type: none"><li>Acceso a almacenamiento de red con el sistema de archivos de red (NFS)</li><li>Acceso a almacenamiento de red con SMB</li></ul>                                                                     |

# Montaje de almacenamiento de red con NFS

## Objetivos

Luego de finalizar esta sección, los estudiantes deberán poder montar, acceder y desmontar manualmente un recurso compartido de NFS.

## Montaje y desmontaje manual de archivos compartidos de NFS

NFS, el *sistema de archivos de red*, es un protocolo estándar de Internet usado por Linux, UNIX y sistemas operativos similares como su sistema de archivos de red nativo. Es una extensión abierta y activa bajo un estándar que admite características nativas de sistemas de archivos y permisos de Linux.

Red Hat Enterprise Linux 7 admite NFSv4 (versión 4 del protocolo) de forma predeterminada y, si no está disponible, recurre automáticamente a NFSv3 y NFSv2. NFSv4 utiliza el protocolo TCP para comunicarse con el servidor, mientras las versiones anteriores de NFS pueden usar TCP o UDP.

Los servidores de NFS *exportan* recursos compartidos (directorios) y los clientes de NFS montan los recursos compartidos en un punto de montaje local (directorio). El punto de montaje local debe existir. Los recursos compartidos de NFS se pueden montar de diversas maneras:

- montar manualmente un recurso compartido de NFS usando el comando **mount**.
- montar automáticamente un recurso compartido de NFS en el arranque usando **/etc/fstab**.
- montar un recurso compartido de NFS a pedido a través de un proceso conocido como *automontaje*.

### Protección del acceso a archivos con recursos compartidos de NFS

Los servidores NFS protegen el acceso a archivos usando varios métodos: **none**, **sys**, **krb5**, **krb5i** y **krb5p**. El servidor NFS puede elegir ofrecer un único método o varios métodos para cada recurso compartido exportado. Los clientes NFS deben conectarse al recurso compartido exportado usando uno de los métodos obligatorios para ese recurso compartido, especificado como una opción de montaje **sec=method**.

### Métodos de protección

- **none**: Acceso anónimo a los archivos, a las escrituras en el servidor (si está permitido) se les asignará UID y GID de **nfsnobody**.
- **sys**: Acceso a archivos basado en los permisos de archivos Linux estándares para valores de UID y GID. Si no se especifica, este es el valor predeterminado.
- **krb5**: los clientes deben probar su identidad mediante Kerberos, y luego se aplican los permisos de archivos de Linux estándares.
- **krb5i**: agrega criptográficamente una garantía sólida de que los datos de cada solicitud aún no han sido utilizados de forma indebida.

- **krb5p:** agrega un cifrado a todas las solicitudes entre el cliente y el servidor, lo que evita la exposición de los datos en la red. Esto tendrá un impacto en el rendimiento.



## Importante

Las opciones de Kerberos requerirán, como mínimo, **/etc/krb5.keytab** y una configuración de autenticación adicional que no está cubierta en esta sección (que se une al dominio de Kerberos). Normalmente, **/etc/krb5.keytab** será proporcionado por el administrador de autenticación o de seguridad. Solicite una **keytab** que incluya un *director de host*, *director de nfs* o (idealmente) ambos.

NFS usa el servicio **nfs-secure** para ayudar a negociar y administrar la comunicación con el servidor al conectarse a recursos compartidos protegidos por Kerberos. Se debe ejecutar para usar los recursos compartidos de NFS protegidos; **inícielo** y **habilitelo** para asegurarse de que siempre esté disponible.

```
[student@desktopX ~]$ sudo systemctl enable nfs-secure
ln -s '/usr/lib/systemd/system/nfs-secure.service' ...
[student@desktopX ~]$ sudo systemctl start nfs-secure
```



## nota

El servicio **nfs-secure** es parte del paquete **nfs-utils**, que debe instalarse de forma predeterminada. Si no está instalado, use:

```
[student@desktopX ~]$ sudo yum -y install nfs-utils
```

## Montar un recurso compartido de NFS

Son tres los pasos básicos para montar un recurso compartido de NFS:

1. **Identificar:** El administrador del servidor NFS puede proporcionar detalles de exportación, incluidos los requisitos de seguridad. De forma alternativa:

Los recursos compartidos de NFSv4 se pueden identificar al montar la carpeta root del servidor NFS y al explorar los directorios exportados. Haga esto como **root**. El acceso a recursos compartidos que están usando Kerberos será denegado, pero el nombre del recurso compartido (directorio) estará visible. Otros directorios compartidos se podrán explorar.

```
[student@desktopX ~]$ sudo mkdir /mountpoint
[student@desktopX ~]$ sudo mount serverX:/ /mountpoint
[student@desktopX ~]$ sudo ls /mountpoint
```

Los recursos compartidos de NFSv2 y de NFSv3 se pueden descubrir mediante el uso de **showmount**.

```
[student@desktopX ~]$ showmount -e serverX
```

2. **Punto de montaje:** Use `mkdir -p` para crear un punto de montaje en una ubicación adecuada.

```
[student@desktopX ~]$ mkdir -p /mountpoint
```

3. **Montaje:** Hay dos opciones aquí: hacerlo de forma manual o que esté incorporado en el archivo `/etc/fstab`. Cambie a `root` o use `sudo` para cualquiera de las dos operaciones.

- *Manual:* Use el comando `mount`.

```
[student@desktopX ~]$ sudo mount -t nfs -o sync serverX:/share /mountpoint
```

La opción `-t nfs` es el tipo de sistema de archivos para recursos compartidos de NFS (no es estrictamente obligatorio, se muestra para ofrecer una visión completa). La opción `-o sync` indica a `mount` sincronizar inmediatamente las operaciones de escritura con el servidor NFS (el valor predeterminado es asíncrono). Se usará el método de protección predeterminado (`sec=sys`) para intentar montar el recurso compartido de NFS, usando permisos de archivos Linux estándares.

- */etc/fstab:* Use `vim` para editar el archivo `/etc/fstab` y agregar la entrada de montaje en la parte inferior del archivo. El recurso compartido de NFS se montará en cada arranque del sistema.

```
[student@desktopX ~]$ sudo vim /etc/fstab
...
serverX:/share /mountpoint nfs sync 0 0
```

Use `umount`, usando los privilegios `root`, para desmontar manualmente el recurso compartido.

```
[student@desktopX ~]$ sudo umount /mountpoint
```

## Referencias

Páginas del manual: `mount(8)`, `umount(8)`, `fstab(5)` y `mount .nfs(8)`.

# Práctica: Montaje y desmontaje de NFS

En este trabajo de laboratorio, montará manualmente un recurso compartido de NFS protegido por Kerberos, accederá a este y, opcionalmente, lo desmontará. Cree un montaje de recurso compartido persistente en /etc/fstab, móntelo y acceda a este. serverX es el host de NFSv4.

| <b>Recursos:</b> |                                                   |
|------------------|---------------------------------------------------|
| <b>Archivos:</b> | <b>nfs_ldapuserX.txt</b> y <b>nfs_student.txt</b> |
| <b>Máquinas:</b> | desktopX y serverX                                |

## Resultados:

- El usuario **ldapuserX** podrá de forma satisfactoria iniciar sesión en el recurso compartido de NFS **public** montado de forma persistente en **/mnt/public**, y acceder a este.
- El recurso compartido de NFS **manual** puede ser montado por usuarios ad hoc en **/mnt/manual**.

## Andes de comenzar

- Restablezca el sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

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

- Restablezca el sistema desktopX.
- Inicie sesión en su sistema de escritorio y configúrelo.

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

- Abra una terminal.



## Importante

La configuración de serverX se utiliza para los ejercicios prácticos de este capítulo. Solo debe ejecutarse una vez.

S.H.I.E.L.D. (Storage Hardware Incorporating Every Last Document, hardware de almacenamiento que incorpora cada último documento) usa un servidor central, serverX, para alojar varios directorios compartidos con documentos. El acceso a la mayoría de los directorios es mediante usuarios basados en LDAP, que se autentican con Kerberos; no obstante, varios directorios compartidos están usando seguridad para el acceso a archivos Linux estándar. Los usuarios deben poder iniciar sesión en el recurso compartido de NFS **manual** y montarlo, y deben tener el recurso compartido de NFS **public** disponible constantemente.

## Capítulo 14. Montaje de sistemas de archivos de red

---

A continuación, se proporcionan los detalles que necesitará:

- Nombre de usuario: **ldapuserX**
  - Contraseña: **kerberos**
  - serverX comparte los dos directorios en **/shares: manual y public**.
  - Punto de montaje de desktopX: **/mnt/public** y **/mnt/manual**
  - El recurso compartido de NFS **public** requiere autenticación de **krb5p** para el acceso; **manual** usa la seguridad **sys**.
  - **krb5.keytab** está disponible en **http://classroom.example.com/pub/keytabs/&dsk;.keytab**.
  - Cada recurso compartido debe tener acceso de lectura y escritura.
1. Descargue e instale el archivo **krb5.keytab** para habilitar el acceso a Kerberos y su seguridad.

```
[student@desktopX ~]$ sudo wget -O /etc/krb5.keytab http://classroom.example.com/pub/keytabs/desktopX.keytab
```

2. Habilite e inicie el servicio **nfs-secure**.

```
[student@desktopX ~]$ sudo systemctl enable nfs-secure
ln -s '/usr/lib/systemd/system/nfs-secure.service' ...
[student@desktopX ~]$ sudo systemctl start nfs-secure
```

3. Use **mkdir** para crear ambos puntos de montaje: **/mnt/public** y **/mnt/manual**.

```
[student@desktopX ~]$ sudo mkdir -p /mnt/{public,manual}
```

4. Cree el montaje persistente. Este montaje solo será accesible para usuarios autenticados.

- 4.1. Use **vim** para editar el archivo **/etc/fstab**.

```
[student@desktopX ~]$ sudo vim /etc/fstab
```

Agregue esta línea al final del archivo:

```
serverX:/shares/public /mnt/public nfs sec=krb5p,sync 0 0
```

- 4.2. Use **mount** para montar el recurso compartido y comenzar a usarlo.

```
[student@desktopX ~]$ sudo mount -a
```

5. Use **mount** para montar manualmente **/shares/manual** en **/mnt/manual**. Debido a que ya tiene un montaje NFSv4 protegido por Kerberos del mismo servidor, deberá especificar la opción **sec=sys**.

```
[student@desktopX ~]$ sudo mount -o sync,sec=sys serverX:/shares/manual /mnt/manual
```

6. Use **ssh** para cambiar a **ldapuserX** en **localhost** y confirme los montajes, y el acceso de lectura/escritura.

6.1. Use **ssh** para iniciar sesión como **ldapuserX**.

```
[student@desktopX ~]$ ssh ldapuserX@localhost
```

Si observa algo similar a lo siguiente, escriba **yes** (sí) para aceptar y continuar.

```
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is d9:cc:73:82:3b:8a:74:e4:11:2f:f3:2b:03:a4:46:4d.
Are you sure you want to continue connecting (yes/no)? yes
```

Ingrese la contraseña: **kerberos**.

```
ldapuserX@localhost's password: kerberos
```

- 6.2. Verifique que puede cambiar a ambos directorios compartidos y confirme que tiene acceso de lectura/escritura.

Use **cd** para cambiar directorios.

```
[ldapuserX@desktopX ~]$ cd /mnt/manual
```

Use **echo** y **cat** para verificar el acceso de lectura y escritura.

```
[ldapuserX@desktopX manual]$ echo hello > test.txt
[ldapuserX@desktopX manual]$ cat test.txt
hello
```

Repita este paso para evaluar **/mnt/public**.

Use **exit** o **Ctrl+D** para cerrar sesión de **ldapuserX**.

- 6.3. Repita el paso anterior como **student** en ambos directorios. Debe poder cambiar de directorio y detallar **/mnt/manual**, pero obtendrá un **permiso denegado** en **/mnt/public** porque **student** no puede autenticar mediante Kerberos.

En lugar de **test.txt**, se recomienda que utilice algo como **test2.txt**, dado que **student** no tiene permiso para escribir archivos que son propiedad de **ldapuserX**.



### nota

Cuando haya terminado de utilizar el almacenamiento de red, puede usar el comando **umount** para desmontar manualmente los archivos compartidos de NFS.

```
[student@desktopX ~]$ sudo umount /mnt/manual
```

# Automontaje de almacenamiento de red con NFS

## Objetivos

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

- Describir los beneficios de usar el servicio de automontaje.
- Automontar los recursos compartidos de NFS usando asignaciones directas e indirectas, incluidos comodines.

## Montaje de recursos compartidos de NFS con el servicio de automontaje

El servicio de automontaje es un servicio (**autofs**) que puede montar automáticamente recursos compartidos de NFS "a pedido", y desmontará automáticamente recursos compartidos de NFS cuando ya no se usen.

### Beneficios del servicio de automontaje

- Los usuarios no necesitan tener privilegios *root* para ejecutar los comandos **mount/umount**.
- Los recursos compartidos de NFS configurados en el servicio de automontaje están disponibles para todos los usuarios de la máquina, sujetos a los permisos de acceso.
- Los recursos compartidos de NFS no están conectados permanentemente como las entradas en **/etc/fstab**, lo que libera recursos de red y sistemas.
- El servicio de automontaje se configura completamente del lado del cliente; no se requiere configuración del lado del servidor.
- El servicio de automontaje usa las mismas opciones de montaje usadas por el comando **mount**, incluidas opciones de seguridad.
- Apoyo tanto para la asignación de puntos de montaje directos como indirectos, lo que proporciona flexibilidad en las ubicaciones de los puntos de montaje.
- Los puntos de montaje indirectos se crean y se eliminan mediante **autofs**, lo que alivia las necesidades de administrarlos manualmente.
- NFS es el sistema de archivos predeterminado para el servicio de automontaje, pero se puede usar para automontar un rango de diferentes sistemas de archivos.
- **autofs** es un servicio que se administra como otros servicios del sistema.

### Crear un automontaje

La configuración de un automontaje es un proceso de varios pasos:

1. Instale el paquete **autofs**.

```
[student@desktopX ~]$ sudo yum -y install autofs
```

## Capítulo 14. Montaje de sistemas de archivos de red

---

Este paquete contiene todo lo necesario para usar el servicio de automontaje para recursos compartidos de NFS.

2. Agregue un archivo de *asignación maestra* a **/etc/auto.master.d**; este archivo identifica el directorio base usado para puntos de montaje e identifica el archivo de asignación usado para crear los automontajes.

Use **vim** para crear y editar el archivo de asignación maestra:

```
[student@desktopX ~]$ sudo vim /etc/auto.master.d/demo.autofs
```

El nombre del archivo de asignación maestra no es importante; pero, normalmente, es algo útil. El único requisito es que debe tener una extensión de **.autofs**. El archivo de asignación maestra puede contener varias entradas de asignación, o usar múltiples archivos para datos de configuración independientes.

Agregue la entrada de asignación maestra, en este caso, para montajes asignados indirectamente:

```
/shares /etc/auto.demo
```

Esta entrada usaría el directorio **/shares** como la base para futuros automontajes indirectos. El archivo **/etc/auto.demo** contiene los detalles de montaje; use un nombre de archivo absoluto. El archivo **auto.demo** debe crearse antes de comenzar el servicio **autofs**.

Para usar directamente puntos de montajes asignados, agregue una entrada en el mismo archivo (o en un archivo por separado):

```
/- /etc/auto.direct
```

Todas las entradas de asignación directa usan "**/-**" como el directorio base. En este caso, el archivo de asignación que contiene los detalles de montaje es **/etc/auto.direct**.

3. Cree los archivos de asignación. El archivo de asignación identifica el punto de montaje, las opciones de montaje y la ubicación de origen que se montará.

Use **vim** para crear y editar el archivo de asignación:

```
[student@desktopX ~]$ sudo vim /etc/auto.demo
```

El nombre del archivo no es importante, pero por convención se ubica en **/etc** y se llama **auto.name**, donde el *nombre* es significativo del contenido incluido.

```
work -rw, sync serverX:/shares/work
```

El formato de una entrada es *punto de montaje, opciones de montaje y ubicación de origen*. En este ejemplo, se muestra una entrada de asignación indirecta básica. Las asignaciones directas y las asignaciones indirectas que usan comodines se tratarán más adelante en esta sección.

- Conocido como la "*clave*" en las páginas del manual, el *punto de montaje* será creado y eliminado automáticamente por el servicio **autofs**. En este caso, el punto de montaje totalmente calificado será **/shares/work**; consulte el archivo de asignación maestra. El directorio **/shares** y el directorio **work** se crearán y eliminarán según sea necesario mediante el servicio **autofs**.

En este ejemplo, el punto de montaje local refleja la estructura del directorio del servidor. El punto de montaje local puede tener cualquier nombre. No hay requisitos relativos a la alineación de los nombres del punto de montaje local y la estructura del directorio del servidor.

- Las *opciones de montaje* comienzan con un "-" (guión) y están separadas por comas sin espacios en blanco. Las opciones de montaje disponibles son las mismas que las disponibles para el comando de montaje manual equivalente. En este ejemplo, el servicio de automontaje intentará y montará el recurso compartido usando el acceso de lectura/escritura, la seguridad se basará en permisos de archivos Linux estándares (el predeterminado: sec=sys) y el servidor será sincronizado inmediatamente durante las operaciones de escritura.

Hay un par de opciones útiles específicas del servicio de automontaje: **-fstype=y** - **strict**. Use **fstype** para especificar el sistema de archivos si no es NFS y use **strict** para tratar errores, cuando monte sistemas de archivos, como graves.

- La *ubicación de origen* para los recursos compartidos de NFS sigue el patrón **host:/ pathname**; en este ejemplo, **&srv;:/shares/work**. Este directorio deberá haber sido *exportado* en serverX con soporte de acceso de lectura/escritura y permisos de archivos Linux estándares para que el montaje sea exitoso.

Si el sistema de archivos que se montará comienza con una "/" (barra), como entradas de dispositivos locales o recursos compartidos SMB, es necesario agregar delante ":" (dos puntos); por ejemplo, un recurso compartido SMB sería **:/&srv;/share**.

#### 4. Inicie y habilite el servicio de automontaje.

Use **systemctl** tanto para iniciar como para habilitar el servicio **autofs**.

```
[student@desktopx ~]$ sudo systemctl enable autofs
ln -s '/usr/lib/systemd/system/autofs.service' ...
[student@desktopx ~]$ sudo systemctl start autofs
```

#### El archivo de asignación: asignaciones directas

Como su nombre lo implica, las asignaciones directas se usan para asignar un recurso compartido de NFS a un punto de montaje existente. El servicio de automontaje no intentará crear el punto de montaje automáticamente; debe existir antes de que el servicio **autofs** se inicie.

Para continuar con el ejemplo anterior, el contenido del archivo **/etc/auto.direct** podría verse del siguiente modo:

```
/mnt/docs -rw, sync serverX:/shares/docs
```

El punto de montaje (o clave) siempre es una ruta absoluta, que comienza con una "/" (barra). El resto del archivo de asignación usa la misma estructura.

Sólo el directorio más a la derecha se coloca bajo el control del servicio de automontaje. Así, la estructura del directorio sobre el punto de montaje (`/mnt` en este ejemplo) no queda oculta por **autofs**.

### El archivo de asignación: asignaciones indirectas de comodines

Cuando un servidor NFS exporta varios subdirectorios dentro de un directorio, el servicio de automontaje se puede configurar para acceder a cualquiera de esos subdirectorios usando una única entrada de asignación. Como ejemplo, esto puede ser realmente útil para montar automáticamente directorios de *inicio* para usuarios desde un servidor NFS.

Para continuar con el ejemplo anterior, si `&srv;:/shares` exporta dos o más subdirectorios y se puede acceder a estos usando las mismas opciones de montaje, el contenido del archivo `/etc/auto.demo` podría verse del siguiente modo:

```
* -rw, sync serverX:/shares/&
```

El punto de montaje (o clave) es un "\*" (asterisco) y el subdirectorio en la ubicación de origen es el símbolo "&". Todo lo demás en la entrada es igual.

Cuando un usuario intenta acceder a `/shares/work`, la clave \* (que es `work` en este ejemplo) reemplazará el símbolo & en la ubicación de origen y `&srv;:/shares/work` se montará. Al igual que con el ejemplo indirecto, el servicio **autofs** creará y eliminará automáticamente el directorio `work`.

## Referencias

Páginas del manual: **autofs(5)**, **automount(8)**, **auto.master(5)** y **mount.nfs(8)**

# Práctica: Automontaje de NFS

En este trabajo de laboratorio, instalará un paquete para admitir el automontaje. Cree un automontaje de asignación directa y un automontaje de asignación indirecta usando comodines. serverX es el host NFSv4.

| <b>Recursos:</b> |                           |
|------------------|---------------------------|
| <b>Archivos:</b> | <b>nfs_ldapuserX.txt</b>  |
| <b>Máquinas:</b> | <b>desktopX y serverX</b> |

## Resultados:

El usuario **ldapuserX** podrá iniciar sesión satisfactoriamente y usará los tres directorios automontados.

### Antes de comenzar

- Restablezca el sistema desktopX.
- Inicie sesión en su sistema de escritorio y configúrelo.

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

- Abra una terminal.



## Importante

La configuración de serverX realizada al comienzo de "Montaje y desmontaje de NFS" también se utiliza para este ejercicio práctico. Si aún no ha realizado la configuración del servidor, ejecútelo ahora. Solo debe ejecutarse una vez para ambos ejercicios de práctica.

S.H.I.E.L.D. (Storage Hardware Incorporating Every Last Document, hardware de almacenamiento que incorpora cada último documento) usa un servidor central, serverX, para alojar varios directorios compartidos con documentos. El acceso a estos directorios es a través de usuarios basados en LDAP, y se autentica el uso de Kerberos con cifrado. Los usuarios deben poder iniciar sesión y que los directorios compartidos se automonten con acceso de lectura y escritura, listos para su uso.

A continuación, se proporcionan los detalles que necesitará:

- Nombre de usuario: **ldapuserX**
- Contraseña: **kerberos**
- serverX comparte tres directorios en **/shares: docs, work y public**.
- El acceso a los archivos está protegido mediante el uso de Kerberos con cifrado: **krb5p**.
- Punto de montaje de desktopX: **/shares** para **docs** y **work** y una asignación directa de **public** a **/mnt/public**.

- **krb5.keytab** está disponible en <http://classroom.example.com/pub/keytabs/&dsk;.keytab>.
- Cada recurso compartido debe tener acceso de lectura y escritura.

Cuando haya finalizado su trabajo, reinicie la máquina **desktopX**, luego ejecute el comando **lsb nfsmount grade** desde la máquina **desktopX** para verificar el trabajo.

1. Descargue e instale el archivo **krb5.keytab** para habilitar el acceso a Kerberos y su seguridad.

```
[student@desktopX ~]$ sudo wget -O /etc/krb5.keytab http://classroom.example.com/pub/keytabs/desktopX.keytab
```

2. Habilite e inicie el servicio **nfs-secure**.

```
[student@desktopX ~]$ sudo systemctl enable nfs-secure
ln -s '/usr/lib/systemd/system/nfs-secure.service' ...
[student@desktopX ~]$ sudo systemctl start nfs-secure
```

3. Use **yum** para instalar **autofs**, necesario para automontar directorios.

```
[student@desktopX ~]$ sudo yum -y install autofs
Loaded plugins: langpacks
Resolving Dependencies
...
Complete!
```

4. Cree los archivos de configuración de automontaje para el automontaje de *asignación directa*.

- 4.1. Use **vim** para crear y editar el archivo **/etc/auto.master.d/direct.autofs**.

```
[student@desktopX ~]$ sudo vim /etc/auto.master.d/direct.autofs
```

**Nota:** La extensión de archivos debe ser **.autofs**.

Agregue la línea de la siguiente manera:

```
/ - /etc/auto.direct
```

- 4.2. Use **vim** para crear y editar el archivo de asignación **auto.direct**.

```
[student@desktopX ~]$ sudo vim /etc/auto.direct
```

Agregue la línea de la siguiente manera:

```
/mnt/public -rw, sync, sec=krb5p serverX:/shares/public
```

**Nota:** Los nombres de los archivos de arriba no son importantes; fueron elegidos de modo que sean significativos.

- 
5. Cree los archivos de configuración de automontaje para los automontajes de *asignación indirecta*.

- 5.1. Use **vim** para crear y editar el archivo **/etc/auto.master.d/shares.autofs**.

```
[student@desktopX ~]$ sudo vim /etc/auto.master.d/shares.autofs
```

**Nota:** La extensión de archivos debe ser **.autofs**.

Agregue la línea de la siguiente manera:

```
/shares /etc/auto.shares
```

- 5.2. Use **vim** para crear y editar el archivo de asignación **auto.shares**.

```
[student@desktopX ~]$ sudo vim /etc/auto.shares
```

Agregue la línea de la siguiente manera:

```
* -rw, sync, sec=krb5p serverX:/shares/&
```

**Nota:** Los nombres de los archivos de arriba no son importantes; fueron elegidos de modo que sean significativos.

6. Use **mkdir** para crear el punto de montaje **/mnt/public** para el automontaje de *asignación directa*.

```
[student@desktopX ~]$ sudo mkdir -p /mnt/public
```

7. Habilite e inicie el servicio de automontaje.

```
[student@desktopX ~]$ sudo systemctl enable autofs
ln -s '/usr/lib/systemd/system/autofs.service' ...
[student@desktopX ~]$ sudo systemctl start autofs
```

8. Use **ssh** para cambiar a **ldapuserX** en **localhost** y confirme los montajes, y el acceso de lectura/escritura.

- 8.1. Use **ssh** para iniciar sesión como **ldapuserX**.

```
[student@desktopX ~]$ ssh ldapuserX@localhost
```

Si observa algo similar a lo siguiente, escriba **yes** (sí) para aceptar y continuar.

```
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is d9:cc:73:82:3b:8a:74:e4:11:2f:f3:2b:03:a4:46:4d.
Are you sure you want to continue connecting (yes/no)? yes
```

Ingrese la contraseña: **kerberos**.

```
[ldapuserX@localhost ~]$ password: kerberos
```

- 8.2. Verifique que puede cambiar a los directorios compartidos automontados y confirme que tiene acceso de lectura/escritura.

Use **cd** para cambiar directorios.

```
[ldapuserX@desktopX ~]$ cd /shares/docs
```

Use **echo** y **cat** para verificar el acceso de lectura y escritura.

```
[ldapuserX@desktopX docs]$ echo hello > test.txt
[ldapuserX@desktopX docs]$ cat test.txt
hello
```

Repita este paso para evaluar **/shares/work** y **/mnt/public**.

Use **exit** o **Ctrl+D** para cerrar sesión de **ldapuserX**.

9. Reinicie la máquina **desktopX**, y luego, ejecute el comando **lab nfsmount grade** desde la máquina **desktopX** para verificar el trabajo.

9.1. 

```
[student@desktopX ~]$ sudo systemctl reboot
```

9.2. 

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

# Acceso a almacenamiento de red con SMB

## Objetivos

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

- Montar y desmontar sistemas de archivos SMB usando la línea de comandos.
- Automontar sistemas de archivos SMB.

## Montaje y desmontaje manual de sistemas de archivos SMB

Muchas organizaciones necesitan proporcionar almacenamiento de red e imprimir servicios para una variedad de sistemas operativos de escritorio. Red Hat Enterprise Linux usa el servidor Samba para proporcionar servicios que los clientes de Microsoft Windows pueden usar. Samba implementa el protocolo Server Message Block (SMB), y Common Internet File System (CIFS) es un dialecto de SMB. A menudo, los dos nombres se usan de forma intercambiable.

### Conexión a recursos compartidos de SMB/CIFS

Los escritorios y servidores de Red Hat se pueden conectar a recursos compartidos ofrecidos a través de *cualquier* servidor que use el protocolo SMB.

### Tres pasos básicos para acceder a un recurso compartido de SMB

1. *Identificar* el recurso compartido remoto al que se desea acceder.
2. *Determinar el punto de montaje* donde el recurso compartido debe montarse y crear el directorio vacío del punto de montaje.
3. *Montar* el sistema de archivos de red mediante un comando o cambio de configuración correspondiente.

Antes de comenzar, hay un paquete que se debe instalar para poder montar los recursos compartidos de SMB: **cifs-utils**. Tanto el comando **mount** como el servicio de automontaje de **autofs** requieren este paquete para montar los sistemas de archivos de CIFS.

Un segundo paquete, **samba-client**, tiene algunas utilidades de línea de comando útiles (por ejemplo, **smbclient**) y a menudo vale la pena instalarlo también.

### Montar un recurso compartido de SMB

1. **Identificación:** El administrador del host del servidor SMB puede proporcionar detalles del recurso compartido, como *nombre de usuario y contraseña*, nombres del *recurso compartido*, etc. Una alternativa es usar un cliente que puede navegar por los recursos compartidos, como **smbclient**.

```
[student@desktopX ~]$ smbclient -L //serverX
```

La opción **-L** pide a **smbclient** que detalle los recursos compartidos disponibles en serverX.

2. **Punto de montaje:** Use `mkdir -p /mountpoint`

```
[student@desktopX ~]$ mkdir -p /mountpoint
```

3. **Montaje:** Hay dos opciones aquí: hacerlo de forma manual o que esté incorporado en el archivo `/etc/fstab`. Cambie a `root` o use `sudo` para cualquiera de las dos operaciones.

- *Manual:* Use el comando `mount`.

```
[student@desktopX ~]$ sudo mount -t cifs -o guest //serverX/share /mountpoint
```

La opción `-t cifs` es el tipo de sistemas de archivos para recursos compartidos de SMB y la opción `-o guest` indica a `mount` que intente y se autentique como una cuenta de `guest` sin una contraseña.

- */etc/fstab:* Use `vim` para editar el archivo `/etc/fstab` y agregar la entrada de montaje en la parte inferior del archivo. El recurso compartido de SMB se montará en cada arranque del sistema.

```
[student@desktopX ~]$ sudo vim /etc/fstab
...
//serverX/share /mountpoint cifs guest 0 0
```

Use `umount`, usando los privilegios de `root`, para desmontar manualmente el recurso compartido.

```
[student@desktopX ~]$ sudo umount /mountpoint
```

### Autenticación de recursos compartidos de SMB

Los recursos compartidos de SMB se pueden marcar como no naveables, lo que significa que los clientes como `smbclient` no los mostrarán. Aún se puede acceder a los recursos compartidos de SMB al especificar explícitamente el nombre del recurso compartido durante la operación de montaje.

Generalmente, los servidores de SMB restringen el acceso a usuarios específicos o grupos de usuarios. El acceso a recursos compartidos requerirá la presentación de las credenciales adecuadas en el servidor SMB. Hay una variedad de métodos de autenticación que un servidor SMB puede elegir implementar, demasiados como para cubrirlos aquí.

Una opción común para la autenticación es el par **nombre de usuario y contraseña**. Estos se pueden agregar al comando `mount` (o la entrada `/etc/fstab`) o almacenar en un archivo de **credenciales** al que se deriva durante la operación de montaje. El comando `mount` solicitará una contraseña si no se la proporciona, pero debe ser proporcionada si se usa `/etc/fstab`. El acceso de guests puede solicitarse explícitamente con la opción `guest`.

*Algunos ejemplos:*

```
[student@desktopX ~]$ sudo mount -t cifs -o guest //serverX/docs /public/docs
```

Monte el recurso compartido de SMB `//&srv;/docs` en `/public/docs` e intente autenticarlo como `guest`.

```
[student@desktopX ~]$ sudo mount -t cifs -o username=watson //serverX/cases /bakerst/cases
```

Monte el recurso compartido de SMB `//&srv;/cases` en `/bakerst/cases` e intente autenticarlo como `watson`. El comando `mount` solicitará la contraseña en este ejemplo.

El archivo de **credenciales** ofrece una mejor seguridad porque la contraseña se almacena en un archivo más seguro, mientras que el archivo `/etc/fstab` se examina fácilmente.

```
[student@desktopX ~]$ sudo mount -t cifs -o credentials=/secure/sherlock //serverX/sherlock /home/sherlock/work
```

Monte el recurso compartido de SMB `//&srv;/sherlock` en `/home/sherlock/work` e intente autenticar con las credenciales almacenadas en `/secure/sherlock`.

El formato para el archivo de **credenciales** es:

```
username=username
password=password
domain=domain
```

Debe colocarse en alguna parte segura con solo acceso `root` (por ejemplo, `chmod 600`).

Durante las operaciones de archivos, el servidor SMB supervisará el acceso de archivos con las credenciales usadas para montar el recurso compartido. El cliente revisará el acceso de archivos con el UID/GID de los archivos enviados desde el servidor. Esto significa que el cliente deberá tener el mismo UID/GID y, si es necesario, la misma membresía de grupo complementaria que los archivos del servidor SMB.

Hay una cantidad de opciones de montaje que manejan métodos de autenticación alternativos y de comprobación del acceso local, como multiusuario (y `cifscreds`) y opciones basadas en Kerberos. No se cubrirán aquí; para obtener más información, consulte las páginas de `man` y los artículos disponibles en [access.redhat.com](http://access.redhat.com).

## Montaje de sistemas de archivos de SMB con el servicio de automontaje

El uso del comando `mount` requiere privilegios de `root` para la conexión con los recursos compartidos de SMB. De forma alternativa, se pueden agregar entradas a `/etc/fstab`, pero las conexiones a los servidores SMB estarían activas todo el tiempo.

El servicio de automontaje, o **autofs**, se puede configurar para montar recursos compartidos de SMB “a pedido”, cuando un proceso intenta acceder a un archivo en el recurso compartido de SMB. El servicio de automontaje luego desmontará el recurso compartido cuando ya no se encuentre en uso, después de un determinado período de inactividad.

El proceso para configurar un automontaje en un recurso compartido de SMB usando **autofs** es básicamente el mismo que otros automontajes:

- Agregue un archivo de configuración `auto.master.d` que identifique el directorio base para recursos compartidos y el archivo de asignación asociado.
- Cree o edite el archivo de asignación para incluir los detalles de montaje para el recurso compartido de SMB.

- Habilite e inicie el servicio **autofs**.



### nota

Si aún no está instalado, instale el paquete **autofs**. Al igual que **mount**, el servicio de automontaje también depende del paquete **cifs-utils** para montar los recursos compartidos de SMB.

### El archivo de asignación

Se debe especificar el tipo de sistema de archivos con la opción **-fstype=cifs** y luego una lista de opciones de montaje separadas por comas, las mismas opciones de montaje usadas por el comando **mount**. Delante de la dirección URI del servidor deben agregarse dos puntos ":".

*Un ejemplo:*

Lo siguiente crea un automontaje en **/bakerst/cases** para el recurso compartido de SMB **//&srv;/cases**, y autentica conforme al archivo de credenciales **/secure/sherlock**.

- **/etc/auto.master.d/bakerst.autofs** Contenido:

```
/bakerst /etc/auto.bakerst
```

- **/etc/auto.bakerst** Contenido:

```
cases -fstype=cifs,credentials=/secure/sherlock ://serverX/cases
```

- Contenido de **/secure/sherlock** (propiedad de **root**, perms **600**):

```
username=sherlock
password=violin221B
domain=BAKERST
```

- Habilitación e inicio de **autofs**:

```
[student@desktopX ~]$ sudo systemctl enable autofs
[student@desktopX ~]$ sudo systemctl start autofs
```



### Referencias

Páginas del manual: **mount(8)**, **umount(8)**, **fstab(5)**, **mount.cifs(8)**, **smbclient(1)**, **autofs(5)**, **automount(8)** y **auto.master(5)**

# Práctica: Montaje de un sistema de archivos de SMB

En este trabajo de laboratorio, creará una entrada de montaje en **/etc/fstab** y la montará.

| <b>Recursos:</b> |                                                               |
|------------------|---------------------------------------------------------------|
| <b>Archivos:</b> | <b>samba.txt</b> en el directorio del servidor, para pruebas. |
| <b>Máquinas:</b> | <b>desktopX</b> y <b>serverX</b>                              |

## Resultados:

- Paquete **cifs-utils** instalado.
- La carpeta de inicio de estudiante de serverX montada en **/home/student/work**.
- El archivo **/etc/fstab** incluye la entrada de montaje.

## Andes de comenzar

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

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

- Restablezca su sistema desktopX.
- Inicie sesión en desktopX y abra una terminal.

Tiene un directorio de inicio en serverX que se utiliza para almacenar documentos relativos al trabajo. El directorio se comparte vía Samba para admitir todos los sistemas operativos de escritorio de la empresa.

El administrador de serverX ha confirmado que el nombre del recurso compartido es **student** y que los **uid/gid** son los mismos que los de su instancia desktopX; la contraseña compartida es **student**.

## 1. Instale el paquete

Use **yum** para instalar **cifs-utils**.

```
[student@desktopX ~]$ sudo yum -y install cifs-utils
Loaded plugins: langpacks
Resolving Dependencies
...
Complete!
```

Este paquete proporciona apoyo para montar sistemas de archivos CIFS y es usado por el comando **mount**.

## 2. Crear el punto de montaje

Use **mkdir** para crear el punto de montaje del directorio **work**.

```
[student@desktopX ~]$ mkdir ~/work
```

### 3. Crear el archivo de credenciales

- 3.1. Use **mkdir** para crear el directorio **secure**.

```
[student@desktopX ~]$ sudo mkdir /secure
```

- 3.2. Use **vim** para crear el archivo de credenciales **student.smb** y complételo.

```
[student@desktopX ~]$ sudo vim /secure/student.smb
```

Agregue las siguientes líneas:

```
username=student
password=student
domain=MYGROUP
```

- 3.3. Use **chmod** para proteger el directorio **secure** y el archivo de credenciales **student.smb**.

```
[student@desktopX ~]$ sudo chmod 770 /secure
[student@desktopX ~]$ sudo chmod 600 /secure/student.smb
```

### 4. Actualizar /etc/fstab y montarlo

- 4.1. Use **vim** para agregar la configuración de montaje al final de **/etc/fstab**.

```
[student@desktopX ~]$ sudo vim /etc/fstab
...
/serverX/student /home/student/work cifs credentials=/secure/student.smb 0
0
```

- 4.2. Use **mount** para verificar la configuración y montar el sistema de archivos.

```
[student@desktopX ~]$ sudo mount -a
```

Este comando no debe informar errores. Si lo hace, verifique su configuración en **/etc/fstab**.

### 5. Verificar su acceso

- 5.1. Use **cat** para generar el archivo **samba.txt**.

```
[student@desktopX ~]$ cat ~/work/samba.txt
Success
```

- 5.2. Use **echo** para escribir el punto de montaje **work**.

---

```
[student@desktopX ~]$ echo testing > ~/work/test.txt
```

# Trabajo de laboratorio: Acceso a almacenamiento de red con sistema de archivos de red (NFS)

En este trabajo de laboratorio, instalará un paquete para admitir el automontaje. Cree un automontaje para el directorio "de inicio" de **ldapuserX** desde **classroom.example.com**, un host NFSv4.

| Recursos: |                                  |  |
|-----------|----------------------------------|--|
| Máquinas: | desktopX y classroom.example.com |  |

## Resultados:

El usuario **ldapuserX** podrá iniciar sesión de forma satisfactoria y usar el directorio de *inicio* montado en **/home/guests/ldapuserX**.

## Andes de comenzar

- Restablezca el sistema desktopX.
- Inicie sesión en su sistema de escritorio y configúrelo.

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

- Abra una terminal.

Umbrella Corp usa un servidor central, **classroom**, para alojar los directorios de *inicio* de los usuarios basados en sus LDAP. Los usuarios deben poder iniciar sesión y que los directorios de *inicio* se automonten con acceso de lectura y escritura, listos para su uso.

A continuación, se proporcionan los detalles que necesitará:

- Nombre de usuario: **ldapuserX**
- Contraseña: **kerberos**
- **classroom.example.com** comparte **/home/guests**.
- desktopX punto de montaje: **/home/guests/ldapuserX**
- El directorio de *inicio* debe tener acceso de lectura y escritura.

Cuando haya finalizado su trabajo, reinicie la máquina **desktopX**, luego ejecute el comando **lab nfs grade** desde la máquina **desktopX** para verificar el trabajo.

1. Instale todos los paquetes necesarios para automontar el directorio de *inicio*.
2. Agregue un archivo de configuración **auto.master.d** que identifique el directorio base y el archivo de asignación asociado (use el nombre que desee para el archivo de configuración, pero debe finalizar con **.autofs**), y cree el archivo de asignación asociado (use el nombre que desee para el archivo de asignación).

- 
3. Habilite e inicie el servicio de automontaje.
  4. Use **ssh** para cambiar a **ldapuserX** en **localhost** y confirme el montaje, y el acceso de lectura/escritura.
  5. Reinicie la máquina **desktopX**, y luego, ejecute el comando **lab nfs grade** desde la máquina **desktopX** para verificar el trabajo.

## Solución

En este trabajo de laboratorio, instalará un paquete para admitir el automontaje. Cree un automontaje para el directorio "de inicio" de **ldapuserX** desde **classroom.example.com**, un host NFSv4.

|                  |                                                |
|------------------|------------------------------------------------|
| <b>Recursos:</b> |                                                |
| <b>Máquinas:</b> | <b>desktopX</b> y <b>classroom.example.com</b> |

### Resultados:

El usuario **ldapuserX** podrá iniciar sesión de forma satisfactoria y usar el directorio de *inicio* montado en **/home/guests/ldapuserX**.

### Antes de comenzar

- Restablezca el sistema desktopX.
- Inicie sesión en su sistema de escritorio y configúrelo.

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

- Abra una terminal.

Umbrella Corp usa un servidor central, **classroom**, para alojar los directorios de *inicio* de los usuarios basados en sus LDAP. Los usuarios deben poder iniciar sesión y que los directorios de *inicio* se automonten con acceso de lectura y escritura, listos para su uso.

A continuación, se proporcionan los detalles que necesitará:

- Nombre de usuario: **ldapuserX**
- Contraseña: **kerberos**
- **classroom.example.com** comparte **/home/guests**.
- desktopX punto de montaje: **/home/guests/ldapuserX**
- El directorio de *inicio* debe tener acceso de lectura y escritura.

Cuando haya finalizado su trabajo, reinicie la máquina **desktopX**, luego ejecute el comando **lab nfs grade** desde la máquina **desktopX** para verificar el trabajo.

1. Instale todos los paquetes necesarios para automontar el directorio de *inicio*.

Use **yum** para instalar **autofs**.

```
[student@desktopX ~]$ sudo yum -y install autofs
Loaded plugins: langpacks
Resolving Dependencies
...
Complete!
```

2. Agregue un archivo de configuración **auto.master.d** que identifique el directorio base y el archivo de asignación asociado (use el nombre que desee para el archivo de

configuración, pero debe finalizar con **.autofs**), y cree el archivo de asignación asociado (use el nombre que desee para el archivo de asignación).

#### 2.1. Use **vim** para crear y editar el archivo **/etc/auto.master.d/home.autofs**.

```
[student@desktopX ~]$ sudo vim /etc/auto.master.d/home.autofs
```

Agregue la línea de la siguiente manera:

```
/home/guests /etc/auto.home
```



#### nota

Esta solución utiliza **home.autofs** como el archivo de asignación maestra y **auto.home** como el archivo de asignación, pero los nombres de archivos no son importantes.

#### 2.2. Use **vim** para crear y editar el archivo de asignación **auto.home**.

```
[student@desktopX ~]$ sudo vim /etc/auto.home
```

Agregue la línea de la siguiente manera:

```
* -rw, sync classroom.example.com:/home/guests/&
```

#### 3. Habilite e inicie el servicio de automontaje.

```
[student@desktopX ~]$ sudo systemctl enable autofs
ln -s '/usr/lib/systemd/system/autofs.service' ...
[student@desktopX ~]$ sudo systemctl start autofs
```

#### 4. Use **ssh** para cambiar a **ldapuserX** en **localhost** y confirme el montaje, y el acceso de lectura/escritura.

##### 4.1. Use **ssh** para iniciar sesión como **ldapuserX**.

```
[student@desktopX ~]$ ssh ldapuserX@localhost
```

Si observa algo similar a lo siguiente, escriba **yes** (sí) para aceptar y continuar.

```
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is d9:cc:73:82:3b:8a:74:e4:11:2f:f3:2b:03:a4:46:4d.
Are you sure you want to continue connecting (yes/no)? yes
```

Ingrese la contraseña: **kerberos**.

```
ldapuserX@localhost's password: kerberos
```

- 4.2. Verifique el directorio actual y el acceso de lectura/escritura.

Use **pwd** para verificar el directorio actual.

```
[ldapuserX@desktopX ~]$ pwd
/home/guests/ldapuserX
```

Use **echo** y **cat** para verificar el acceso de lectura y escritura.

```
[ldapuserX@desktopX ~]$ echo hello > test.txt
[ldapuserX@desktopX ~]$ cat test.txt
hello
```

Use **exit** o **Ctrl+D** para cerrar sesión de **ldapuserX**.

5. Reinicie la máquina **desktopX**, y luego, ejecute el comando **lab nfs grade** desde la máquina **desktopX** para verificar el trabajo.

5.1. 

```
[student@desktopX ~]$ sudo systemctl reboot
```

5.2. 

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

# Trabajo de laboratorio: Acceso a almacenamiento de red con SMB

En este trabajo de laboratorio, instalará paquetes para admitir el automontaje de recursos compartidos de CIFS y crear tres automontajes.

| <b>Recursos:</b> |                                                               |
|------------------|---------------------------------------------------------------|
| <b>Archivos:</b> | <b>samba.txt</b> en cada directorio compartido, para pruebas. |
| <b>Máquinas:</b> | <b>desktopX</b> y <b>serverX</b>                              |

## Resultados:

- Instalación de al menos dos paquetes para admitir el automontaje de recursos compartidos de Samba.
- Automonte **/shares/work** con acceso **RW** autenticado a su directorio de inicio en serverX.
- Automonte **/shares/docs** con acceso **RO** de guest al recurso compartido **public**.
- Automonte **/shares/cases** con acceso **RW** autenticado al recurso compartido de equipo restringido **bakerst**.
- Disponible persistentemente luego de un *reinicio*.

## Andes de comenzar

Si aún no lo ha hecho al inicio del ejercicio anterior:

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

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

Siempre realice este paso:

- Restablezca su sistema desktopX.
- Inicie sesión en desktopX y abra una terminal.

Su empresa ejecuta un servicio de Samba en serverX para proporcionar el intercambio de documentos tanto para clientes de Red Hat Enterprise Linux como de Microsoft Windows. El servidor contiene un directorio para que cada usuario almacene sus documentos personales, un directorio de solo lectura públicamente disponible para documentos comunes y varios directorios de equipo para alojar documentos de colaboración.

Es posible que deba llevar a cabo una administración de usuarios y grupos básica en desktopX para garantizar que **student** pueda acceder a archivos en todos los recursos compartidos.

A continuación, se proporcionan los detalles clave de serverX que necesitará:

- Nombre de usuario: **student**
- Contraseña: **student**
- Membresía de grupo: **bakerst, GID=10221**
- Dominio: **MYGROUP**
- Los recursos compartidos están habilitados y se pueden escribir.

desktopX punto de montaje: **/shares/work**

- Hay un recurso compartido denominado **public** que solo requiere privilegios de guest para acceder.

desktopX punto de montaje: **/shares/docs**

- Su equipo tiene un recurso compartido privado, que se puede escribir, denominado **bakerst** que solo es accesible para miembros del grupo **bakerst**.

desktopX punto de montaje: **/shares/cases**

Cuando haya finalizado, reinicie su máquina **desktopX**, y luego ejecute el comando **labc samba grade** desde su máquina **desktopX** para verificar su trabajo.

1. Instale los dos paquetes necesarios para automontar un sistema de archivos CIFS.
2. Agregue un archivo de configuración **auto.master.d** que identifique el directorio base y el archivo de asignación asociado (use el nombre que desee para el archivo de configuración, pero debe finalizar con **.autofs**) y cree el archivo de asignación asociado (use el nombre que desee para el archivo de asignación), y asegúrese de que cada montaje tenga la autenticación adecuada. Según sea necesario, puede crear otros archivos de configuración para admitir la configuración de asignación de automontajes.
3. Asegúrese de que el nombre de usuario **student** tenga los UID y GID correctos para acceder a cada uno de los recursos compartidos (*Sugerencia: bakerst*). En caso de ser necesario, agregue los grupos nuevos que sean necesarios, modifique la membresía del grupo del estudiante, o realice ambas acciones.

**Nota:** Si agrega un nuevo grupo a los grupos complementarios del estudiante, necesitará salir de la shell e iniciar una nueva shell, o usar **newgrp groupname** para cambiar al grupo agregado recientemente. Esto es necesario porque el entorno con el cual se inicia Bash no se actualiza con los nuevos detalles del estudiante.

4. Habilite e inicie el servicio de automontaje.
5. Compruebe que puede acceder a cada recurso compartido y escribir en los recursos compartidos para los cuales tiene privilegios de escritura: **work** y **cases**.

Hay un archivo denominado **samba.txt** que contiene el mensaje "Success" (Correcto) en cada una de las ubicaciones de recursos compartidos. Use **cat samba.txt**.

Use **echo testing > my.txt** para evaluar si puede escribir en un directorio.

- 
6. Cuando haya finalizado, reinicie su máquina **desktopX**, y luego ejecute el comando **lab samba grade** desde su máquina **desktopX** para verificar su trabajo.

## Solución

En este trabajo de laboratorio, instalará paquetes para admitir el automontaje de recursos compartidos de CIFS y crear tres automontajes.

| Recursos: |                                                        |
|-----------|--------------------------------------------------------|
| Archivos: | samba.txt en cada directorio compartido, para pruebas. |
| Máquinas: | desktopX y serverX                                     |

### Resultados:

- Instalación de al menos dos paquetes para admitir el automontaje de recursos compartidos de Samba.
- Automonte /shares/work con acceso RW autenticado a su directorio de inicio en serverX.
- Automonte /shares/docs con acceso RO de guest al recurso compartido public.
- Automonte /shares/cases con acceso RW autenticado al recurso compartido de equipo restringido bakerst.
- Disponible persistentemente luego de un *reinicio*.

### Andes de comenzar

Si aún no lo ha hecho al inicio del ejercicio anterior:

- Restablezca su sistema serverX.
- Inicie sesión en su sistema servidor y configúrelo.

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

Siempre realice este paso:

- Restablezca su sistema desktopX.
- Inicie sesión en desktopX y abra una terminal.

Su empresa ejecuta un servicio de Samba en serverX para proporcionar el intercambio de documentos tanto para clientes de Red Hat Enterprise Linux como de Microsoft Windows. El servidor contiene un directorio para que cada usuario almacene sus documentos personales, un directorio de solo lectura públicamente disponible para documentos comunes y varios directorios de equipo para alojar documentos de colaboración.

Es posible que deba llevar a cabo una administración de usuarios y grupos básica en desktopX para garantizar que **student** pueda acceder a archivos en todos los recursos compartidos.

A continuación, se proporcionan los detalles clave de serverX que necesitará:

- Nombre de usuario: **student**
- Contraseña: **student**

- Membresía de grupo: **bakerst, GID=10221**
- Dominio: **MYGROUP**
- Los recursos compartidos están habilitados y se pueden escribir.  
desktopX punto de montaje: **/shares/work**
- Hay un recurso compartido denominado **public** que solo requiere privilegios de guest para acceder.  
desktopX punto de montaje: **/shares/docs**
- Su equipo tiene un recurso compartido privado, que se puede escribir, denominado **bakerst** que solo es accesible para miembros del grupo **bakerst**.  
desktopX punto de montaje: **/shares/cases**

Cuando haya finalizado, reinicie su máquina **desktopX**, y luego ejecute el comando **lab samba grade** desde su máquina **desktopX** para verificar su trabajo.

1. Instale los dos paquetes necesarios para automontar un sistema de archivos CIFS.

```
[student@desktopX ~]$ sudo yum -y install cifs-utils autofs
Loaded plugins: langpacks
Resolving Dependencies
...
Complete!
```

2. Agregue un archivo de configuración **auto.master.d** que identifique el directorio base y el archivo de asignación asociado (use el nombre que desee para el archivo de configuración, pero debe finalizar con **.autofs**) y cree el archivo de asignación asociado (use el nombre que desee para el archivo de asignación), y asegúrese de que cada montaje tenga la autenticación adecuada. Según sea necesario, puede crear otros archivos de configuración para admitir la configuración de asignación de automontajes.

- 2.1. Use **vim** para crear y editar el archivo **/etc/auto.master.d/shares.autofs**.

```
[student@desktopX ~]$ sudo vim /etc/auto.master.d/shares.autofs
```

Agregue la siguiente línea:

```
/shares /etc/auto.shares
```



### nota

Esta solución utiliza **shares.autofs** como el archivo de asignación maestra y **auto.shares** como el archivo de asignación, pero los nombres de archivos no son importantes.

- 2.2. Use **vim** para crear el archivo de asignación **auto.shares**.

```
[student@desktopX ~]$ sudo vim /etc/auto.shares
```

Agregue las siguientes líneas:

```
work -fstype=cifs,credentials=/etc/me.cred :://serverX/student
docs -fstype=cifs,guest :://serverX/public
cases -fstype=cifs,credentials=/etc/me.cred :://serverX/bakerst
```



### nota

Una alternativa al archivo de credenciales (y los pasos mostrados aquí para crearlo y editarlo) sería sustituir la entrada **credentials=**/**etc/me.cred** en el archivo **auto.shares** con dos entradas, **username=student, password=student**, pero sería menos seguro.

2.3. Use **vim** para crear el archivo de credenciales.

```
[student@desktopX ~]$ sudo vim /etc/me.cred
```

Agregue las siguientes líneas:

```
username=student
password=student
domain=MYGROUP
```

2.4. Use **chmod** para proteger el archivo de credenciales.

```
[student@desktopX ~]$ sudo chmod 600 /etc/me.cred
```



### nota

Este paso no es fundamental para este trabajo de laboratorio, pero se muestra para ofrecer una visión completa.

3. Asegúrese de que el nombre de usuario **student** tenga los UID y GID correctos para acceder a cada uno de los recursos compartidos (*Sugerencia: bakerst*). En caso de ser necesario, agregue los grupos nuevos que sean necesarios, modifique la membresía del grupo del estudiante, o realice ambas acciones.

**Nota:** Si agrega un nuevo grupo a los grupos complementarios del estudiante, necesitará salir de la shell e iniciar una nueva shell, o usar **newgrp groupname** para cambiar al grupo agregado recientemente. Esto es necesario porque el entorno con el cual se inicia Bash no se actualiza con los nuevos detalles del estudiante.

- 3.1. Use el comando **groups** para verificar las membresías del grupo actual correspondientes al usuario **student**.

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

La cuenta **student** no pertenece al grupo **bakerst** (GID **10221**) y deberá agregarse.

- 3.2. Compruebe si el grupo **bakerst** existe en desktopX. Use **grep** para comprobar el archivo **/etc/group**.

```
[student@desktopX ~]$ grep -e bakerst -e 10221 /etc/group
```

El grupo **bakerst** tampoco existe; deberá agregarse primero.

- 3.3. Use **groupadd** para agregar el grupo **bakerst** con GID **10221**.

```
[student@desktopX ~]$ sudo groupadd -g 10221 bakerst
```

- 3.4. Use **usermod** para agregar el grupo **bakerst** a **student** como un grupo complementario.

```
[student@desktopX ~]$ sudo usermod -aG bakerst student
```



### nota

Generalmente, este método no es la mejor solución para alinear valores de UID y GID, dado que hay opciones de montaje que pueden manejar esto. Sin embargo, es una solución adecuada para este trabajo de laboratorio, y usted practica algunas habilidades de administración de usuarios y grupos.

- 3.5. Use **newgrp** para cambiar a **bakerst**.

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

4. Habilite e inicie el servicio de automontaje.

```
[student@desktopX ~]$ sudo systemctl enable autofs
ln -s '/usr/lib/systemd/system/autofs.service' ...
[student@desktopX ~]$ sudo systemctl start autofs
```

5. Compruebe que puede acceder a cada recurso compartido y escribir en los recursos compartidos para los cuales tiene privilegios de escritura: **work** y **cases**.

Hay un archivo denominado **samba.txt** que contiene el mensaje "Success" (Correcto) en cada una de las ubicaciones de recursos compartidos. Use **cat samba.txt**.

Use **echo testing > my.txt** para evaluar si puede escribir en un directorio.

- 5.1. Compruebe que puede leer y escribir en **work**:

```
[student@desktopX ~]$ cd /shares/work
[student@desktopX work]$ cat samba.txt
Success
[student@desktopX work]$ echo testing > my.txt
```

5.2. Compruebe que puede leer, pero no escribir en **docs**:

```
[student@desktopX work]$ cd ../docs
[student@desktopX docs]$ cat samba.txt
Success
[student@desktopX docs]$ echo testing > my.txt
bash: my.txt: Permission denied
```

5.3. Compruebe que puede leer y escribir en **cases**:

```
[student@desktopX docs]$ cd ../cases
[student@desktopX cases]$ cat samba.txt
Success
[student@desktopX cases]$ echo testing > my.txt
```

6. Cuando haya finalizado, reinicie su máquina **desktopX**, y luego ejecute el comando **lab samba grade** desde su máquina **desktopX** para verificar su trabajo.

6.1. 

```
[student@desktopX ~]$ sudo systemctl reboot
```

6.2. 

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

# Resumen

## Montaje de almacenamiento de red con NFS

- Identifique los detalles del recurso compartido de NFS; monte con NFSv4 la carpeta root del servidor de NFS.
- Cree un directorio de punto de montaje.
- Use **mount** o actualice **/etc/fstab** para montar el recurso compartido de NFS.
- Use para desmontar un recurso compartido de NFS.**umount**

## Automontaje de almacenamiento de red con NFS

- Instale el paquete necesario: **autofs**.
- Cree un archivo de asignación maestra en **/etc/auto.master.d/file.autofs**.
- Cree un archivo de asignación para acceder al recurso compartido de NFS: **/etc/auto.name**.
  - Asignaciones directas.
  - Asignaciones indirectas.
  - Asignaciones indirectas usando comodines.
- Inicie y habilite el servicio **autofs** mediante **systemctl**.

## Acceso a almacenamiento de red con SMB

- Identifique los detalles del recurso compartido; por ejemplo, **smbclient -L // server**.
- Cree un directorio de punto de montaje.
- Use **mount** o actualice **/etc/fstab** para montar el recurso compartido de SMB.
- Use para desmontar un recurso compartido.**umount**
- Use el servicio **autofs** para el automontaje, usando las mismas opciones de montaje que **mount**.
  - **enable**, para habilitar el servicio de modo que se inicie en el arranque.
  - **start**, para iniciar el servicio.
- Use **-fstype=cifs** coloque ":" delante de la URI.





## CAPÍTULO 15

# CONFIGURACIÓN DEL FIREWALL

| Descripción general           |                                                                                                                                                                          |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Meta</b>                   | Configurar un firewall básico.                                                                                                                                           |
| <b>Objetivos</b>              | <ul style="list-style-type: none"><li>Configurar un firewall básico usando <code>firewallctl</code>, <code>firewall-config</code> y <code>firewall-cmd</code>.</li></ul> |
| <b>Secciones</b>              | <ul style="list-style-type: none"><li>Limitación de la comunicación de red (y práctica)</li></ul>                                                                        |
| <b>Trabajo de laboratorio</b> | <ul style="list-style-type: none"><li>Limitación de la comunicación de red con <code>firewallctl</code></li></ul>                                                        |

# Limitación de la comunicación de red

## Objetivos

Luego de completar esta sección, los estudiantes deberían poder configurar un firewall básico.

## Conceptos netfilter y firewalld

El kernel Linux incluye un potente subsistema de filtrado de red, **netfilter**. El subsistema **netfilter** permite a los módulos del kernel inspeccionar cada paquete que atraviese el sistema. Esto significa que cualquier paquete de red entrante, saliente o que se reenvíe se puede inspeccionar, modificar, soltar o rechazar de una manera programática, antes de llegar a los componentes en el espacio del usuario. Este es el principal componente para crear un firewall en una máquina Red Hat Enterprise Linux 7.

### Interacción con netfilter

Si bien es teóricamente posible para los administradores del sistema escribir sus propios módulos del kernel para interactuar con **netfilter**, esto típicamente no sucede. En cambio, se usan otros programas para interactuar con **netfilter**. Uno de los más comunes y conocidos de estos programas es **iptables**. En versiones anteriores de Red Hat Enterprise Linux, **iptables** fue el principal método de interacción con el subsistema de **netfilter** del kernel.

El comando **iptables** es una herramienta de bajo nivel, y administrar correctamente los firewall con esta herramienta puede presentar un desafío. Además, solo se ajusta a las reglas de firewall IPv4. Para una cobertura de firewall más completa, se deben usar otras utilidades, como **ip6tables** para IPv6 y **ebtables**.

### Presentación de firewalld

En Red Hat Enterprise Linux 7, se ha presentado un nuevo método de interacción con **netfilter**: **firewalld**. **firewalld** es un daemon del sistema que puede configurar y supervisar las reglas del firewall del sistema. Las aplicaciones pueden hablar con **firewalld** para solicitar que se abran puertos usando el sistema de mensajería **DBus**, una función que se puede desactivar o bloquear. Cubre tanto IPv4 como IPv6, y potencialmente la configuración **ebtables**. El daemon **firewalld** se instala desde el paquete **firewalld**. Este paquete es parte de una instalación **base**, pero no parte de una instalación **minimal**.

**firewalld** simplifica la administración de firewall al clasificar todo el tráfico de la red en **zonas**. En función de los criterios como la dirección IP de la fuente de un paquete o la interfaz de red entrante, el tráfico luego se desvía a las reglas de firewall para la zona adecuada. Cada zona tiene su propia lista de puertos y servicios para abrir o cerrar.



## nota

En el caso de equipos portátiles u otras máquinas que cambian regularmente las redes, **NetworkManager** se puede usar para configurar automáticamente la zona de firewall para una conexión. Las zonas se pueden personalizar con reglas adecuadas para conexiones particulares.

Esto es especialmente útil en el traslado entre el *hogar*, el *trabajo* y las redes inalámbricas *públicas*. Un usuario podría desear llegar al servicio **sshd** de su sistema cuando se conecta a las redes de su hogar y corporativas, pero no cuando se conecta a la red inalámbrica pública en la tienda de café local.

Cada paquete que viene en el sistema se revisará primero para determinar la *dirección de origen*. Si esa dirección de origen está conectada a una zona específica, las reglas de esa zona se analizarán. Si la dirección de origen no está conectada a una zona, se usará la zona de la interfaz de red *entrante*.

Si la interfaz de red no está asociada con una zona por algún motivo, se usará la zona *predeterminada*. La zona predeterminada no es una zona por separado en sí; es una de las otras zonas. De forma predeterminada, se usa la zona **public** (pública), pero el administrador del sistema puede cambiarla.

La mayoría de las zonas permitirá el tráfico a través del firewall que relaciona una lista de puertos y protocolos ("631/udp") o servicios predefinidos ("ssh"). Si el tráfico no relaciona un puerto/protocolo o servicio permitidos, generalmente será rechazado. (La zona **trusted** [de confianza], que permite todo el tráfico de forma predeterminada, es una excepción a esto).

### Zonas predefinidas

**firewalld** incluye un número de zonas predefinidas, aptas para varios propósitos. La zona predeterminada está configurada en **public** y las interfaces se asignan a **public** si no se hacen cambios. La interfaz **lo** se trata como si estuviera en la zona **trusted** (de confianza). En la siguiente tabla, se detalla la configuración de estas zonas en la instalación, pero el administrador del sistema puede luego personalizar estas zonas para que tengan diferentes configuraciones. De forma predeterminada, todas las zonas permiten todo el tráfico entrante que sea parte de una comunicación iniciada por el sistema y todo el tráfico saliente.

### Configuración predeterminada de zonas firewalld

| Nombre de la zona             | Configuración predeterminada                                                                                                                                                                                                                                            |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trusted</b> (de confianza) | Permite todo el tráfico entrante.                                                                                                                                                                                                                                       |
| <b>inicio</b>                 | Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos <b>ssh</b> , <b>mdns</b> , <b>ipp-client</b> , <b>samba-client</b> o <b>dhcpv6-client</b> .                                                    |
| <b>internal</b> (interna)     | Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos <b>sssh</b> , <b>mdns</b> , <b>ipp-client</b> , <b>samba-client</b> , or <b>dhcpv6-client</b> (lo mismo que la zona <b>home</b> para empezar). |
| <b>work</b> (trabajo)         | Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relacione los servicios predefinidos <b>ssh</b> , <b>ipp-client</b> o <b>dhcpv6-client</b> .                                                                                        |

| Nombre de la zona         | Configuración predeterminada                                                                                                                                                                                                                                                                            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>public (pública)</b>   | Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relate los servicios predefinidos <b>ssh</b> o <b>dhcpv6-client</b> . Zona <i>predeterminada para interfaces de red recientemente agregadas</i> .                                                                   |
| <b>external (externa)</b> | Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relate el servicio predefinido <b>ssh</b> . El tráfico IPv4 saliente reenviado a través de esta zona se <i>enmascara</i> para que luzca como que se originó desde la dirección IPv4 de la interfaz de red saliente. |
| <b>dmz</b>                | Rechaza el tráfico entrante a menos que esté relacionado con tráfico saliente o que relate el servicio predefinido <b>ssh</b> .                                                                                                                                                                         |
| <b>block (bloqueo)</b>    | Rechaza todo el tráfico entrante, a menos que esté relacionado con tráfico saliente.                                                                                                                                                                                                                    |
| <b>drop (caída)</b>       | Deja caer todo el tráfico entrante a menos que esté relacionado con tráfico saliente (ni siquiera responde con errores ICMP).                                                                                                                                                                           |

Para conocer una lista de todas las zonas predefinidas y sus usos previstos, consulte la página del manual **firewalld.zones(5)**.

#### Servicios predefinidos

**firewalld** también incluye un número de servicios predefinidos. Estas definiciones de servicios se pueden usar para permitir fácilmente que el tráfico de servicios de red particulares pase a través del firewall. En la siguiente tabla, se detalla la configuración de los servicios predefinidos usados en la configuración predeterminada de las zonas de firewall.

#### Servicios **firewalld** predefinidos seleccionados

| Nombre del servicio  | Configuración                                                                                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ssh</b>           | Servidor SSH local. Tráfico a 22/tcp                                                                                                                                                 |
| <b>dhcpv6-client</b> | Cliente DHCPv6 local. Tráfico a 546/udp en la red fe80::/64 IPv6                                                                                                                     |
| <b>ipp-client</b>    | Impresión IPP local. Tráfico a 631/udp.                                                                                                                                              |
| <b>samba-client</b>  | Archivo Windows local y cliente de intercambio de impresión. Tráfico a 137/udp y 138/udp.                                                                                            |
| <b>mdns</b>          | Resolución del nombre del enlace local DNS (mDNS) multidifusión (multicast). Tráfico a 5353/udp a las direcciones de multidifusión (multicast) 224.0.0.251 (IPv4) o ff02::fb (IPv6). |



## nota

Existen muchos otros servicios predefinidos. El comando **firewall-cmd --get-services** los mostrará. Los archivos de configuración que definen los incluidos en el paquete *firewalld* se pueden encontrar en el directorio **/usr/lib/firewalld/services**, en un formato definido por **firewalld.zone**(5). No analizaremos en más detalle estos archivos en este capítulo.

Para los fines de este capítulo, las opciones más simples para un administrador de sistemas nuevo en **firewalld** es usar servicios predefinidos, o bien especificar explícitamente el puerto/protocolo que desean permitir. La herramienta gráfica **firewall-config** también se puede usar para revisar los servicios predefinidos y para definir servicios adicionales.

# Configurar parámetros de firewall

Hay tres formas principales de que los administradores de sistemas interactúen con **firewalld**:

- Al editar directamente archivos de configuración en **/etc/firewalld/** (no analizado en este capítulo)
- Al usar la herramienta gráfica **firewall-config**
- Al usar **firewall-cmd** desde la línea de comandos

### Configurar parámetros de firewall con firewall-config

**firewall-config** es una herramienta gráfica que se puede usar para alterar e inspeccionar tanto la configuración en ejecución en memoria para **firewalld**, así como la configuración persistente en disco. La herramienta **firewall-config** se puede instalar desde el paquete *firewall-config*.

Una vez instalado, **firewall-config** se puede iniciar desde la línea de comandos como **firewall-config**, o desde el menú Applications (Aplicaciones) bajo Applications > Sundry > Firewall. Si un usuario sin privilegios inicia **firewall-config**, se le solicitará la contraseña **root** para continuar.

## Capítulo 15. Configuración del firewall

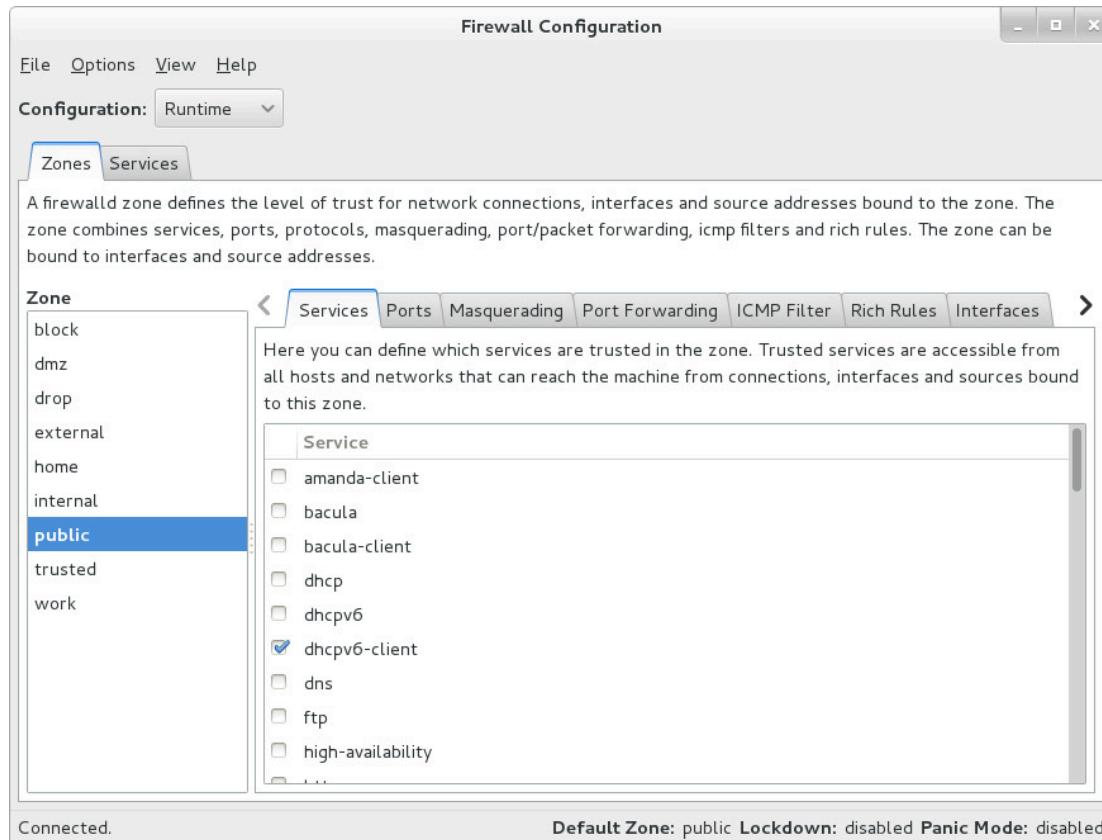


Figura 15.1: Pantalla de configuración de firewall principal

En la pantalla principal de **firewall-config**, un administrador de sistemas puede elegir entre modificar la configuración en memoria actual o la configuración en disco persistente que se usará luego de un nuevo inicio/nueva recarga de **firewalld**. Esto se logra con el menú desplegable **Configuration** (Configuración). En la mayoría de los casos, los administradores de sistemas desearán ajustar la configuración persistente (**Permanent** [Permanente]) y luego usar la entrada de menú **Options (Opciones)** > **Reload Firewalld** (**Volver a cargar firewalld**) para activar sus cambios.

Para modificar una zona, seleccione la zona en el menú **Zone** (Zona) a la izquierda. Interfaces de red y rangos/direcciones IP de origen se pueden asignar en las pestañas **Interfaces** (Interfaces) y **Sources** (Orígenes) a la derecha, respectivamente.

Se pueden abrir puertos al poner una marca de verificación adelante de estos en la pestaña **Services** (Servicios) o al agregar un nuevo puerto en la pestaña **Ports** (Puertos) de esa zona.

Si un conjunto de puertos específicos tiene que abrirse en múltiples zonas, un administrador del sistema también puede definir un servicio para esos puertos. Esto se puede hacer en la pestaña **Services** (Servicios) en la parte superior de la ventana.

La zona *predeterminada* para conexiones especificadas de otro modo se puede cambiar en **Options (Opciones)** > **Change Default Zone** (Cambiar zona predeterminada).



## Importante

Todos los cambios hechos en la configuración **Permanent** (Permanente) no estarán activos hasta la próxima vez que la unidad de servicio **firewalld** se reinicie o se recargue. Del mismo modo, los cambios realizados en la configuración de **Runtime** (Tiempo de ejecución) no sobrevivirán una recarga o un reinicio del servicio **firewalld**.

### Configurar parámetros del firewall con **firewall-cmd**

Para aquellos administradores de sistemas que prefieren trabajar en la línea de comandos o que no pueden usar un entorno gráfico por algún motivo, también hay un cliente de línea de comandos para interactuar con **firewalld**, **firewall-cmd**.

**firewall-cmd** se instala como parte del paquete principal *firewalld*. **firewall-cmd** puede realizar las mismas acciones que **firewall-config**.

En la siguiente tabla, se detallan varios comandos de **firewall-cmd** usados frecuentemente, junto con una explicación. Observe que, a menos que se especifique de otro modo, casi todos los comandos funcionarán en la configuración de *tiempo de ejecución*, a menos que se especifique la opción **--permanent**. Muchos de los comandos detallados toman la opción **--zone=<ZONE>** para determinar qué zona afectan.

| Comandos <b>firewall-cmd</b>                                | Explicación                                                                                                                                                                                                    |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--get-default-zone</b>                                   | Consultar la zona predeterminada actual.                                                                                                                                                                       |
| <b>--set-default-zone=&lt;ZONE&gt;</b>                      | Configurar la zona predeterminada. Esto cambia tanto la configuración del tiempo de ejecución como la permanente.                                                                                              |
| <b>--get-zones</b>                                          | Mostrar todas las zonas disponibles.                                                                                                                                                                           |
| <b>--get-active-zones</b>                                   | Mostrar todas las zonas que están actualmente en uso (tienen una interfaz u origen conectado a esta), junto con la información de su interfaz y origen.                                                        |
| <b>--add-source=&lt;CIDR&gt; [ --zone=&lt;ZONE&gt; ]</b>    | Enrutar todo el tráfico que proviene de la dirección IP o red/máscara de red <b>&lt;CIDR&gt;</b> a la zona especificada. Si no se proporciona ninguna opción <b>--zone=</b> , se usará la zona predeterminada. |
| <b>--remove-source=&lt;CIDR&gt; [ --zone=&lt;ZONE&gt; ]</b> | Eliminar la regla que enruta todo el tráfico que proviene de la dirección IP o red/máscara de red <b>&lt;CIDR&gt;</b> de la zona especificada. Si no se proporciona ninguna                                    |

| Comandos <code>firewall-cmd</code>                                      | Explicación                                                                                                                                                                                          |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                         | opción <code>--zone=</code> , se usará la zona predeterminada.                                                                                                                                       |
| <code>--add-interface=&lt;INTERFACE&gt; [--zone=&lt;ZONE&gt;]</code>    | Enrutar todo el tráfico que proviene de <code>&lt;INTERFACE&gt;</code> a la zona especificada. Si no se proporciona ninguna opción <code>--zone=</code> , se usará la zona predeterminada.           |
| <code>--change-interface=&lt;INTERFACE&gt; [--zone=&lt;ZONE&gt;]</code> | Asociar la interfaz con <code>&lt;ZONE&gt;</code> en lugar de su zona actual. Si no se proporciona ninguna opción <code>--zone=</code> , se usará la zona predeterminada.                            |
| <code>--list-all [--zone=&lt;ZONE&gt;]</code>                           | Mostrar todas las interfaces, fuentes, servicios y puertos configurados para <code>&lt;ZONE&gt;</code> . Si no se proporciona ninguna opción <code>--zone=</code> , se usará la zona predeterminada. |
| <code>--list-all-zones</code>                                           | Recuperar toda la información para todas las zonas. (Interfaces, orígenes, puertos, servicios, etc.)                                                                                                 |
| <code>--add-service=&lt;SERVICE&gt; [--zone=&lt;ZONE&gt;]</code>        | Permitir el tráfico a <code>&lt;SERVICE&gt;</code> . Si no se proporciona ninguna opción <code>--zone=</code> , se usará la zona predeterminada.                                                     |
| <code>--add-port=&lt;PORT/PROTOCOL&gt; [--zone=&lt;ZONE&gt;]</code>     | Permitir el tráfico a los puertos <code>&lt;PORT/PROTOCOL&gt;</code> . Si no se proporciona ninguna opción <code>--zone=</code> , se usará la zona predeterminada.                                   |
| <code>--remove-service=&lt;SERVICE&gt; [--zone=&lt;ZONE&gt;]</code>     | Eliminar <code>&lt;SERVICE&gt;</code> de la lista permitida para la zona. Si no se proporciona ninguna opción <code>--zone=</code> , se usará la zona predeterminada.                                |
| <code>--remove-port=&lt;PORT/PROTOCOL&gt; [--zone=&lt;ZONE&gt;]</code>  | Eliminar los puertos <code>&lt;PORT/PROTOCOL&gt;</code> de la lista permitida para la zona. Si no se proporciona ninguna opción <code>--zone=</code> , se usará la zona predeterminada.              |
| <code>--reload</code>                                                   | Dejar caer la configuración del tiempo de ejecución y aplicar la configuración persistente.                                                                                                          |

### Ejemplo de firewall-cmd

Los siguientes ejemplos muestran la zona predeterminada que se configura en **dmz**, todo el tráfico proveniente de la red **192.168.0.0/24** que se asigna a la zona **internal** (interna) y los puertos de red para **mysql** que se abren en la zona **internal** (interna).

```
[root@serverX ~]# firewall-cmd --set-default-zone=dmz
[root@serverX ~]# firewall-cmd --permanent --zone=internal --add-source=192.168.0.0/24
[root@serverX ~]# firewall-cmd --permanent --zone=internal --add-service=mysql
[root@serverX ~]# firewall-cmd --reload
```



### nota

En situaciones donde la sintaxis básica de **firewalld** no es suficiente, los administradores de sistemas también pueden agregar *rich-rules* (*reglas enriquecidas*), una sintaxis más expresiva, para escribir reglas más complejas. Si así la sintaxis de las reglas enriquecidas no es suficiente, los administradores de sistemas también pueden usar *reglas de Direct Configuration* (*Configuración directa*), básicamente la sintaxis de **iptables** sin formato que se mezclará con las reglas de **firewalld**.

Estos modos avanzados no están incluidos en el alcance de este capítulo.



### Referencias

Páginas del manual: **firewall-cmd(1)**, **firewall-config(1)**, **firewalld(1)**, **firewalld.zone(5)** y **firewalld.zones(5)**

# Práctica: Limitación de la comunicación de red

En este trabajo de laboratorio, configurará un firewall básico.

| Recursos  |                    |
|-----------|--------------------|
| Máquinas: | serverX y desktopX |

## Resultados:

Luego de finalizar este ejercicio, su máquina **serverX** debe tener un servidor web en ejecución que escuche en el puerto sin cifrar **80/TCP** y el puerto encapsulado SSL **443/TCP**. La configuración de firewall en **serverX** solo debe permitir conexiones al puerto encapsulado SSL.

El firewall debe permitir el acceso a **sshd** y **vnc** desde todos los hosts.

## Andes de comenzar

- Restablezca su sistema **serverX**.
- En su sistema **serverX**, asegúrese de que tanto el paquete **httpd** como el paquete **mod\_ssl** estén instalados. Estos paquetes proporcionan el servidor web **Apache** que usted protegerá con un firewall, y las extensiones necesarias para el servidor web para servir contenido mediante SSL.
    - [student@serverX ~]\$ sudo yum -y install httpd mod\_ssl
  - En su sistema **serverX**, cree un nuevo archivo denominado **/var/www/html/index.html**, con el siguiente contenido:
 

```
I am alive
```

    - [student@serverX ~]\$ sudo bash -c "echo 'I am alive' > /var/www/html/index.html"
  - Inicie y habilite el servicio **httpd** en su sistema **serverX**.
    - [student@serverX ~]\$ sudo systemctl start httpd
    - [student@serverX ~]\$ sudo systemctl enable httpd
  - En su sistema **serverX**, asegúrese de que tanto el servicio **iptables** como el **ip6tables** estén *enmascarados*, y de que el servicio **firewalld** esté habilitado y en ejecución.
    - [student@serverX ~]\$ sudo systemctl mask iptables  
[student@serverX ~]\$ sudo systemctl mask ip6tables  
[student@serverX ~]\$ sudo systemctl status firewalld

5. En su sistema **serverX**, inicie la aplicación **firewall-config**. Cuando se le solicite la contraseña de **student**, ingrese **student**.

5.1.

```
[student@serverX ~]$ firewall-config
```

o

Seleccione **Applications (Aplicaciones) > Sundry > Firewall** del menú del sistema.

6. En el menú desplegable **Configuration (Configuración)**, seleccione **Permanent (Permanente)** para cambiar a la edición de la configuración permanente.
7. Agregue el servicio **https** a la lista de servicios permitidos en la zona **public** (pública).
  - 7.1. En la lista **Zone (Zona)**, seleccione **public** (pública). Dado que esta zona es también la zona predeterminada, se destaca en negrita.
  - 7.2. En la pestaña **Services (Servicios)**, agregue una marca de verificación delante del servicio **https**.
  - 7.3. **Importante:** También agregue una marca de verificación delante del servicio **vnc-server**. Si no lo hace, se bloqueará la interfaz gráfica cuando active el firewall. Si accidentalmente se bloquea, recupere el acceso con **ssh -X & srv; firewall-config** desde su máquina **desktopX**.
8. Active la configuración de su firewall seleccionando **Options (Opciones) > Reload Firewalld (Recargar firewalld)** desde el menú.
9. Verifique su trabajo al intentar ver el contenido de su servidor web desde **desktopX**.

9.1. Este comando debería fallar:

```
[student@desktopX ~]$ curl -k http://serverX.example.com
```

9.2. Este comando debe arrojar resultados satisfactorios:

```
[student@desktopX ~]$ curl -k https://serverX.example.com
```



### nota

Si usa **firefox** para conectarse al servidor web, le solicitará la verificación del certificado del host si pasa el firewall satisfactoriamente.

# Trabajo de laboratorio: Limitación de la comunicación de red

En este trabajo de laboratorio, configurará un firewall en su sistema **serverX** para bloquear todo acceso a los servicios que no sean **ssh** y un servidor web que se ejecuta en un puerto **8080/TCP**.

| Recursos  |                    |
|-----------|--------------------|
| Máquinas: | serverX y desktopX |

## Resultados:

Un firewall configurado en **serverX** que bloquea el acceso a servicios que no sean **ssh** y **8080/TCP**.

### Andes de comenzar

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

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

- Restablezca su sistema **desktopX**.

Su empresa ha decidio ejecutar una nueva aplicación. Esta aplicación escucha en puertos **80/TCP** y **8080/TCP**. Debido a consideraciones de seguridad, solo se debe poder llegar al puerto **8080/TCP** desde el mundo exterior. Se entiende que **ssh** (puerto **22/TCP**) también debe estar disponible. Todos los cambios que hace deben persistir en un reinicio.

**Importante:** La interfaz gráfica usada en el entorno Aprendizaje en línea de Red Hat necesita el puerto **5900/TCP** para permanecer disponible también. Este puerto también es conocido bajo el nombre del servicio **vnc-server**. Si accidentalmente se bloquea a usted mismo fuera de su **serverX**, puede intentar recuperar el acceso al usar **ssh** para su máquina **serverX** desde su máquina **desktopX** o restablecer su máquina **serverX**. Si elige restablecer su máquina **serverX**, tendrá que ejecutar los scripts de configuración para este trabajo de laboratorio nuevamente. La configuración de sus máquinas ya incluye una zona personalizada denominada **ROL** que abre estos puertos.

Cuando haya finalizado su trabajo, vuelva a arrancar su máquina **serverX**, y luego, ejecute el comando **lab firewall grade** desde su máquina **desktopX** para verificar su trabajo.

1. Configure su sistema de modo que los servicios **iptables** y **ip6tables** no sean iniciados accidentalmente por un administrador.
2. Verifique si el servicio **firewalld** se está ejecutando. Si no, inícielo.
3. Verifique que la zona de firewall predeterminada esté configurada en **public** (pública).
4. Verifique que no haya puertos no deseados abiertos en la configuración permanente para la zona **public** (pública).

- 
5. Agregue el puerto **8080/TCP** a la configuración permanente para la zona **public** (pública). Verifique su configuración.
  6. Reinicie su máquina **serverX**. (Para realizar una evaluación rápida, también puede usar **sudo firewall-cmd --reload**).
  7. Desde su máquina **desktopX**, ejecute **lab firewall grade** para verificar su trabajo.

## Solución

En este trabajo de laboratorio, configurará un firewall en su sistema **serverX** para bloquear todo acceso a los servicios que no sean **ssh** y un servidor web que se ejecuta en un puerto **8080/TCP**.

| Recursos         |                                  |
|------------------|----------------------------------|
| <b>Máquinas:</b> | <b>serverX</b> y <b>desktopX</b> |

### Resultados:

Un firewall configurado en **serverX** que bloquea el acceso a servicios que no sean **ssh** y **8080/TCP**.

### Andes de comenzar

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

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

- Restablezca su sistema **desktopX**.

Su empresa ha decidio ejecutar una nueva aplicación. Esta aplicación escucha en puertos **80/TCP** y **8080/TCP**. Debido a consideraciones de seguridad, solo se debe poder llegar al puerto **8080/TCP** desde el mundo exterior. Se entiende que **ssh** (puerto **22/TCP**) también debe estar disponible. Todos los cambios que hace deben persistir en un reinicio.

**Importante:** La interfaz gráfica usada en el entorno Aprendizaje en línea de Red Hat necesita el puerto **5900/TCP** para permanecer disponible también. Este puerto también es conocido bajo el nombre del servicio **vnc-server**. Si accidentalmente se bloquea a usted mismo fuera de su **serverX**, puede intentar recuperar el acceso al usar **ssh** para su máquina **serverX** desde su máquina **desktopX** o restablecer su máquina **serverX**. Si elige restablecer su máquina **serverX**, tendrá que ejecutar los scripts de configuración para este trabajo de laboratorio nuevamente. La configuración de sus máquinas ya incluye una zona personalizada denominada **ROL** que abre estos puertos.

Cuando haya finalizado su trabajo, vuelva a arrancar su máquina **serverX**, y luego, ejecute el comando **lab firewall grade** desde su máquina **desktopX** para verificar su trabajo.

1. Configure su sistema de modo que los servicios **iptables** y **ip6tables** no sean iniciados accidentalmente por un administrador.

- 1.1.
 

```
[student@serverX ~]$ sudo systemctl mask iptables
[student@serverX ~]$ sudo systemctl mask ip6tables
```

2. Verifique si el servicio **firewalld** se está ejecutando. Si no, inícielo.

- 2.1.
 

```
[student@serverX ~]$ sudo systemctl status firewalld
```

- 2.2. Si el paso anterior indicó que **firewalld** no estaba habilitado ni ejecutándose:

```
[student@serverX ~]$ sudo systemctl enable firewalld
[student@serverX ~]$ sudo systemctl start firewalld
```

3. Verifique que la zona de firewall predeterminada esté configurada en **public** (pública).

3.1.

```
[student@serverX ~]$ sudo firewall-cmd --get-default-zone
public
```

3.2. Si el paso anterior arrojó otra zona:

```
[student@serverX ~]$ sudo firewall-cmd --set-default-zone public
```

4. Verifique que no haya puertos no deseados abiertos en la configuración permanente para la zona **public** (pública).

4.1.

```
[student@serverX ~]$ sudo firewall-cmd --permanent --zone=public --list-all
public (default)
interfaces:
sources:
services: dhcpcv6-client ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

5. Agregue el puerto **8080/TCP** a la configuración permanente para la zona **public** (pública). Verifique su configuración.

5.1.

```
[student@serverX ~]$ sudo firewall-cmd --permanent --zone=public --add-port
8080/tcp
```

5.2.

```
[student@serverX ~]$ sudo firewall-cmd --permanent --zone=public --list-all
public (default)
interfaces:
sources:
services: dhcpcv6-client ssh
ports: 8080/tcp
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

6. Reinicie su máquina **serverX**. (Para realizar una evaluación rápida, también puede usar **sudo firewall-cmd --reload**).

7. Desde su máquina **desktopX**, ejecute **lab firewall grade** para verificar su trabajo.

7.1.

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

## Resumen

### Limitación de la comunicación de red

- El kernel Linux tiene un subsistema llamado **netfilter** para filtrar el tráfico de red.
- **firewalld** es el componente de espacio del usuario que administra las reglas del firewall.
- **firewalld** divide el tráfico en zonas basadas en la dirección de origen y la interfaz de red a la que llega, y cada zona tiene sus propias reglas de firewall.
- **firewall-config** y **firewall-cmd** se pueden usar para controlar las reglas de firewall.



## CAPÍTULO 16

# VIRTUALIZACIÓN Y KICKSTART

| Descripción general |                                                                                                                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Meta</b>         | Automatizar la instalación de Red Hat Enterprise Linux en máquinas virtuales con máquina virtual basada en kernel (KVM) y libvirt.                                                                                                                                       |
| <b>Objetivos</b>    | <ul style="list-style-type: none"><li>• Explicar los conceptos y la arquitectura de Kickstart.</li><li>• Crear un archivo de configuración de Kickstart.</li><li>• Instalar un sistema Red Hat Enterprise Linux como un host para ejecutar máquinas virtuales.</li></ul> |
| <b>Secciones</b>    | <ul style="list-style-type: none"><li>• Definición del sistema Anaconda Kickstart (y práctica)</li><li>• Implementación de un nuevo sistema virtual con Kickstart (y práctica)</li><li>• Administración de un host de virtualización local (y práctica)</li></ul>        |

# Definición del sistema Anaconda Kickstart

## Objetivos

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

## Introducción a instalaciones Kickstart

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



### nota

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

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

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

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

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

## Comandos de archivo de configuración Kickstart

### Comandos de instalación

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

Ejemplo:

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

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

Ejemplo:

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

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

Ejemplo:

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

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

#### Comandos de partición

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

Ejemplo:

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

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

Ejemplo:

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

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

Ejemplo:

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

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

Ejemplo:

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

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

Ejemplo:

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

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

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

### Comandos de red

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

Ejemplo:

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

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

Ejemplo:

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

### Comandos de configuración

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

Ejemplo:

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

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

Ejemplo:

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

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

Ejemplo:

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

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

Ejemplo:

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

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

Ejemplo:

```
rootpw --plaintext redhat
```

o

```
rootpw --iscrypted 6KUnFfrTz08jv.PiH$YlBb0tXBkWzoMuRfb0.SpbQ....XDR1UuchoMG1
```

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

Ejemplo:

```
selinux --enforcing
```

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

Ejemplo:

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

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

Ejemplo:

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

## Comandos varios

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

Ejemplo:

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

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

Ejemplo:

```
firstboot --disabled
```

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



### nota

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

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

## Ejemplo de un archivo kickstart:

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

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

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

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

```

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

%end

```

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

```

%post --erroronfail

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

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

%end

```



## nota

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



## Referencias

Página del manual (1)**ksverdiff**

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

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

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

## Práctica: Sintaxis y modificación del archivo Kickstart

Relacione los comandos Kickstart con sus descripciones en la tabla.

|           |        |          |           |         |
|-----------|--------|----------|-----------|---------|
| %packages | %post  | auth     | clearpart | network |
| part      | rootpw | services | timezone  | url     |

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

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

## Solución

Relacione los comandos Kickstart con sus descripciones en la tabla.

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

| Descripción                                                                    | Comando        |
|--------------------------------------------------------------------------------|----------------|
| Determina la configuración de red para la instalación y el sistema de destino. | <b>network</b> |

# Implementación de un nuevo sistema virtual con Kickstart

## Objetivos

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

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

## Pasos de instalación Kickstart

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

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

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

## Creación de un archivo de configuración Kickstart

Hay dos maneras de crear un archivo de configuración Kickstart:

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

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

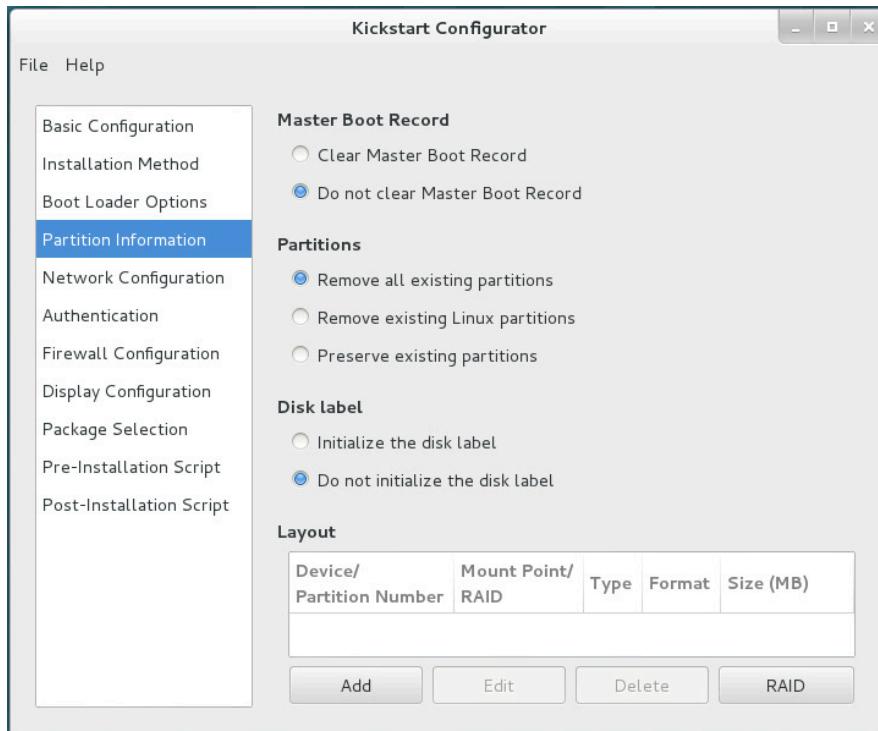


Figura 16.1: Configuración del almacenamiento con system-config-kickstart

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

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

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

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

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

Unknown command: firewall
```

```
[student@desktopX]$ ksvalidator /tmp/anaconda-ks.cfg
The following problem occurred on line 10 of the kickstart file:
no such option: --dsabled
```

El RPM `pykickstart` proporciona `ksvalidator`.

## Publicar el archivo de configuración Kickstart para Anaconda

Ponga el archivo de configuración Kickstart a disposición del instalador:

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

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

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

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

## Arrancar Anaconda y apuntarlo al archivo de configuración Kickstart

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

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

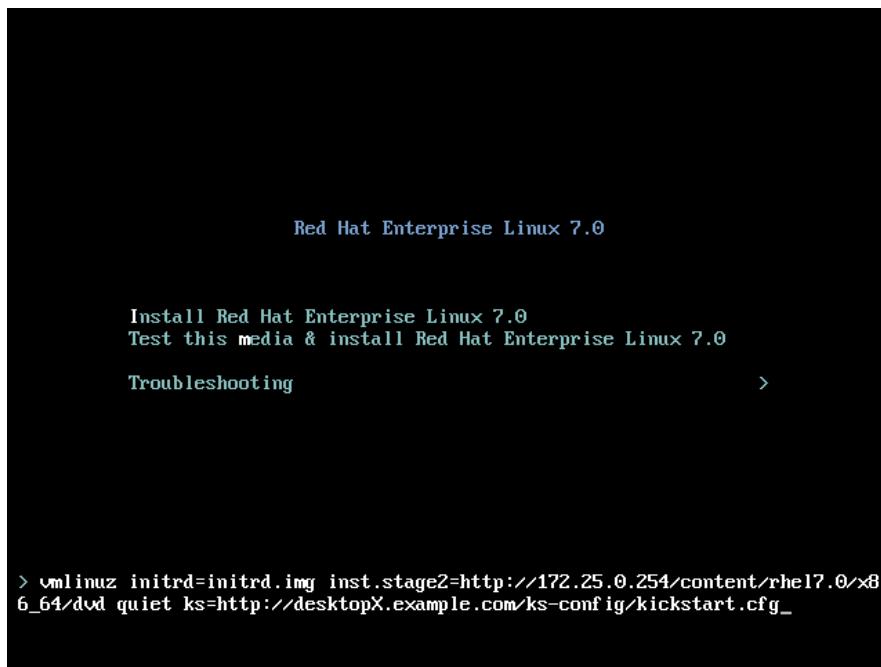


Figura 16.2: Especificación de la ubicación del archivo Kickstart durante el arranque PXE

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



## Nota

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



## Referencias

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

# Práctica: Instalación de un sistema usando Kickstart

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

| Recursos         |                       |
|------------------|-----------------------|
| <b>Archivos:</b> | /root/anaconda-ks.cfg |
| <b>Máquinas:</b> | desktopX              |

## Resultados

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

### Antes de comenzar

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

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

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

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

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

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

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

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

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

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

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

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

Asegúrese de que el tamaño se ajuste a 5120.

2.4. Comente la directiva **reiniciar**:

```
#reboot
```

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

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

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

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

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

```
rootpw --plaintext redhat
```

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

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

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

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

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

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

## Capítulo 16. Virtualización y Kickstart

---

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

# 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.

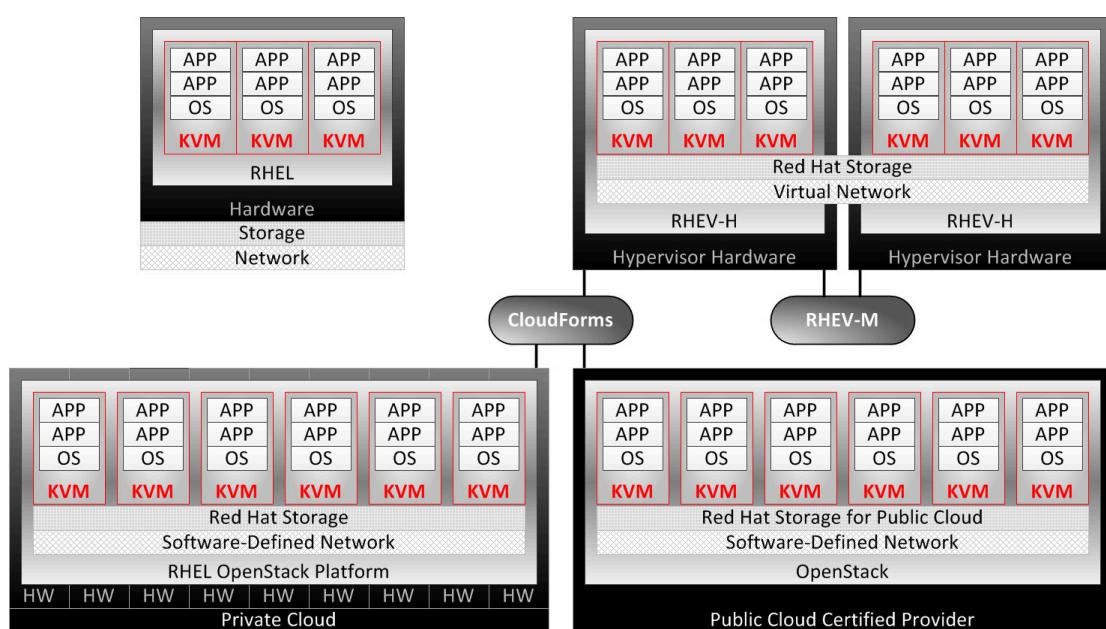


Figura 16.3: KVM en toda la infraestructura en nube de Red Hat

KVM proporciona la tecnología de máquina virtual (VM) en todos los productos Red Hat, que van desde instalaciones 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.

### 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 librerías 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 librería libvirt-client como la API de administración.
- libvirt-client: Proporciona las librerías y API de cliente para el acceso a servidores libvirt, incluida la herramienta de la línea de comandos virsh para administrar y controlar VM.

## Capítulo 16. Virtualización y Kickstart

```
[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 (add-ons) 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 (add-ons) **Virtualization Platform** ubicada en el panel derecho para incluir las herramientas y las utilidades de administración, como se muestra en la siguiente figura.

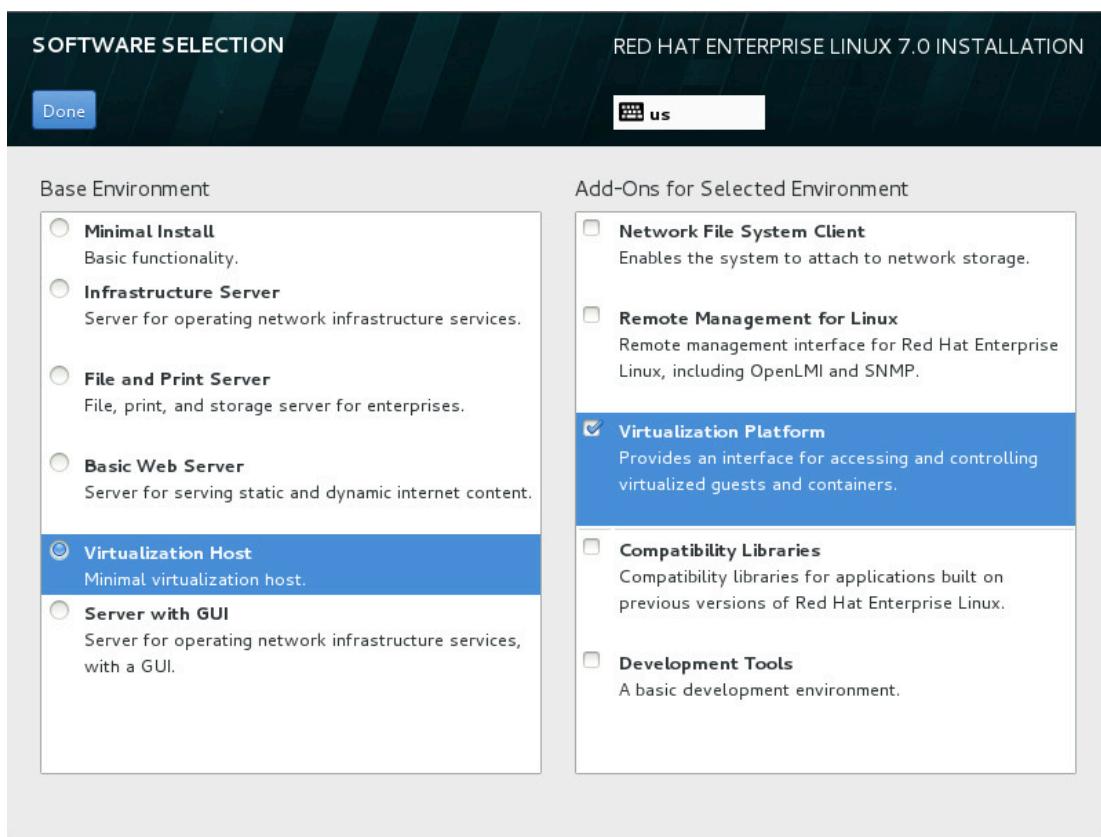


Figura 16.4: Creación de un host de virtualización durante una instalación gráfica

## 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.

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                                                              | <b>virsh subcommand<br/>(virsh subcomando)</b> |
|------------------------------------------------------------------------|------------------------------------------------|
| 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                                                              | <b>virsh subcommand<br/>(virsh subcomando)</b> |
|------------------------------------------------------------------------|------------------------------------------------|
| 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)                               |

# Resumen

## Definición del sistema Anaconda Kickstart

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

## Implementación de un nuevo sistema virtual con Kickstart

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

## Administración de un host de virtualización local

Preparación y creación de una infraestructura de virtualización con Red Hat Enterprise Linux.

